



**Master Agreement**

**Effective Date:** 11/01/22

**Expiration Date:** 10/31/25

**Master Agreement Description:** Consulting Services -Comprehensive disaster planning service

**Buyer Information**

Sue Garcia 207-624-7338 ext. SUE.H.GARCIA@MAINE.GOV

**Issuer Information**

Julie Austin 207-458-9556 ext. Julie.Austin@Maine.gov

**Requestor Information**

Joe Legee 207-215-0442 ext. Joe.Legee@Maine.gov

**Agreement Reporting Categories**

**Reason For Modification:** Amending MA - Amend Scope of work. Please see attached amendment.

**Authorized Departments**

ALL

**Vendor Information**

**Vendor Line #:** 1

**Vendor ID**

VS0000023560

**Vendor Name**

Tidal Basin Government Consulting

**Alias/DBA**

**Vendor Address Information**

126 Business Park Dr Bldg 2

Utica, NY 13502

US

**Vendor Contact Information**

MARY RICCO  
315-272-2107 ext. 102  
AR@RPHC.COM

**Payment Discount Terms**

**Discount 1:** 0.0000% 0 Days

**Commodity Information**

**Vendor Line #:** 1

**Vendor Name:** Tidal Basin Government Consulting

**Commodity Line #:** 1

**Commodity Code:** 91800

**Commodity Description:** Consulting Services -Comprehensive disaster planning service

**Commodity Specifications:** Provide general emergency planning expertise, staffing, and other support across all phases of emergency management as assigned in accordance with an assigned Task Order

**Commodity Extended Description:** Provide professional planning services to assist in aligning identified portions of the State's Comprehensive Emergency Management Plan with Emergency Management Accreditation Program (EMAP) standards as well as general emergency planning expertise and development services across all phases of emergency management; mitigation, preparedness, response, and recovery.

<b>Quantity</b>	<b>UOM</b>	<b>Unit Price</b>
0.00000		0.000000
<b>Delivery Days</b>	<b>Free On Board</b>	
<b>Contract Amount</b>	<b>Service Start Date</b>	<b>Service End Date</b>
0.00	11/01/22	10/31/25
<b>Catalog Name</b>	<b>Discount</b>	
	0.0000 %	
	<b>Discount Start Date</b>	<b>Discount End Date</b>

Please see authorized signatures displayed on the next page

Each signatory below represents that the person has the requisite authority to enter into this Contract.  
The parties sign and cause this Contract to be executed.

State of Maine - Department of Administrative and Financial Services

---

Signature \_\_\_\_\_ Date \_\_\_\_\_

David Morris, Acting Chief Procurement Officer

Vendor

---

Signature \_\_\_\_\_ Date \_\_\_\_\_

---

Print Representative Name and Title \_\_\_\_\_



**AMENDMENT**

DATE: January 31, 2024

ADVANTAGE CONTRACT #: MA 18P 22110900000000000074

DEPARTMENT AGREEMENT #: Department Agreement RFP 202204062

AMENDMENT AMOUNT: \$ 322,545.30

This Amendment, is between the following Department of the State of Maine and Provider:

**STATE OF MAINE DEPARTMENT**

DEPARTMENT: **Department of Veterans Emergency Management / Maine Emergency Management Agency**

Address: **45 Commerce Drive SHS# 72**

City: **Augusta**

State: **Maine**

Zip Code: **04330**

**PROVIDER**

PROVIDER: **Tidal Basin Government Consulting, LLC**

Address: **126 Business Park Drive**

City: **Utica**

State: **NY**

Zip Code: **13502**

Provider's Vendor Customer #: **VS-0000023560**

Each signatory below represents that the person has the requisite authority to enter into this Contract. The parties sign and cause this Contract Amendment to be executed.

**Department: Department of Veterans Emergency Management / Maine Emergency Management Agency**

**Provider: Tidal Basin Government Consulting**

DocuSigned by:

*Joe Legee*

2/6/2024

889D6CC6CB3D479...

Signature **Joe Legee, Deputy Director**

Date

DocuSigned by:

*Stephanie Murphy*

A3B400740611457...

Signature **Stephanie Murphy, VP of**

**Preparedness**

Date **2/2/2024**

*Amendment rev. May 2020*

*Upon final approval by the Division of Procurement Services, a case details page will be made part of this contract.*

<b>AMENDMENT</b>
------------------

The contract is hereby amended as follows: (Check and complete all that apply)

<input type="checkbox"/>	<b>Amended Period:</b>	Original Start Date: Amendment Start Date:  Reason:	Current End Date: New End Date:
<input checked="" type="checkbox"/>	<b>Amended Contract Amount:</b>	Amount of Adjustment: \$ <a href="#">Click or tap here to enter text.</a> New Contract Amount: The billing for Phase IV will be for Time & Materials (T&M) with a Not to Exceed (NTE) amount of \$322,545.30.  Reason: Phase IV	
<input checked="" type="checkbox"/>	<b>Amended Scope of Work:</b>	<p>The Scope of Work is amended as follows:</p> <ol style="list-style-type: none"> <li>1. This Scope of Work builds upon the work completed to date and identified in the first <b>Project Work Plan (PWP)</b> approved March 10, 2023 and identified here as <b>Attachment A.1. (Attachment A.1: Tidal Basin Project Work Plan)</b>. The following deliverables are removed from PWP, Phase III, and no longer required from the Vendor: Incident Response Planning; Vulnerability Management Planning; and Tabletop Exercise (TTX).</li> <li>2. The Tasks and related deliverables for <b>Phase IV, State and Local Cybersecurity Grant Program (SLCGP) Plan Implementation Phase, are as follows:</b> <ol style="list-style-type: none"> <li>A. <b>Task 1:</b> The Vendor will prepare for the Department's approval a detailed second Project Work Plan (PWP #2), including a budget and schedule, for the activities and deliverables identified below for Phase IV, SLCGP Plan Implementation Phase. PWP #2 must include information about the Vendor's project management approach (including team organization, team decision-making, roles and responsibilities and interaction with the SLCGP Planning Team (Planning Team) and SLCGP Cybersecurity Planning Committee (Committee) responsible for coordinating, developing, and approving the strategic Cybersecurity Plan for Maine. The PWP must address quality assurance and quality control procedures, as well as include a project schedule that incorporates compliance with meeting CISA and FEMA's federal SLCGP guidance as identified in the <a href="#">Notice of Funding Opportunity</a> and other related federal guidance documents. In the event federal guidance is revised, or state/federal resources/needs are adjusted, the Department may revise the scope of work as necessary to reflect the Department's requirements.           <ol style="list-style-type: none"> <li>1. Deliverables that must be included in PWP #2 are as follows:               <ol style="list-style-type: none"> <li>i. Compile a comprehensive set of contacts in Maine that will serve as the basis for the Vendor's performance of strategic Planning Team and Committee's outreach efforts to state and local entities for SLCGP-related training and resource offerings.</li> <li>ii. Lead and support the Committee and Planning Team's efforts to communicate with state and local entities regarding SLCGP funding opportunities, resources, and services during Phase IV of SLCGP plan implementation.</li> <li>iii. Lead and support coordination and communication efforts to educate state and local stakeholders about SLCGP resource offerings, working with state and federal resource providers.</li> <li>iv. Support Planning Team's efforts for vendor bid solicitation and vendor coordination for shared service offerings selected for purchase and delivery under the SLCGP Cybersecurity Plan. Vendor is responsible for monitoring the Planning Team's contracts with third party vendors to ensure the successful tracking and delivery of goods/services purchased by the State under the SLCGP from the point of sale to the receiving entity (e.g., state and local entities that qualify as eligible recipients of SLCGP funding through shared products and services). On behalf of the Planning Team, the vendor will work with third party vendors to attempt to resolve any challenges that arise in the successful delivery of shared products and services to state and local entities. In the event that the Vendor identifies an issue with a third party vendor's performance, which has not been remedied in the regular course of business, including without limitation if the third party vendor provides deficient or unsatisfactory products, goods or services, or if there is an issue with the receiving entity, Vendor shall escalate the matter to the Planning Team. Should the State set forth or approve a written corrective action plan or similar written instrument that outlines the steps and requirements the third party vendor must meet to cure the deficiency, Vendor may assist the State in the management, supervision, and monitoring of the third party vendor's compliance to ensure the successful delivery of shared products and services to state and local entities. Notwithstanding the foregoing, the</li> </ol> </li> </ol> </li> </ol> </li> </ol>	





# State of Maine Cybersecurity Planning Services

Project Work Plan

March 10, 2023





## TABLE OF CONTENTS

<b>Overview</b> .....	<b>1</b>
<b>Project Objectives</b> .....	<b>1</b>
<b>Project Management</b> .....	<b>1</b>
Contract Information.....	1
Administration and Management of the Project.....	2
Staffing .....	3
<b>Project Deliverables and Schedule</b> .....	<b>5</b>
Potential Risks to timeline .....	10
<b>Project Team</b> .....	<b>11</b>
<b>Appendix A: Project Work Plan Approval</b> .....	<b>13</b>





## Overview

The Project Work Plan (PWP) is a formal, approved document that defines the objective of the project, as well as how the project is to be executed, monitored, and controlled. The PWP defines the approach to be used by the project team to deliver the intended objective of the project. An approved PWP indicates that it has been reviewed and approved by the Maine Office of Information Technology (OIT) as the Project Sponsor. The period of performance is February 6, 2023 to September 30, 2023.

## Project Objectives

The State of Maine has selected Tidal Basin Government Consulting LLC (Tidal Basin) to assist with conducting a statewide cybersecurity assessment, developing a statewide cybersecurity plan, and ensuring and managing communications and information with local and state partners and stakeholders throughout the project. Our team will support the State in developing and facilitating the assessment, resulting in an analysis of statewide capacity which will inform the cybersecurity plan.

The goal of this project is to support Maine in its pursuit through participation in the State and Local Cybersecurity Grant Program under FEMA/DHS to become a ready and resilient state against current and future cybersecurity threats.

Project objectives (as defined in the Department of Homeland Security's State and Local Cybersecurity Grant Program (SLCGP) guidance) include:

- **Objective 1:** Develop and establish appropriate governance structures, including developing, implementing, or revising cybersecurity plans, to improve capabilities to respond to cybersecurity incidents and ensure continuity of operations.
- **Objective 2:** Understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured assessments.
- **Objective 3:** Implement security protections commensurate with risk.
- **Objective 4:** Ensure organization personnel are appropriately trained in cybersecurity, commensurate with responsibility.

## Project Management

### Contract Information

- **Period of Performance.** The period of performance is February – September 2023, nine months in duration.
- **Master Service Contract Agreement:** Advantage Contract MA 18P  
22110900000000000074



- **Contract Value.** The contract value for this project is a firm-fixed cost of \$516,275.00 as outlined in the proposal.
- **Invoices and Payment Terms.** The State of Maine will pay Tidal Basin in accordance with the terms and conditions provided for in the Contract.

## Administration and Management of the Project

Effective project management includes setting realistic expectations up front and following through with active management and communication throughout the project. Over years of experience and hundreds of projects, our team has established the following means and methods to ensure project success:

- **Kickoff Meeting.** The Kickoff Meeting gets our team and yours together to discuss the project and put an actionable plan in place. This plan is documented as the Project Work Plan (PWP).
  - **Project Work Plan.** The PWP will be our blueprint and guide for ensuring the project stays on time and on task. Following the Project Kickoff Meeting, we will finalize the PWP, ensuring all appropriate deadlines and deliverables are agreed to and included. The PWP documents the agreements reached at the Project Kickoff Meeting relating to the scope, staff assignments, in-depth project schedule(s), administrative and communication procedures, reference documents, and quality assurance / quality control.
  - **Weekly Project Management Meetings.** Weekly meetings allow the Tidal Basin team and Core Planning Team to come together at regular intervals to discuss project progress, near term deliverables and address outstanding issues.
  - **Monthly Progress Reports.** Tidal Basin will develop and submit monthly progress reports to the Project Sponsor detailing each task of the project and including a statement regarding task status, accomplishments from the previous month, unmet needs, and tasks to be completed in the upcoming month. Reports will be submitted to the Project Sponsors on the first Friday of every month throughout the project performance period. Monthly reports will be provided in electronic format.
  - **Other or Ad Hoc In-Person Meetings / Virtual Conference Calls.** Our staff is available for same-day conference calls (phone, video, and webinar / shared screen). We can meet in person with 48-72 hours notice if not already scheduled to be on-site.
- Issue Management.** All Tidal Basin staff are trained to report issues to the Project Manager (PM). Initial issue resolution is conducted by the PM. If the issue cannot initially be resolved, the PM coordinates with Tidal Basin executive leadership as needed to apply resources to resolve the issue or address the need. We believe that open and honest communication is critical so that we can best support the development of the deliverables. Should the need arise, Tidal Basin's executive leadership can work directly with the Project Sponsor or other leadership to resolve issues or unmet needs.
- **Inclusivity.** Our team understands one of the keys to solid emergency planning is employing an approach that is inclusive of the Whole Community. Tidal Basin will work with



OIT to identify partners who are representative of all facets of your stakeholder community to ensure the approach to this project is inclusive of a diverse population with varied needs, priorities, and responsibilities. Partners will be invited to participate as members of the Planning Team, and/or to be consulted as needed during the development of deliverables to ensure our approach is appropriate and representative of all stakeholders, including those with disabilities and access and functional needs (DAFN). Our Whole Community approach ensures that inclusive behaviors are incorporated into stakeholder engagement and coordination efforts, and that deliverables consider diversity, equity, and inclusionary (DEI) elements and principles.

- **Deliverables.** Copies of all deliverables are the property of the State of Maine and will be submitted directly to the Project Sponsor or specific representative throughout the period of performance in electronic format (through a shared drive for live feedback and comments or via email if needed/preferred). The file name indicates either “DRAFT” or “FINAL” of the deliverable. Products are provided in editable format including Word, PowerPoint, Excel, or other appropriate formats.
- **File Management.** Central project files will be maintained in a Microsoft Teams site established by OIT.
- **Sensitive Data Collection.** Confidentiality language has been provided by the State of Maine and will be utilized as appropriate during the collection of sensitive cybersecurity information throughout the assessment and other grant-related data/information collection in furtherance of the SLCGP.
- **Quality Assurance and Quality Control (QA/QC).** A robust QA/QC process ensures multiple levels of review are undertaken, including proofreading and copy editing, industry benchmarking, evaluation against standards, methodology, visual appeal, and readability.

## Staffing

- **OIT Project Sponsor.** Serve as the primary point of contact for Tidal Basin and will coordinate activities with Tidal Basin and outside agencies involved in or affected by the project, to include identifying planning team members and supplying their contact information. The Project Sponsor is responsible for identifying a Core Planning Team and State and Local Cybersecurity Grant Program (SLCGP) Committee (Planning Team) members, which will act as the larger stakeholder group. The Project Sponsor will also assist in identifying appropriate assessment respondents and help facilitate the gathering of their contact information.
- **Project Executive:** Provides project guidance and strategy. Responsible for problem resolution and overall contract performance. Provides high-level strategic planning, facilitates agency liaison and negotiation, defines personnel and resource requirements on a contract level, and assists in directing corporate resources for the performance of the contract and project administration.
- **Project Manager.** Provides project implementation. Responsible for managing the operation and direction of the project and developing strategies for achieving project goals and



objectives. Develops and maintains the PWP, including budget and schedule, serves as the primary point of contact between client and project team, and provides written and oral reports to contract management and client representatives.

- **Deputy Project Manager.** Provides subject matter expertise for all project phases and tasks. Responsible for supporting the PM with all project deliverables. Facilitates meetings and documentation development, manages assigned team members, ensures project deliverables are provided on time, and acts on behalf of the PM when designated.
- **Subject Matter Expert.** Provides expertise based on their specialty. Reviews and analyzes documents, provides recommendations, authors and reviews products as assigned, and participates in meetings. Responsible for the implementation of work under the direction of the PM or designee to ensure task milestones, schedules, and requirements are met.



# Project Deliverables and Schedule

PROJECT SCHEDULE								
Phase	FEB	MAR	APR	MAY	JUN	JUL	AUG	SEP
Task 1.1: Kickoff Meeting	■							
Task 1.2: Form a Collaborative Planning Team	■							
Task 1.3: Active Stakeholder Communication	■	■	■	■	■	■	■	■
Task 1.4: Project Administration	■	■	■	■	■	■	■	■
Task 2.1: Gather Data	■	■						
Task 2.2: Conduct the Assessment		■	■	■				
Task 3.1: Plan Development			■	■	■	■		
Task 3.2: Plan Preparation, Review, and Approval						■	■	
Task 3.3: FEMA/CISA Plan Acceptance							■	■
Task 3.4 Implementation and Maintenance					■	■	■	■

\*Note: The Project Schedule aligns with milestone delivery from the project proposal. This Project Schedule is subject to change as needed and approved by the Project Sponsor.

■ Suggested Task phase      ■ Suggested Milestone Delivery



PHASE 1 – PROJECT INITIATION		
✓	2/1/2023 1100-1200 EST In-Person and Virtual	<b>TASK 1.1: Kickoff Meeting</b>  <b>Deliverables</b> <ul style="list-style-type: none"> <li>› Kickoff meeting materials, agenda, and meeting minutes</li> </ul>
✓	2/17/2023	<b>TASK 1.2: Form a Collaborative Planning Team</b>  <b>Deliverables</b> <ul style="list-style-type: none"> <li>› Planning Team List &amp; Contact Information (Provided by Project Sponsor)</li> <li>› OIT will provision Microsoft Teams/SharePoint access to core team members</li> </ul>
✓	2/20/2023	President's Day Holiday
✓	On-Going	<b>TASK 1.3: Active Stakeholder Communication</b>  <b>Deliverables</b> <ul style="list-style-type: none"> <li>› Communications Strategy</li> <li>› Project One-Pager</li> <li>› Video demonstrating assessment completion</li> </ul>
✓	On-Going	<b>TASK 1.4: Project Administration – Project Work Plan</b>  <b>Deliverables</b> <ul style="list-style-type: none"> <li>› PWP (including finalized goals and objectives)</li> </ul>
✓	Every Thursday, 0815 - 0900	<b>TASK 1.4: Project Administration – Weekly Calls</b>  <i>Subject to change due to holidays or schedule conflicts. Changes will be agreed upon by the PM and Project Sponsor prior to the meeting date.</i>  <b>Deliverables</b> <ul style="list-style-type: none"> <li>› Meeting minutes</li> </ul>
✓	Monthly – Delivered to Project Sponsor no later than the first Friday of each month	<b>Task 1.4 Project Administration – Monthly Reports</b> <ul style="list-style-type: none"> <li>› Friday, March 3, 2023</li> <li>› Friday, April 7, 2023</li> <li>› Friday, May 5, 2023</li> <li>› Friday, June 2, 2023</li> <li>› Friday, July 7, 2023</li> <li>› Friday, August 4, 2023</li> <li>› Friday, September 1, 2023</li> </ul>



		› Friday, October 6, 2023 – Final Report
<b>PHASE 2 – ASSESSMENT</b>		
✓	Estimated completion by March 2023	<p><b>TASK 2.1: Gather Data</b></p> <p><b>Deliverables/Actions:</b></p> <ul style="list-style-type: none"> <li>› Establish data call repository</li> <li>› Inventory of data call submissions</li> <li>› Develop municipal/K-12 school district survey</li> </ul>
✓	March - May 2023	<p><b>TASK 2.2 Conduct the Assessment</b></p> <p><b>Deliverables/Actions:</b></p> <ul style="list-style-type: none"> <li>› Draft assessment questions for Project Sponsor and/or Planning Team review. Assessment questions will be drafted to inform the development of the Cybersecurity Plan, capturing gaps in cybersecurity statewide and providing additional contextual information on cyber capabilities at the state and local level. Per the <a href="#">NOFO</a>, the assessment of statewide current capabilities will also serve as the justification for individual projects.</li> <li>› The assessment will expand upon the THIRA/SPR, allowing for the collection of in-depth, cyber-specific capabilities and needs across the State. The assessment will serve as the road map for individual projects and activities using SLCGP funds.</li> <li>› The Cybersecurity Plan Capabilities Assessment Worksheet, and the <a href="#">Cybersecurity Plan Template</a> provided by CISA will be used to assist with capturing this information and will be customized as appropriate.</li> <li>› Establish and host the assessment during a thirty-day response period</li> <li>› Provide stakeholder support as needed during the thirty-day response period</li> <li>› Risk Assessment Report (RAR)</li> <li>› Cyber Readiness Review (CRR)</li> <li>› Cybersecurity Plan Capabilities Assessment Worksheet</li> </ul>
<b>PHASE 3 – PLAN DEVELOPMENT, DOCUMENTATION AND OUTREACH</b>		
✓	4/17/2023	Patriot’s Day Holiday



✓	5/29/2023	Memorial Day Holiday
✓	6/19/2023	Juneteenth Holiday
✓	April – June 2023	<p><b>TASK 3.1: Plan Development</b></p> <p><b>Deliverables/Actions:</b></p> <ul style="list-style-type: none"> <li>› Planning Meeting #1 – conduct, agenda, PPT, and minutes</li> <li>› Plan outline/template for Project Sponsor and/or Planning Team review and approval</li> <li>› Submit a Draft Cybersecurity Plan written to meet the baseline requirements as prescribed in the DHS NOFO, Appendix C. The Plan will leverage threat information previously collected by the State (THIRA/SPR), as well as information from the Nationwide Cybersecurity Review (NCSR).</li> <li>› The Plan will be written in the manner prescribed under the NOFO, and will include the NOFO's Cybersecurity Plan Template and its fillable Project Plan Worksheet.</li> <li>› The Plan will address how the best practices listed in the NOFO and the 16 required elements (NOFO, Appendix C) will be implemented across the State. In addition to the 16 required elements, the Plan will include the following cybersecurity best practices (listed under required element 5) will be included in the Plan:             <ul style="list-style-type: none"> <li>○ Multi-factor authentication;</li> <li>○ Enhanced logging;</li> <li>○ Data encryption for data at rest and in transit;</li> <li>○ End use of unsupported/end of life software and hardware that are accessible from the Internet;</li> <li>○ Prohibit use of known/fixed/default passwords and credentials;</li> <li>○ The ability to reconstitute systems (backups); and</li> <li>○ Migration to the .gov internet domain.</li> </ul> </li> <li>› Per the NOFO, Cybersecurity Plan Metrics will be included in the Plan, detailing how the State will measure both: 1) how the state will implement the plan; and 2) how the state will reduce cybersecurity risks to, and identify, respond to, and recover from cybersecurity threats to, information systems owned or operated by, or</li> </ul>





		<p>on behalf of, the state or local governments within the state. These measures should be at the macro level, related to the goals, objectives, and priorities as part of the overarching strategic plan and not associated with individual projects (See page 6 of the NOFO).</p> <ul style="list-style-type: none"> <li>› <b>Throughout plan development the SLCPG Committee (Planning Team) will be engaged and provided an opportunity to provide guidance, identify funding priorities, and identify a process for obtaining local consent, in compliance with the NOFO.</b></li> <li>› Per the NOFO, the Plan will identify the State role as leader and service provider.</li> </ul>
✓	July 2023	<ul style="list-style-type: none"> <li>› <b>Provide the SLCGP Committee (Planning Team) with the Draft plan for review and initiate the local consent process</b></li> </ul>
✓	7/4/2023	Independence Day Holiday
✓	August 2023	<p><b>TASK 3.2: Plan Review and Approval</b></p> <p><b>Deliverables/Actions:</b></p> <ul style="list-style-type: none"> <li>› Hold Bi-Weekly or monthly coordination calls to review plan drafts and solicit feedback from the Planning Team</li> <li>› Conduct Planning Meeting #2 (agenda, PPT and minutes)</li> <li>› <b>Receive and aggregate feedback on the Draft Plan and begin to make revisions incorporating feedback from the SLCPG Committee (Planning Team)</b></li> <li>› <b>Ensure local consent is received and documented</b></li> <li>› <b>Submit Final Cybersecurity Plan to the SLCGP Committee (Planning Team) for approval</b></li> </ul>
	NLT September 30, 2023	<ul style="list-style-type: none"> <li>› Once signed off on by the SLCGP Committee (Planning Team) and CIO/CISO, the Plan will be submitted for approval by the SAA (MEMA) for submission to DHS in advance of the deadline of September 30, 2023. The Plan will be submitted in Word and PDF formats; all associated documents required for submission within the Plan have also been reviewed and submitted in the preferred format prescribed under the NOFO.</li> </ul>



	Post submission	<b>TASK 3.3: FEMA/CISA Plan Acceptance</b>  <b>Deliverables</b> <ul style="list-style-type: none"> <li>› Answer questions or provide responses to questions in coordination with the Project Sponsor</li> <li>› In-scope plan revisions as necessary</li> </ul>
✓	9/4/2023	Labor Day Holiday
✓	Running concurrently with the plan finalization and acceptance period (Jul/Aug/Sept 2023)	<b>TASK 3.4: Outreach and Education (Implementation and Maintenance)</b>  <b>Deliverables</b> <i>(The timing of this task will be contingent on availability and opportunities to conduct outreach and education with stakeholders and will align with priorities established in the Plan)</i> <b>The focus of these trainings is to ensure personnel develop fundamental knowledge and skills necessary to recognize cybersecurity risks and understand their roles and responsibilities within cybersecurity policies, procedures, and practices. Trainings may also focus on the availability of no-cost services or resources available to stakeholders.</b> <ul style="list-style-type: none"> <li>› Kickoff meeting to solidify the scope of education and training – conduct, agenda, PPT and minutes</li> <li>› Live and/or virtual training – conduct, training materials, registration, and participant rosters</li> <li>› Incident response tabletop exercise – planning meetings, conduct, exercise documents, registration, and participant rosters</li> <li>› Ongoing support/technical assistance from cybersecurity experts for in-scope participants</li> </ul>

### Potential Risks to timeline:

- ◆ Lack of attendance/participation at Planning Meetings
- ◆ Lack of information sharing with stakeholders (surveys, document collection, etc.)
- ◆ Delay in providing feedback by predetermined due dates
- ◆ Changes to the scope or project timeline
- ◆ Changes in Team Members or leadership



## Project Team

PROJECT MANAGEMENT TEAM – TIDAL BASIN					
Position	Name	Email	Phone (Cell)	Time Zone	Preferred Communication
Project Executive	Stephanie Murphy	<a href="mailto:smurphy@tidalbasin.rphc.com">smurphy@tidalbasin.rphc.com</a>	949.533.0390	Eastern	No preference
Project Manager	Michelle Burnett	<a href="mailto:mburnett@tidalbasin.rphc.com">mburnett@tidalbasin.rphc.com</a>	401.952.3538	Eastern	No preference
Deputy Project Manager	Diana Kennedy	<a href="mailto:dkennedy@tidalbasin.rphc.com">dkennedy@tidalbasin.rphc.com</a>	410.972.8868	Eastern	Email
Deputy Project Manager	Emily Kaster	<a href="mailto:ekaster@tidalbasin.rphc.com">ekaster@tidalbasin.rphc.com</a>	978.766.7157	Eastern	Email
Subject Matter Expert	David McDowell	<a href="mailto:dmcowell@tidalbasin.rphc.com">dmcowell@tidalbasin.rphc.com</a>	571.730.8464	Eastern	Email
Subject Matter Expert	Keeyan Williams	<a href="mailto:keyaan.williams@class-llc.com">keyaan.williams@class-llc.com</a>	770.354.9341	Eastern	Email
Subject Matter Expert	Steven J. Byndloss	<a href="mailto:steven.byndloss@class-llc.com">steven.byndloss@class-llc.com</a>	770.355.8575	Eastern	Email
Subject Matter Expert	Leida Hardmon	<a href="mailto:leida.hardmon@class-llc.com">leida.hardmon@class-llc.com</a>	404.316.6776	Eastern	Email




PROJECT MANAGEMENT TEAM – OIT					
Position	Name	Email	Phone (Cell)	Time Zone	Preferred Communication
Project Sponsor	Charles Rote	<a href="mailto:Charles.x.rote@maine.gov">Charles.x.rote@maine.gov</a>	207.441.7631	Eastern	Email or Teams
Project Sponsor	Nathan Willigar	<a href="mailto:Nathan.willigar@maine.gov">Nathan.willigar@maine.gov</a>	207.458.1320	Eastern	Email or Teams



## Appendix A: Project Work Plan Approval

The undersigned acknowledge they have reviewed the State of Maine Cybersecurity Services PWP and agree with the approach it presents. Changes to this PWP will be coordinated with and approved by the undersigned or their designated representatives.

Signature:  Date: 3/13/2023  
Nathan Willigar (Mar 13, 2023 09:01 EDT)  
Print Name: Nathan Willigar  
Title: Chief Information Security Officer  
Role: Project Sponsor

Signature: \_\_\_\_\_ Date: \_\_\_\_\_  
Print Name: \_\_\_\_\_  
Title: \_\_\_\_\_  
Role: \_\_\_\_\_






# Maine\_Cybersecurity Services\_PWP\_FINAL\_10 MAR23

Final Audit Report

2023-03-13

Created:	2023-03-13
By:	charles rote (charles.X.Rote@maine.gov)
Status:	Signed
Transaction ID:	CBJCHBCAABAAtkNuWAF-xuPhAQh2A9OeUuXBSSx1iOhG

## "Maine\_Cybersecurity Services\_PWP\_FINAL\_10MAR23" History

-  Document created by charles rote (charles.X.Rote@maine.gov)  
2023-03-13 - 12:59:39 PM GMT
-  Document emailed to Nathan Willigar (Nathan.Willigar@maine.gov) for signature  
2023-03-13 - 1:00:01 PM GMT
-  Email viewed by Nathan Willigar (Nathan.Willigar@maine.gov)  
2023-03-13 - 1:00:55 PM GMT
-  Document e-signed by Nathan Willigar (Nathan.Willigar@maine.gov)  
Signature Date: 2023-03-13 - 1:01:03 PM GMT - Time Source: server
-  Agreement completed.  
2023-03-13 - 1:01:03 PM GMT

