SECTION A. Project Title: Schneider Electric WSTB ICS Development

SECTION B. Project Description and Purpose:

Revision 1 (Umbrella):

Currently, no large-scale, Operational Technology (OT)-enabled water system environment can be disrupted or destructively tested. There is a need for an adaptable testing and training environment to support prevention, mitigation, and response to cyber-physical incidents.

As part of this Umbrella statement of work (SOW), Idaho National Laboratory (INL) and the contractor will build out a large scale, cyber-physical test bed for the purpose of:

- Demonstrating cyber-physical vulnerabilities in municipal water systems, and
- Testing processes and methods for increasing the resilience of water systems to cyber intrusions.

The system will expanded and upgrade the infrastructure of the INL's Water Security Test Bed(WSTB), which has historically been used to test decontamination and recovery from water system contamination events due to accidental or intentional acts or natural disasters.

The Umbrella SOW provides a general overview of the tasks required for the project. As the scope of each task is defined, a separate Project Task Scope (PTS) will be issued. Each PTS will be reviewed against this ECP to ensure the scope of the PTS is included. Revisions to this ECP will be made as needed to cover any changes in scope, documenting any significant environmental impacts.

The tasks shown below in Table 1 include three different categories of work for the project. The following work will be completed at the WSTB:

- Installation of a concrete pad (~10x10'),
- Power and communication wiring runs, and
- Hardware and equipment such as tanks, pumps, etc.

Equipment purchased will include, but is not limited to, hardware for a water system and an industrial control system such as tanks, pumps, piping, sensors, valve actuators, and variable frequency drives. The equipment will be distributed to other projects prior to being excesses after use. The water consumed during experiments, water samples, and chemicals will be discharged to the Central Facility Area (CFA) sewage.

The water samples and samples of the pipe interior walls will be collected during experiments and sent to the Environmental Protection Agency (EPA) labs or commercial labs for analysis. The samples will not be returned and some samples will be analyzed on site. The samples will not be hazardous and will be disposed in wastewater or in the household trash similar to general industrial waste like general PPE (gloves, wipes). The specific sampling details for each individual experiment will be covered in future PTSs. The sample volume per experiment will be a few gallons.

Hazardous chemicals may be used during experiments and will be disposed of via Waste Generator Services (WGS). The waste generated from general industrial waste such as PPE/wipes will be a few gallons per experiment. Other industrial waste from the concrete pad and power and communication wiring will be general wiring debris and trimmings that will consist of a few pounds of wiring, conduit, and electrical connectors. A few cubic feet of concrete waste will be generated.

The configuration of the software and computer services will occur in a lab at INL Research Center (IRC)- 603.

Table. 1 Category Descriptions

Category	Description	Tasks

1	Install a control room trailer at the WSTB. Configure the industrial control system (ICS) servers and Programmable logic controller (PLC). – In addition to funding this configuration step, Schneider will provide an engineer to configure the hardware and software. INL will provide the facilities and operations support required to complete the configuration.	• Build the instrumentation cabinets that will hold the PLCs and associated power supplies and equipment.
		• *Configure the ICS servers and PLC.*
		• Place the control room trailer and install control room equipment.
		  ▪ Grade, compact, gravel trailer location
		  ▪ Connect power and fiber optic lines to trailer.
		  ▪ Install servers, operator station (HMI)
		  ▪ Configure fiber connection between control room and INL laboratories in Idaho Falls
		• Install PLC cabinets and power and communications lines.
		  ▪ Pour concrete pad for PLC cabinets.
		  ▪ Trench and install power and communications runs.
		  ▪ Mount PLC cabinets to pad
		  ▪ *Configure connections between PLC cabinets and control room.*
		• *System operability testing*
		• Initial experiments
		  ▪ *Conduct an initial demonstration of a physical effect of a cyber intrusion.* Examples:
		  ▪ Spoof the chlorine meter to read normal chlorine levels while injecting sodium thiosulfate into the pipeline. This would simulate a combined cyber-physical attack to poison the water system.
		    • Spoof the chlorine meter to read low chlorine levels, causing the automatic hydrant flusher to trigger – releasing/wasting treated water when it should not.

2	Installation of two 5,000 gal. tanks and a VFD-driven pump. Additional installation of associated infrastructure, e.g., secondary containment, piping, sensors, pump controller, etc.	Procure components, equipment, materials
		• Installation step 1
		  ○ Prep ground and pour concrete pad for the tank-pump-tank system
		  ○ Install and line containment trench around the concrete pad
		• Installation step 2
		  ○ Install 2 × 5,000 gal tanks and stair platform.
		  ○ Install pump and variable frequency drive (VFD).
		  ○ Install piping, valves, sensors.
		• Installation step 3
		  ○ Pressure/leak test the system.
		  ○ Configure and test sensors and controls (VFD, valve actuators).

3	Conduct experiments to demonstrate physical impacts from cyber intrusions. The focus and details of each individual experiment will be covered in subsequent project task statements. Examples of tests that may be performed:	• Overflow a tank, while spoofing the tank level sensors. • Run a tank dry by spoofing the level sensors and/or changing the valve assignments in the control room, so that the operator opens/closes the incorrect valve combination. • Attack the pump VFD to force a pump failure. (This would be a potentially destructive test, which may require replacing the pump [an additional cost].)

Original ECP:

The original EC INL-13-049 covered Phase I of the Water Security Test Bed (WSTB). This ECP covers Phase II. Since its inception, United States (U.S.) Environmental Protection Agency (EPA) Office of Homeland Security Research Program (ORD), has been providing water professionals with information and technology that aid in assessing vulnerabilities and detecting contamination in water distribution systems. While this work will continue, future research will also focus on helping with contingency planning, decontamination of water infrastructure and designing future infrastructure to be more resilient to intentional damage and damage from natural causes.

Contamination of drinking water distribution systems could result in adverse public health and economic consequences. The magnitude of consequences could be reduced if contaminant detection is rapid and accurate. While emerging technologies for the detection of chemical, biological, and radiological contaminants in drinking water are promising, existing technologies can be improved. The focus of this project is to test and evaluate commercially available technologies, as well as emerging and pre-commercial technologies. The resulting data will provide water utilities with information to make decisions on which technologies to utilize. This project will also provide rigorous scientific data to identify gaps in technology performance that can be resolved through enhancements.

Water systems within the United States rely more and more upon automated remotely controlled valves and pumps. An authorized operator can now sit in a control room and use Supervisory Control and Data Acquisition (SCADA) software to open and close valves and turn pumps on and off without having to physically be present at the remote site and perform the actions manually. However, this technology also creates opportunities for hackers and malicious actors to attempt to control or disrupt water supply and distribution operations. Very little full-scale research and technology testing has been done for water systems. The WSTB is an ideal venue to perform cyber testing along with other water infrastructure decontamination experiments.

Idaho National Laboratory (INL) is the only location and organization that has the required cyber security testing infrastructure and scientific interest in collaborating on water security experiments. EPA examined a variety of potential locations for this work, including two of INL's own laboratories, but ultimately selected the INL in part because of the scientific interest in water contamination they have. INL is also the home of the Department of Homeland Security's Industrial Control System Cyber Emergency Response Team (ICS-CERT) program and has invested heavily in building cyber security testing infrastructure. In addition, the INL's WSTB can be attacked as many times as necessary to test equipment and train operators without affecting "real" water customers. EPA and INL have already jointly invested over $3.5 million into the design construction and operation of the WSTB such that further experiments can benefit greatly from this previous investment.

The purpose of Phase II of this Strategic Partnership Project (SPP) is to design and construct a cybersecurity test bed using some of the components of the existing WSTB and conduct experiments with it. Phase I of this project has come to completion and this modification outlines the tasks for Phase II.

Phase I of the project included design and installation of the experimental WSTB system. Phase II will focus on designing and building a cyber security simulator and performing experiments at the WSTB. Phase II is a follow-on project which will make use of the WSTB assets as mentioned in the original SOW of this Strategic Partnership Project (SPP). Future SOWs may be introduced as written modifications or new SPP agreements, subject to US Department of Energy (DOE) approval.

In Phase I, INL installed an above-ground piped water system at the INL PBF/CITRC area. It was designed to allow the study of phenomena associated with intentional or accidental contamination of the water and piping system by a variety of contaminants – radiological, biological, and chemical. INL's system was designed to simulate the diurnal flow demand of a typical water distribution system in a square pipe lay out above ground with dimension of approximately 300 feet by 600 feet. Chemical feed pump(s) were incorporated to allow for introduction of contaminants. Sampling points were installed throughout the pipe system to simulate household service connections.

Accommodations for wastewater storage were included to allow for treatment and disposal in accordance with the federal and state standards applicable to INL's procedures. Wastewater is sampled to verify that it meets discharge limits prior to disposal at any location. If disposal is to the ground, limits established in PLN-8104 are followed. Discharge to other units, such as the CFA STP have additional concentration limits.

The WSTB is not connected to existing drinking water systems. Water from the PBF potable water system is isolated by a double check valve or pumped into a clean WSTB supply tank via an air gap and then removed from the system. The WSTB system is designed to allow for water recycle/reuse to the maximum extent practicable. Test bed assembly/operation and discharge permits/agreements were obtained, as required.

Phase II of this project will be focused on providing a safe cybersecurity testing facility. Research in chem/rad/bio decontamination methods, similar to what was conducted in Phase I, will continue. The two lines of inquiry will complement one another and support the overarching goal of providing critical data and methods to utilities and other drinking water providers.

Upon completion of Phase II of this project, in approximately five years, INL will dismantle the WSTB upon the agreement of EPA. EPA will be responsible for the costs of dismantlement and disposition of all components. Prior to dismantlement, EPA will consult with INL to determine if the INL desires to maintain the WSTB for its own purposes. If INL opts to maintain the WSTB past the end of EPA's programmatic needs, INL will assume responsibility for all costs going forward, including maintenance and disposition.

Tasks

Phase I:

Design and installation of the experimental Water Security Test Bed (WSTB) system.

Phase I - Complete			
Task No.	Tasks	Contractor Role/Responsibilities	Task Status
1	Design Water Security Test Bed	Submit assembly drawings and equipment specifications to the Sponsor for approval. The Contractor and Sponsor will coordinate type of drawings required but will be compatible with INL QL-3 standards.	Complete
2	Logistics	Obtain the aged cast iron pipe, fire hydrants, valves and other fittings for the WSTB facility by excavating and stockpiling materials at the proposed test facility. Provide all the necessary parts by the beginning of the assembly period.	Complete
3	Assemble Test Bed	The above ground WSTB will be assembled and pumps installed. The Sponsor will make a site visit to check the operations and to look at hydraulic parameters including the absence of leaks from the system.	Complete
4	Maintain Test Bed	The Contractor will perform maintenance as need for the WSTB in accordance with manufacturer's recommendation.	Ongoing

Phase II:

Design and build a cybersecurity simulator and perform experiments at the Water Security Test Bed (WSTB).

Phase II			
Task No.	Tasks	Contractor Role/Responsibilities	Task Duration
1	Develop the Quality Assurance Project Plan	Provide input to Sponsor as needed to prepare the QAPPs for approval	Month 1-60
2	Design the Cybersecurity Two Tank Automated Pumping Simulator	Design and install a fully automated water distribution pumping system with two 5,000-gallon tanks.	Month 1-2
3	Procure major equipment items	Procure two 5000 -Gallon tanks, variable drive pump, PLC(s), piping, software, telemetry, and automation controls	Month 2-5
4	Construct Concrete Pads	Construct concrete pads for the foundation of the two 5000-gallon tanks	Month 2-5
5	Construct containment trenches	Construct trenches, berms, and geo-liner to control the flow of water and contain any spills or leaks	Month 2-5
6	Install Plumbing systems	Install piping, fittings and valves (plumbing) between the two tanks	Month 5-14
7	Install Variable Pump Drive System	Install variable drive pump to transfer water between the two tanks	Month 5-14
8	Install PLC and Telemetry Systems	Install PLC and telemetry to remotely control the operation of the variable drive pump. Additionally, install floats and pressure sensors in tanks to provide input to SCADA software	Month 5-14
9	Install Software Control System	Install automation software to control room computers to control pump operations	Month 5-14
10	Conduct Experiments	Provide input to Sponsor as needed to prepare the scope for specific experiments on the WSTB /Cyber test bed during subsequent years.	Month 1-60

* Task Start/Finish dates listed in months from the date of execution of this agreement.

The added infrastructure will remain contained in the existing ~4-acre footprint at the CITRC area, adjacent to buildings PBF 632 and PBF 638, on the INL site. Installation methods and materials will be similar to those used in Phase I. The first step in Phase II of the project will be to complete design and installation of the ICS and supporting infrastructure – specifically a sub-system consisting of two 5,000-gallon tanks and a pump controlled by a variable frequency drive, along with associated hardware (e.g., valves, sensors, controllers). Following installation and operability testing of the ICS and the pump and tank sub-system, the project will transition into conducting cybersecurity and decontamination testing. Additions to and/or modifications of the infrastructure will be made as needed to accommodate the goals of future experiments.

This ECP covers the entire project scope – in particular the added cyber and physical infrastructure installation. As was done in Phase I, a NEPA determination (an ECP) will be written for each subsequent experiment that addresses the specific environmental impacts of that experiment.

SECTION C. Environmental Aspects or Potential Sources of Impact:

Air Emissions

Construction has the potential to generate fugitive dust. Actions to minimize fugitive dust, such as application of water spray, shall be implemented, as necessary, to minimize fugitive dust. As required in the INL Title V Air Permit, fugitive dust suppression efforts must be logged by the PI, including the date, time, method, and amount of suppressant applied. These records may be inspected by state regulators. System assembly may require ephemeral use of mobile or portable generators. While emissions are exempt from permitting requirements, records must be available regarding the annual hours of use and preventive maintenance; contact the PEL for details if generators will be used.

Discharging to Surface-, Storm-, or Ground Water

Prior to discharge, water must be verified to comply with discharge requirements established via PLN-8104 and the Waste Acceptance Criteria, if any, of the receiving facility. WGS would characterize and dispose of all waste

Disturbing Cultural or Biological Resources

A Section 106 review was completed under CRMO project number (BEA-20-30 and BEA-20-H158) and resulted in No Historic Properties Affected. Please refer to the Cultural Resource Review (CRR) (BEA-20-30 and BEA-20-H158) for details or Hold Points and Project Specific Instructions of the ECP.

Generating and Managing Waste

Construction and leak-testing of the basic piping system is expected to generate industrial waste. Industrial waste is expected to include scrap metal, common trash, and approximately 50-100 gallons of water released during leak-testing the system. Scrap metal will be recycled/excessed to the maximum extent practicable. Potable water from initial leak testing would be discharged directly to the asphalt or ground surface in accordance with PLN-8104.

At the end of each experiment in which contaminants are introduced into the WSTB, water would be drained from the system to a holding tank or containment lagoon pending treatment to meet criteria for disposal of the treated wastewater at an INL wastewater facility, such as the CFA sewage treatment plant.

Experiments must be reviewed by ESH personnel prior to use of the WSTB. The review must include a determination of the maximum allowable concentration for use in the WSTB, possible treatment methods, and identifying the required treatment levels prior to discharge. Treatment levels for discharge shall be identified through PLN-8104.

Industrial waste will be generated such as concrete waste, PPE, wiring, conduit, and electrical connectors.

Releasing Contaminants

Although not anticipated, there is a potential for spills when using chemicals or fueling equipment. In the event of a spill, notify facility Environmental Staff. If Environmental Staff cannot be contacted, report the release to the Spill Notification Team (208-241-6400). Clean up the spill and turn over spill cleanup materials to WGS.

Using, Reusing, and Conserving Natural Resources

Waste water will be re-used the maximum extent practicable. Scrap metal will be recycled/excessed to the maximum extent practicable. All applicable waste will be diverted from disposal in the landfill when possible. Project personnel will use every opportunity to recycle, reuse, and recover materials and divert waste from the landfill when possible. The project will practice sustainable acquisition, as appropriate and practicable, by procuring construction materials that are energy efficient, water efficient, are bio-based in content, environmentally preferable, non-ozone depleting, have recycled content, or are non-toxic or less-toxic alternatives. New equipment will meet either the Energy Star or SNAP requirements as appropriate.

Environmental Justice

NA

SECTION D.	**Determine Recommended Level of Environmental Review, Identify Reference(s), and State Justification:** Identify the applicable categorical exclusion from 10 Code of Federal Regulation (CFR) 1021, Appendix B, give the appropriate justification, and the approval date.

For Categorical Exclusions (CXs), the proposed action must not: (1) threaten a violation of applicable statutory, regulatory, or permit requirements for environmental, safety, and health, or similar requirements of Department of Energy (DOE) or Executive Orders; (2) require siting and construction or major expansion of waste storage, disposal, recovery, or treatment or facilities; (3) disturb hazardous substances, pollutants, contaminants, or Comprehensive Environmental Response, Compensation, and Liability Act (CERCLA)-excluded petroleum and natural gas products that pre-exist in the environment such that there would be uncontrolled or unpermitted releases; (4) have the potential to cause significant impacts on environmentally sensitive resources (see 10 CFR 1021). In addition, no extraordinary circumstances related to the proposal exist that would affect the significance of the action. In addition, the action is not “connected” to other action actions (40 CFR 1508.25(a)(1) and is not related to other actions with individually insignificant but cumulatively significant impacts (40 CFR 1608.27(b)(7)).

References: B3.6 "Small-scale research and development, laboratory operations, and pilot projects"

Justification: B3.6 Siting, construction, modification, operation, and decommissioning of facilities for small-scale research and development projects; conventional laboratory operations (such as preparation of chemical standards and sample analysis); and small-scale pilot projects (generally less than 2 years) frequently conducted to verify a concept before demonstration actions, provided that construction or modification would be within or contiguous to a previously disturbed or developed area (where active utilities and currently used roads are readily accessible). Not included in this category are demonstration actions, meaning actions that are undertaken at a scale to show whether a technology would be viable on a larger scale and suitable for commercial deployment.

Is the project funded by the American Recovery and Reinvestment Act of 2009 (Recovery Act) ☐ Yes ☒ No

Approved by Robert Douglas Herzog, DOE-ID NEPA Compliance Officer on: 3/27/2024