DOE-ID NEPA CX DETERMINATION
Idaho National Laboratory

CX Posting No.: DOE-ID-INL-20-021

SECTION A. Project Title: NAVFAC - Engineering Command Operational Technology Cybersecurity Support

SECTION B. Project Description and Purpose:

The Navy is requesting support to advance cybersecurity incident response, assessment training, and cyber design effectiveness of U.S. Navy critical infrastructure control systems. The Navy has determined that it requires the unique cybersecurity and cyber incident response subject matter expertise available within Idaho National Laboratories (INL) and the Department of Energy's National Laboratory System to meet these needs.

The following defines tasks to be performed and deliverables required from efforts to be undertaken by Idaho National Laboratories (INL). This project will be a partnership and level-of-effort agreement between the Department of Energy Idaho Field Office, Idaho National Laboratory, and the Navy to provide training, assessment support, subject matter expertise, incident response expertise and other support as requested by the US Government.

Scope of Work

In support of this project, INL subject matter experts (SMEs) will conduct the following tasks and level of effort (LOE) work.

In each task and/or LOE effort, INL will perform project leadership, integration, and oversight of all subtasks, including, but not be limited to: overseeing technical performance of all other tasks, monthly reporting on financial status of program scheduling tasks and program reviews with the sponsor organization, task leads, Contracting Officer Representative (COR), Technical Point of Contact (TPOC), and INL leadership, and other organizations as requested to support.

Task 1: Cyber Physical Risk Assessment and Mitigation Engagements

An INL team will perform a Consequence-driven Cyber-informed Engineering (CCE) engagement at selected facilities. Early engagement will identify potential mitigations, protections, and tripwires for control systems under evaluation, along with identifying cyber-informed engineering principles that could be applied to control systems to enhance overall cybersecurity posture.

CCE provides a framework to help organizations take the steps necessary to evaluate and mitigate the impact of cyber-attacks against industrial control systems (ICS) environments. At its core, CCE is an engineering, analytic, and targeting effort that eliminates the technology trust assumption and fills the existing cybersecurity gaps through a series of repeatable procedures: 1) Consequence Prioritization; 2) System-of-Systems Breakdown; 3) Consequence-based Targeting; and 4) Mitigations and Protections.

The LOE tasking will require a CCE team to travel to selected facilities and meet with key site personnel to determine the scope and priorities of proposed engagements. The LOE task will require Navy assistance to determine what constitutes full scope. Additional funding may be required depending on depth and breadth of scope identified for two locations.

INL will document the process followed for the two locations selected in order to create an easily repeatable engagement process for future sites and military construction projects where INL CCE engagement would be advantageous to the Navy.

INL will provide additional consultation on the assessment process and provide SME/insight on the Navy's recommended requirements to mitigate the potential vulnerabilities identified through the engagement.

Task 2: Operational Technology (OT) Cybersecurity Training

The initial scope of the OT cybersecurity training in this project covers the development and delivery of Navy-specific cybersecurity courses, including:

- OT assessor training
- Facility-related control system
- ICS cybersecurity fundamental training
- OT first responder training
- OT incident response
- Incident response kit training.

The trainings will use an interactive model of program planning that includes ADDIE (analysis, design, development, implementation, and evaluation) as a foundation for curriculum development. This model ensures learners achieve the goals of the course through quality design, clear learning objectives, carefully structured content, relevant learning activities, and an assessment strongly tied to learning objectives.

The following equipment kits will be referenced in the training section of this EC: Industrial Control Systems (ICS) demo kit, and OT incident response kit. The ICS demo kit is a demonstration version of an actual control system that includes control system components. The ICS demo kits are used to show trainees the physical effects of cyber actions. The OT incident response kits will be used in the OT incident response training course as well as during an actual cyber incident.

INL has assumed that the Navy will have an equipment pool of ICS demo kits, laptops, and classroom equipment. The trainings will be scheduled so equipment from the pool is available for each training. If trainings are to be held at the same time or consecutively, it will be necessary to purchase additional equipment. Equipment counts may vary based on the finalized course analysis, and additional equipment may be required to support larger class sizes.

2.1 Navy-Specific OT Assessment Training

INL currently provides OT cyber assessment training for DoD (Department of Defense) personnel. The purpose of this training is to provide team members with a baseline of knowledge and skills specific to operations technology processes, procedures, and tools. The training is specifically designed to enable trainees to conduct ICS cyber vulnerability evaluations of DoD critical infrastructure. It is intended to provide a consistent quality of vulnerability assessments in an environment where the composition of the team includes a variety of capabilities and involves personnel from several agencies.

Specifically, the course covers methods for assessing ICS cybersecurity posture at the device level and system level, utilizing ICS defense-in-depth concepts. This course teaches the delta between OT knowledge and skills, and current skills of information technology (IT) cyber assessment teams.

Navy would like to make modifications to the current OT assessment training to better fit its mission. INL will perform analysis and design reviews to identify the changes required. The Navy has identified the following modifications in advance:

- Update and incorporate the Cyber Security Evaluation Tool (CSET®) course materials removed from previous Army trainings.
- Rewrite the building automation system and ICS device level training to integrate the CyberStrike or other suitable substitute kits. The materials will be owned by the Navy and available for its certified trainers to teach. Navy may refine the learning objectives to include device level training and exercises using Raspberry Pi devices.

INL will acquisition and produce the CyberStrike or suitable substitute ICS kits, laptops, software, wireless equipment, and classroom equipment needed for the training, and will charge the Navy for the materials, labor, and time associated with these efforts. As such, although purchased by INL, these materials belong to the Navy and will be transitioned at an appropriate time.

INL will tighten the script for the mega exercise to make it shorter and more aligned with the Navy mission. INL will investigate ways to reduce the number of instructors required for the exercise to make it easier to transfer to certified Navy instructors.

Lesson plans, trainee manuals, presentation slides, design plan, training event checklists, equipment checklists, and evaluation tools will be developed for the Navy.

The trainings will be held in Idaho Falls, Idaho. The first training will be a pilot and will be occur in August/September of 2020.

2.2 Quarterly OT Assessment Trainings

INL will incorporate requested changes after the August/September pilot. INL will provide trainings during each of the quarters of 2021. These trainings will be held in Idaho Falls, Idaho.

2.3 New OT Assessment Instructor Orientation and Transition

The Navy OT assessment training outlined in Section 2.2.1 will be turned over to certified Navy instructors to teach after the final course in 2021. Certified Navy instructors will attend at least one assessment training prior to the final course. INL will provide the instructors with all course materials. The Navy instructors will review the lesson plan, presentation materials, event checklists, and equipment checklists before attending the new instructor orientation training.

INL instructors and instructional design team members will spend two days going over equipment setup and answering questions. INL instructors will co-teach the final training with certified Navy instructors and answer any questions after the training. If Navy instructors attend additional courses and start co-teaching before the final course, INL can provide the new instructor orientation sooner or on a per instructor basis.

2.4 Facility-Related Control System (FRCS) ICS Cybersecurity Fundamental Course Development and Pilots

INL will develop a 5-day Navy-specific Facility-Related Control Systems (FRCS) ICS Fundamentals training course. This will require INL to gather content, write lesson plans, create interactive exercises with specific evaluation methods, create learning aids (e.g., student guides, slides, etc.), and develop self-study and/or web-based components, as appropriate. INL will provide a lesson plan, trainee guide, course presentation, equipment, event checklists, equipment checklists, surveys, and pre- and post-tests for evaluation.

INL will reuse portions of the cybersecurity and OT materials from the ICS Maritime Cybersecurity Fundamental course developed for the Navy Cyber Warfare Development Group (NCWDG). New content will be developed to supplement the cybersecurity training as defined in the design review.

INL will execute an initial pilot course that includes defining facility requirements, coordinating the needed staff, conducting the pilot training, summarizing the evaluation comments and feedback, and incorporating pilot comments and feedback into subsequent products.

INL will execute two additional pilot courses and incorporate any requested changes before finalizing the course.

The three pilot courses will be taught at facilities identified by The Navy. These facilities must be able to accommodate students, as well as the interactive exercises developed for the course. The Navy will be responsible for any facility costs as they are not included in the cost estimate for this task.

If the Navy would like to have Navy instructors take over the training, a new instructor orientation course could be provided.

2.5 FRCS ICS Cybersecurity Fundamental Regional Trainings

INL will provide three regional trainings after the pilot trainings have been completed and the course if finalized. Between the three pilot trainings and these additional trainings, all six domestic Navy regions will receive the training. INL will provide instructors, ship the equipment and materials, and provide training registration if requested.

The courses will be taught at facilities identified by the Navy. These facilities must be able to accommodate students in the class, as well as the interactive exercises developed for the course. The Navy will be responsible for any facility costs as they are not included in the cost estimate for this task.

Training locations will be inside the United States. Additional funding may be required for international training.

2.6 Develop and Pilot an ICS Cyber First Responder Course

INL will develop a 5-day first responder course to train personnel on how to respond in the case of an ICS cyber incident. The course will help OT personnel understand cyber areas to investigate when something unexpected happens with their equipment. Trainees will learn the optimal ways to contain/halt the malicious activity while saving forensics data for later analysis. INL will incorporate the existing Navy first responder educational materials and tabletop exercise if appropriate. Portions of the DHS Basic Incident Response training will be reused if identified as useful in the design review. INL will perform analysis and design reviews with the customer to identify target audience, prerequisites, class size, learning objectives, and additional course requirements.

INL will gather content, write lesson plans, create interactive exercises with specific evaluation methods, create learning aids (e.g., student guides, slides, etc.), and develop self-study and/or web-based components, as appropriate. INL will provide a lesson plan, trainee guide, course presentation, equipment, event checklists, equipment checklists, surveys, and pre- and post-tests for evaluation.

INL will implement and evaluate the course by coordinating facilities and staff needs, conducting the pilot, summarizing the evaluation comments and feedback, and incorporating pilot comments and feedback into final products.

INL will provide three pilot trainings. After the second pilot, a new instructor orientation course will be provided for certified Navy instructors. Certified Navy instructors will teach at least a portion of the final pilot with INL instructors available for support.

2.7 Provide Two Finalized ICS Cyber First Responder Trainings

INL will provide two finalized ICS Cyber First Responder trainings at the INL following completions of the pilot classes.

2.8 Develop and Pilot an Advanced OT Incident Response Course

INL will develop a 5-day advanced incident response training. The training will provide a deeper dive into specific incident response areas and provide hands on incident response experience. The first part of the week will include lecture and some hands-on exercises. Trainees will learn to use tools from the IR kits developed in Task 3. Next, INL will provide team exercises to increase the trainees' understanding of the concepts. Finally, the trainees will act as an incident response team responding to an ICS incident. INL will perform a design review with the Navy to identify target audience, prerequisites, class size, learning objectives, and course requirements.

INL will gather content, write lesson plans, create interactive exercises with specific evaluation methods, create learning aids (e.g., student guides, slides, etc.), and develop self-study and/or web-based components, as appropriate. INL will provide a lesson plan, trainee guide, course presentations, event checklists, equipment checklists, surveys, and pre- and post-tests for evaluation.

INL will implement and evaluate the course by coordinating facilities and staff needs, conducting the pilot, summarizing the evaluation comments and feedback, and incorporating pilot comments and feedback into final products.

INL will provide three pilot trainings.

2.9 Provide Two Advanced OT Incident Response Trainings

INL will provide two finalized Advanced OT Incident Response trainings at the INL following the completion of the pilot classes.

***Task 3:* Blue Team Capability Development**

INL will work with US Navy Cyber Assessors, Navy Cybersecurity Technical Warrant holder, and authorities as necessary to design a Navy OT-specific fly-away kit for use during incident response, operational cyber assessments and for follow-on assessments. INL will procure, assemble, capability check, and use the kit during the pilot assessor course. The kit will be provided to a Navy cyber assessor (blue team) unit at the completion of the course. The kit will be provided with only the remaining manufacturer's warrantees and will not include any additional maintenance or support beyond the warranty periods. At the direction of the Navy, additional fly-away kits may be procured, assembled and provided to Navy cyber assessor units.

INL will review U.S. Navy Fleet Cyber Command (FCC) standards and coordinate with the appropriate Navy personnel to understand the blue team SOP requirements.

INL will develop a blue team OT assessment standard operating procedures (SOP) that is compliant with FCC standards and meets defined requirements. The development will include field testing the SOP with assessment teams and incorporating changes.

INL will provide a list of recommended positions for an incident response team. Recommended knowledge, skills and abilities (KSAs) will be defined for each position on the team. The team member KSAs will include the information needed to write a position description for a contractor hire.

***Task 4:* Technical SME Support**

INL will provide control system cybersecurity SME input on tasks related to automation technology and process environments including:

- Secure technology design & architecture
- Security engineering
- Incident response, forensics and threat management
- Impact-driven technical risk management, including critical business impact analysis, technical assessment of existing Attack Surface Exposure (ASE), and gap analysis of known ICS threats or best practices vs customer ASE
- Root cause analysis or hazards analysis for cybersecurity, automation technology, and the physical process
- Reliability analysis based on automation technology's influence on total cost of ownership
- Operations Engineering and Excellence (OE&E) support related to
    - New or changing process environments
    - Process disruptions or interruptions related to automation technology
    - Issues originating from cybersecurity, technology administration, or technology design events.

***Task 5:* Technical Evaluation of Navy Enterprise Architecture for FRCS**

INL will perform a cybersecurity review of the Navy Control System Platform Enclave (CSPE) architecture, to include the Navy Utility Monitoring and Control System (NUMCS) and Navy Smart Grid (SG). INL will provide design recommendations, identify cybersecurity gaps, and provide recommended mitigations.

INL will assist in leading discussions to inform the effort and properly enable a sufficient architecture review. INL will complete threat modeling, which will include logging analysis, traffic analysis, threat analysis, identification of possible threat vectors, identification of compensating controls, and provide the visibility to detect those events that cannot be prevented. In addition, INL will review hardware and software settings to confirm they are appropriately configured to minimize attack surface and reduce the threat-based risk.

Assessment will include interfaces between key systems. These interface assessments will include communications protocol and rule set research and analysis, as well as non-intrusive testing such as the analysis of passive packet captures.

Additional analysis will include industry-standard tools to conduct live assessments of the network architecture, evaluate traffic shaping and characterization, and to perform vulnerability scanning. Authenticated vulnerability scans will be performed when technically feasible. This will assist in identifying cybersecurity gaps and assessing system connection traffic schemes.

***Task 6:* Engineering Analysis of Proposed Changes to the Navy OT Enterprise Architecture**

During the Unit Testing portion of the System Operational Verification Test (SOVT), the INL SME will verify if the operational system modules function in a manner consistent with system specifications stated in the corresponding vendor documentation. The SME will apply the Verification Plan provided by Naval Surface Warfare Center (NSWC) Corona. This verification plan outlines the methods to be used for testing the system modules, including test strategies, unit test scope definition, system element test requirements and scoping, and a test matrix connecting the testing performed to the system requirements.

This task above assumes there will be two SOVTs conducted during this project's period of performance.

The INL SME will assist in determining testable Smart Grid tactics, techniques, and procedures in support of Navy coordinated table-top exercises that lead to cybersecurity intrusion prevention on selected naval facility building(s) that are integrated into an Area Wide Energy Management System (AWEMS) and Smart Grid. The SME will assist in demonstrating effective processes that lead to actionable and sustainable cost/energy savings in a cybersecure manner.

This task above assumes there will be three tabletop exercises conducted during this project's period of performance.

***Task 7:** Project Management*

The project management task includes all activities related to establishing the project baseline, executing, monitoring and controlling, and project closeout. Project Management tasks include, but are not limited to:

1. Developing the detailed planning required to complete the scope described above.
2. Maintaining communications with the customer: providing scope, financial and schedule status; discussing any unplanned conditions; providing suggested course corrections and/or mitigations, if needed; providing a liaison between the technical team and the customer when called upon; participate in regular conference calls to coordinate with and status the Navy TPOC.
3. Providing leadership in all areas of project management including but not limited to integration, scope, cost, schedule, human resources, quality, safety, safeguards and security, data protection, risk, and procurement management.
4. Providing accountability to INL and DOE organizational management.
5. Represent the project team in meetings and or other assignments as required by the Navy.

SECTION C. Environmental Aspects or Potential Sources of Impact:

Air Emissions

NA

Discharging to Surface-, Storm-, or Ground Water

NA

Disturbing Cultural or Biological Resources

NA

Generating and Managing Waste

The assembly of computer kits may result in the generation of packing material such as cardboard, foam, etc. Scrap wire may also be generated. Waste will be managed with the assistance of WGS.

Releasing Contaminants

NA

Using, Reusing, and Conserving Natural Resources

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. and are non-toxic or less-toxic alternatives. New equipment will meet either the Energy Star or Significant New Alternatives Policy (SNAP) requirements as appropriate (see http://www.sftool.gov/GreenProcurement/ProductCategory/14).

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: 10 CFR 1021, Appendix B to subpart D, items B1.2 "Training exercises and simulations" and B1.24 "Property Transfers."
Justification: The proposed R&D activities are consistent with CX B1.2 "Training exercises and simulations (including, but not limited to, firing-range training, small-scale and short-duration force-on-force exercises, emergency response training, fire fighter and rescue training, and decontamination and spill cleanup training) conducted under appropriately controlled conditions and in accordance with applicable requirements."

B1.24 "Transfer, lease, disposition, or acquisition of interests in personal property (including, but not limited to, equipment and materials) or real property (including, but not limited to, permanent structures and land), provided that under reasonably foreseeable uses (1) there would be no potential for release of substances at a level, or in a form, that could pose a threat to public health or the environment and (2) the covered actions would not have the potential to cause a significant change in impacts from before the transfer, lease, disposition, or acquisition of interests."

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

Approved by Jason Sturm, DOE-ID NEPA Compliance Officer on: 4/20/2020