REQUEST FOR PROPOSALS

REQUESTING PROPOSALS FOR NETWORK SECURITY APPLICATION PENETRATION TESTING SERVICES

for

GREENVILLE UTILITIES COMMISSION
PO Box 1847
Greenville, North Carolina 27835-1847

ISSUE DATE: NOVEMBER 17, 2023

PROPOSAL PACKAGES SHALL BE RECEIVED BY 3:00 PM (EST) ON DECEMBER 19, 2023.

PURPOSE OF REQUEST FOR PROPOSALS

The Greenville Utilities Commission (GUC) is seeking proposals from firms for a Network Security and Application Penetration Test.

Vendors submitting proposals must have experience doing assessments on organizations with Supervisory Control and Data Acquisition (SCADA) systems. Vendors who have experience conducting assessments with utilities are preferred. Project must be completed and paid for in our current fiscal year that ends on June 30, 2024.

PROPOSALS SHALL BE RECEIVED BY 3:00 PM (EST) ON December 19, 2023. Proposals shall be submitted via e-mail to: haddocgc@guc.com. Attention: Cleve Haddock, Lifetime CLGPO, Procurement Manager, Greenville Utilities Commission, 401 S. Greene Street, Greenville, North Carolina 27834. GUC reserves the right to reject any and all Proposals.

Questions regarding this Request for Proposals (RFP) should be received by or before November 30, 2023. Answers shall be communicated by December 8, 2023. All questions shall be directed to the attention of Cleve Haddock, Lifetime CLGPO, Procurement Manager, (252) 551-1533, at haddocgc@guc.com.

Scope of Services:

The services are to include, but not be limited to:

- Include all of GUC's networks: corporate network and each of the SCADA networks (Electric, Water, Wastewater, and Natural Gas)
- Number of external IPs: 38
- Number of internal IPs (Endpoints) accounts: 510
- Number of IT (non-SCADA) servers (Windows and Linux): 233
- Number of Business Applications: 1
- Number of servers supporting selected business application: 5
- Time allowed for reconnaissance and OSINT: 10 hours

Internal Scope

- Attempt to discover and identify Personally Identifiable Information (PII) or other high value documents of interest
- Attempt to exploit and gain access to four identified SCADA machines with no impact to the production system
- Attempt to compromise the one provided non-production SCADA HMI client or workstation
- Perform application focused penetration test with a single ERP application.

External Scope

- Attempt to gain remote access to as many networks or devices on network as allowed by scope with no impact on production
- Attempt to gain unauthorized access to systems, email, or other applications via breached credentials, exploits or other offensive toolsets
- Reconnaissance and OSINT - Look for any credentials, privileged or confidential documents, items of proprietary interest
- Perform application focused PEN test with a single application – ERP

Deliverables:

Conduct comprehensive network security penetration test and provide a detailed report which includes:

- An Executive Summary
- A description of the methodology used to perform the assessment and any standards they are adhering to.
- Findings of all items in **Scope in Services** with description, rationale, remediation, and impact.
- All recommendations should be identified as either relating to industry best practices, including the source of the best practice recommendation (such as a regulatory, compliance, or authorization scheme), or otherwise identified as the opinion of the contractor and its team.
- A prioritized listing of findings with remediation suggestions.
- Findings should include description of exploits and vulnerabilities used in the attack.
- An output of any vulnerability scans that were performed.

Contract Period:

It is the intent of Greenville Utilities Commission (GUC) to enter into a multi-year contract at the time the contract is awarded by GUC to the successful proposer for a total contract period not to exceed three (3) years. **Prices shall remain fixed during the first year** with option for annual extensions at the same or negotiated prices for up to two (2) additional years if market and service conditions so warrant and prove to be in the best interest of GUC.

PROPOSAL REQUIREMENTS

All proposals must contain, at a minimum, the information listed below. Vendors are asked not to submit advertising material in substitution for responding to below.

1. A Cover Letter.

2. Brief History of Firm.

3. Statement of Professional Qualifications: Include résumés of key staff proposed to perform consulting and design work. One staff member should be designated as the proposed Project Manager, with supporting staff identification.

4. List of Recent Similar Projects Completed: List should include projects with similar scope proposed for this Project, and indicate which staff from the proposed team, if any, participated in the design of each project. List must also include clients' names, contact person, addresses, and telephone numbers for each project for reference.

5. List of Subconsultants: If any subconsultants are used to assist with the services, list the names of the firms along with professional qualifications and recent similar projects completed.

6. Schedule of Rates: List rates charged on an hourly basis for each classification of personnel.

7. Conceptual Project Schedule: Include a conceptual project schedule from project kickoff to completion and total number of hours estimated to complete.

8. Location of Office: Geographic location of office assigned to perform work with listing of key staff who actually work at that location on a permanent basis.

9. Special Considerations: Include any special considerations, conditions, or other circumstances that is foreseen affecting the project.

10. Responses are limited to a total of 40 pages; however, an attachment of a sample report can be beyond the 40-page limit. The font size shall not be smaller than 11-point. E-mail your RFP Submission in a PDF. Format to: haddocgc@guc.com.

SELECTION PROCESS

- Proposals should be received no later than 3:00 PM (EST) December 19, 2023. All firms submitting proposals must be duly licensed to practice business in the State of North Carolina.

- Screening of proposals by a staff committee should be completed by January 12, 2024. The staff committee will review the potential firm's recent specialized experience, firm's staff qualifications, firm's capacity to accomplish the work, firm's past performance, location of the firm and other considerations when screening proposals.

- Contract negotiations with the selected firm should conclude with contract execution on or about January 30, 2024.

EVALUATION AND AWARD:

Proposals will be evaluated by GUC personnel. Selected vendors may be requested to present formal presentations/unit demonstrations on site on a date and time mutually agreeable by both parties.

Evaluation Criteria:

Vendor/unit selection shall be based on evaluation and rating of Vendor's demonstrated competence and qualifications/performance for the type of unit/services/products to be offered. The following guidelines will be used as minimum criteria for rating the Vendor:

- The quality of references from past customers of vendor.
- Quality of approach and methodology that demonstrates an understanding of the unit's requirements
- Quality, extent and relevance of vendor's staff to the project.
- Vendor's schedule and capacity for accomplishing the work in the required time frame
- Overall Costs

GUC reserves the right to reject all proposals or accept such proposals, as appears in its own best interest, and to waive technicalities or irregularities of any kind in the proposal. GUC is not obligated to accept the lowest cost proposal. If a proposal is to be awarded, it will be awarded to the responsible, responsive respondent whose evaluation by GUC indicates that the award will be in GUC's best interests.

TERMS AND CONDITIONS

GUC reserves the right to reject all Proposals or accept such Proposals, as appears in its own best interest, and to waive technicalities or irregularities of any kind in the proposal. GUC is not obligated to accept the lowest cost proposal.

CONFLICT OF INTEREST

In general, conflicts of interest relate to the potential for self-gain usually, but not always, of a fiscal nature. Potential for self-gain can serve to undermine the judgment or objectivity of Proposers providing consultation services. A potential or actual conflict of interest exists when commitments and obligations to GUC are likely to be compromised by a Proposer's other interests or commitments, especially economic, particularly if those interests or commitments are not disclosed. Not all conflicting interests are necessarily impermissible. Timely and complete disclosure of potential conflicts of interest may be a satisfactory remedy and protects the consultant from suspicion and accusations of breach of professional integrity. Proposers are asked to disclose any situation or relationship that might be regarded as potential conflict of interest with, but not limited to, their expected duties and recommendations as defined in this RFP.

PROPOSER INCURRED COSTS

All costs that may be incurred to prepare Qualifications, attend meetings, attend site inspections, provide requested follow-up information, make formal and informal presentations, and for the entire contract negotiations process if applicable, shall be the sole responsibility of each Proposer. GUC is not responsible under any circumstances for reimbursement of any costs that may be incurred by Proposers during the proposal preparation, subsequent selection or negotiation stages.

MINORITY BUSINESS PARTICIPATION PROGRAM

GUC has adopted an Affirmative Action and Minority and Women Business Enterprise Plan (M/WBE) Program. Firms submitting a proposal are attesting that they also have taken affirmative action to ensure equality of opportunity in all aspects of employment, and to utilize M/WBE suppliers of materials and/or labor.

PROPOSAL WITHDRAWAL

A proposer must notify GUC in writing of its request to withdraw a proposal within seventy-two (72) hours after the proposal opening, not including Saturdays, Sundays, or holidays. In order to justify withdrawal, the proposer must demonstrate that a substantial error exists and that the proposal was submitted in good faith.

AFFIRMATIVE ACTION

The Provider will take affirmative action in complying with all Federal and State requirements concerning fair employment and employment of the handicapped, and concerning the treatment of all employees, without discrimination by reason of race, color, religion, sex, national origin, or physical handicap.

MEDIATION/BINDING ARBITRATION

In the event of any dispute between the Parties, the Parties agree to submit any dispute to nonbinding mediation before a mutually agreeable Mediator prior to initiating litigation. If the Parties are unable to agree upon a Mediator within thirty (30) days after demand therefore, either Party may petition a Court of competent jurisdiction for the designation of

a qualified Mediator for these purposes. Each Party shall bear its own costs and expenses of participating 5

in the mediation (including, without limitation, reasonable attorneys' fees), and each Party shall bear one-half (1/2) of the costs and expenses of the Mediator. Unless otherwise agreed, the Parties will hold the mediation in Greenville, North Carolina. The matters discussed or revealed in the mediation session shall not be disclosed in any subsequent litigation. In the event the matter is not resolved in mediation, either Party may request arbitration. The parties shall jointly select an Arbitrator, and shall be bound by the decision of the Arbitrator with respect to any dispute between the parties with respect to this Agreement. If the parties are unable to mutually agree upon an Arbitrator, the Parties shall each select an Arbitrator, and the two Arbitrators so selected shall select a third Arbitrator, and the decision of the majority of the Arbitrators shall be conclusive and binding upon the Parties. The Parties at all times agree to equally split the costs of any Arbitrator(s) selected in an effort to resolve the dispute between the Parties. Any party desiring to resolve a dispute under the terms of this Agreement shall notify the other Party in writing, and the Parties shall seek to agree upon a mutually agreed upon Arbitrator within a period of ten (10) days from the date of such written demand. If the Parties are unable to agree within such ten (10) day period, the Parties shall each select an Arbitrator, and the two (2) Arbitrators so selected shall select a third Arbitrator within fifteen (15) days from the date of the written demand for arbitration, and a decision shall be rendered by the Arbitrator(s) so selected within five (5) days after such Arbitrator(s) is selected.

INDEMNITY PROVISION

Provider agrees to indemnify and save GREENVILLE UTILITIES COMMISSION of the City of Greenville, Pitt County, North Carolina, and the City of Greenville, North Carolina, its co-owners, joint venturers, agents, employees, and insurance carriers harmless from any and all losses, claims, actions, costs, expenses including reasonable attorney fees, judgments, subrogations, or other damages resulting from injury to any person (including injury resulting in death), or damage (including loss or destruction) to property of whatsoever nature of any person arising out of or incident to the performance of the terms of this Contract by Provider, including, but not limited to, Provider's employees, agents, subcontractors, and others designated by Provider to perform work or services in, about, or attendant to, the work and services under the terms of this Contract. Provider shall not be held responsible for any losses, expenses, claims, subrogations, actions, costs, judgments, or other damages, directly, solely, and proximately caused by the negligence of Greenville Utilities Commission of the City of Greenville, Pitt County, North Carolina. Insurance covering this indemnity agreement by the Provider in favor of Greenville Utilities Commission of the City of Greenville, Pitt County, North Carolina, shall be provided by Provider.

GOVERNING LAWS

All requests, contracts, transactions, agreements, etc., are made under and shall be governed by and construed in accordance with the laws of the State of North Carolina.

UNIFORM GUIDANCE

Contracts funded with federal grant or loan funds must be procured in a manner that conforms with all applicable federal laws, policies, and standards, including those under the Uniform Guidance (2 C.F.R. Part 200).

ADMINISTRATIVE CODE

Proposals, bids, Qualifications, and awards are subject to applicable provisions of the North Carolina Administrative Code.

[Balance of page left blank intentionally]

GUC INFORMATION TECHNOLOGY CONTRACT PROVISIONS

In accepting this Order ("Order"), your company (the "VENDOR"), acknowledges and agrees to abide by the Terms and Conditions set forth below. In the event that a binding written contract signed by both the VENDOR and Greenville Utilities Commission of the City of Greenville (GUC) exists, the terms and conditions of this agreement shall supersede any conflicting terms and conditions of the aforementioned contract.

1. INFORMATION SECURITY

1.1 VENDOR agrees to ensure its software and services comply with all applicable laws and regulations. VENDOR shall, at no additional charge, promptly furnish any updates to the software and services necessary for compliance with any changes in laws or regulations during the terms of this Agreement.

1.2 GUC may, at its expense and for reasonable grounds, require VENDOR to participate in audits and tests relative to GUC and/or services provided by VENDOR on behalf of the GUC.

1.3 VENDOR will take every reasonable precaution to ensure the services and software do not introduce nor contain any virus or similar code that may destroy, modify, alter or cause destruction, modification, or alteration in whole or in part, of any GUC data, equipment, networks, software or utility infrastructure.

1.4 VENDOR agrees to allow GUC access to system security logs that affect this contract, its data, and/or its processes. The VENDOR must provide self-service log reporting or review option, or the VENDOR must produce logs based on regulatory retention requirements of data held (e.g. PCI, HIPAA, etc.)

1.5 Notification of security incident or data breach: GUC requires notification of event no later than twenty-four (24) hours after initial identification by VENDOR, when any data protection is compromised, or security incident occurs which may impact GUC. Unauthorized access or disclosure of non-public data is considered a breach. The VENDOR will provide notification to the GUC as soon as it is aware of the breach. If the VENDOR is liable for the loss, the VENDOR shall bear all costs associated with the investigation, response, and recovery from the breach. The breach must be communicated to GUC Information Security Officer (ISO).

1.6 Prior to the effective date of this agreement, VENDOR will, at its expense conduct or certify that the following certifications have been performed:

i. A SOC 2 audit of VENDORS security policies, procedures and controls, to be reviewed and assessed by GUC or its agent or complete a GUC provided security assessment. The SOC 2

and/or security assessment must report on security controls of the solution/application and/or services to be provided.

1.7 VENDOR shall protect GUC data against deterioration or degradation of data quality and authenticity, including, but not limited to, annual third-party data integrity audits performed by an independent, external organization to determine the VENDOR's compliance with standards.

2. NETWORK SECURITY

2.1 VENDOR agrees at all times to maintain network security that, at a minimum, includes network firewall provisioning, intrusion detection, and regular third-party vulnerability assessments. Likewise, VENDOR agrees to maintain network security that conforms to generally recognized industry standards and best practices that VENDOR then applies to its own network.

3. USER AUTHENTICATION AND ACCESS RIGHTS

3.1 All facilities used to store, and process GUC data will implement and maintain administrative, physical, technical and procedural safeguards and industry best practices at a level sufficient to secure such data from unauthorized access, destruction, use, modification or discloser. Such measures will be no less protective than those used to secure the VENDOR's own data of a similar type, and in no event less than, for data of the same type and nature, during the term of this Agreement.

3.2 The VENDOR must take the same care to prevent the disclosure of GUC's confidential information as it takes to prevent disclosure of its own information of a similar nature. In no event, may the VENDOR take less than a reasonable degree of care.

3.3 VENDOR warrants that all GUC data will be encrypted in transmission and at rest (including via web interface).

4. ACCEPTABLE USE

4.1 Confidential Information of the other party may be used by the receiving party only about the performance of or as specifically authorized by this Agreement. Each party will protect the confidentiality of Confidential Information of the other party in the same manner that it protects the confidentiality of its own proprietary and confidential information, including, without limitation, by entering appropriate confidentiality agreements with employees, affiliates, independent contractors and subcontractors. Access to Confidential Information will be restricted to the VENDOR's, its personnel (as well as its agents and independent contractors) engaged in a use permitted under this Agreement. Confidential Information may not

be copied or reproduced without the disclosing party's prior written consent, except as necessary for use about this Agreement.

4.2 GUC data cannot be used or modified outside of the terms of this agreement without written consent of those actions to be performed.

4.3 Subject to the provisions governing all Confidential Information made available under this Agreement, including copies thereof, will be returned or certified destroyed upon the termination of this Agreement or immediately upon the other party's request; provided, that, subject to the terms of this Section, each party may retain copies of the other party's Confidential Information required for its compliance with its record keeping or quality assurance requirements.

5. PUBLIC RECORDS

5.1 Notwithstanding anything contained herein to the contrary, the parties recognize and acknowledge that GUC is a subdivision of the State of North Carolina and is, therefore, subject to the North Carolina Public Records Act (the "Act") at N.C. Gen. Stat. 132-1 et seq. The parties further acknowledge that any information that is not otherwise protected by law is a public record under North Carolina law and may be released and disclosed GUC pursuant to the Act, and that any such release or disclosure shall not in any way constitute a breach of this Agreement, nor shall GUC be liable to the VENDOR for such release or disclosure. In the event GUC receives a request for disclosure of Confidential Information which the VENDOR has specifically marked "Confidential" or "Proprietary" GUC shall give the VENDOR written notice of such request (the "Notice of Request for Disclosure"). In the event the VENDOR has a reasonable basis for contending that the disclosure of such Confidential Information is not required by the Act, the VENDOR shall within ten (10) calendar days after receipt of the Notice of Request for Disclosure notify GUC in writing of its objection to disclosure and the basis therefor. The VENDOR shall indemnify, defend and hold harmless GUC from and against all losses, damages, liabilities, costs, obligations and expenses (including reasonable attorneys' fees) incurred by GUC in connection with any refusal by GUC to disclose Confidential Information after receiving an objection to disclosure from the VENDOR. If GUC receives no written objection from the VENDOR within ten (10) calendar days after the VENDOR's receipt of a Notice of Request for Disclosure, GUC shall disclose the Confidential Information referenced in the Notice of Request for Disclosure. Notwithstanding the foregoing, the parties agree that the computer database information that GUC is required to disclose under N.C. Gen. Stat. §132-6.1 shall not be deemed Confidential Information, and that GUC shall be entitled to disclose such information without notice to the VENDOR.

5.2 In accordance with the North Carolina electronic data-processing records law N.C.G.S. §132-6-1, all software and documentation provided by the VENDOR or its subcontractors is subject to potential public inspection and examination.

6. THIRD PARTY VENDORS

6.1 The VENDOR shall inform GUC of any outsourced functionality and its VENDOR.

6.2 Unless otherwise stated within this agreement, no assignment of the contract or components of the contract can occur without explicit, written agreement from GUC. If portions of the service are provided by a third party, the VENDOR is directly responsible for all terms of the contract, regardless of outsourced functions.

7. EXIT

7.1 VENDOR further agrees that following successful transmission of all data to GUC, any and all GUC data will be erased, destroyed, and rendered unrecoverable and certify in writing that these actions have been completed within thirty (30) calendar days of the termination of this Agreement. At a minimum, a "clear" media sanitization is to be performed in accordance to standards enumerated by the National Institute of Standards, Guidelines for Media Sanitization. During the period between termination of the Agreement and authorization for destruction, all security measures must remain intact, including, but not limited to, encryption, backup, and storage.

8.0 INSURANCE

8.1 Coverage – During the term of the contract, the VENDOR at its sole cost and expense shall provide commercial insurance of such type and with the following coverage and limits:

8.1.1 Workers' Compensation – The VENDOR shall provide and maintain Workers' Compensation Insurance, as required by the laws of North Carolina, as well as employer's liability coverage with minimum limits of $1,000,000 each accident, covering all VENDOR's employees who are engaged in any work under the contract. If any work is sublet, the VENDOR shall require the subcontractor to provide the same coverage for any of its employees engaged in any work under the contract.

8.1.2 General Liability – The VENDOR shall provide and maintain Commercial Liability Coverage written on an "occurrence" basis in the minimum amount of $1,000,000 per occurrence.

8.1.3 Automobile – The VENDOR shall provide and maintain Automobile Liability Insurance, to include coverage for all owned, hired, and non-

owned vehicles used in connection the contract with a minimum combined single limit of $1,000,000 per accident.

8.1.3 Network security & Privacy Liability - The VENDOR shall provide and maintain Commercial Network Security & Privacy Liability insurance, including 3rd party coverage in the minimum amount of $5,000,000 per occurrence.

8.2 Requirements - Providing and maintaining adequate insurance coverage is a material obligation of the VENDOR. All such insurance shall meet all laws of the State of North Carolina. Such insurance coverage shall be obtained from companies that are authorized to provide such coverage and that are authorized to do business in North Carolina by the Commissioner of Insurance. The VENDOR shall at all times comply with the terms of such insurance policies and all requirements of the insurer under any of such insurance policies, except as they may conflict with existing North Carolina laws or this contract. The limits of coverage under each insurance policy maintained by the VENDOR shall not be interpreted as limiting the VENDOR's liability and obligations under the contract. It is agreed that the coverage as stated shall not be canceled or changed until thirty (30) days after written notice of such termination or alteration has been sent by registered mail to GUC's Procurement Manager

[Balance of page left blank intentionally]

Letter of Compliance to E-Verify for Greenville Utilities Commission

1. I have submitted a bid for contract or desire to enter into a contract with the Greenville Utilities Commission
2. As part of my duties and responsibilities pursuant to said bid and/or contract, I affirm that I am aware of and in compliance with the requirements of E-Verify, Article 2 of Chapter 64 of the North Carolina General Statutes, to include (mark which applies):

   ☐ After hiring an employee to work in the United States I verify the work authorization of said employee through E-Verify and retain the record of the verification of work authorization while the employee is employed and for one year thereafter; or

   ☐ I employ less than twenty-five (25) employees in the State of North Carolina.

3. As part of my duties and responsibilities pursuant to said bid and/or contract, I affirm that to the best of my knowledge and subcontractors employed as a part of this bid and/or contract, are in compliance with the requirements of E-Verify, Article 2 of Chapter 64 of the North Carolina General Statutes, to include (mark which applies):

   ☐ After hiring an employee to work in the United States I verify the work authorization of said employee through E-Verify and retain the record of the verification of work authorization while the employee is employed and for one year thereafter; or

   ☐ I employ less than twenty-five (25) employees in the State of North Carolina.

   Specify subcontractor:
   _____

_____ (Company Name)

By: _____ (Typed Name)

_____ (Authorized Signatory)

_____ (Title)

_____ (Date)

It is certified that this Proposal is made in good faith and without collusion or connection with any other person submitting a proposal on these services. It is also certified that this proposal is made in good faith and without collusion or connection with any GUC employee(s).

Certified check or cash for $ n/a ____ or bid bond for $ n/a _ attached.

Firm Name _____ Phone (____)_____

Address _____

City _____ State_____ Zip Code_____

Fax (_____) _____ E-Mail _____

Authorized Official_____ Title_____
Typed Name

_____ Date _____
Signature

Your proposal should be received no later than DECEMBER 19, 2023 at 3:00 pm (EST).

Exhibit A

Additional information for Vendors

The first goal of this pen test is to determine if an outsider can penetrate our network firewalls. For this external portion of the project, we will provide you with our external IP range that has a total of 38 IP addresses. You will then conduct reconnaissance and OSINT for up to 10 hours and then provide a preliminary report of findings for GUC to review.

Next, we will assume you have been able to gain access to our network and want to know if you can move laterally and escalate within our network. We will provide you with a generic AD user account with general user privileges for you to use to attempt to exploit and gain access to workstations, servers or systems in a non-obtrusive and non-destructive manner. Our goal is for you to find and identify weaknesses in our environment that would allow gaining root access, access to PII or other high value documents, etc. If you wish to provide a VM or appliance that has needed tools for doing such reconnaissance, we will install it and provide you with secure remote access to it for this phase of the project.

Finally, from that same foothold in our network, you are to attempt to access our SCADA production networks with the goal of finding any weaknesses in the internal firewalls that separate the general network from our SCADA networks. Further, we will provide you with the IP address of 1 device (workstation, switch, or server) in each of the 4 SCADA networks for you to scan and try to gain control of. Since you will be in a SCADA production environment, you are NOT to do a general scan of the network or attempt any action on any other device except the 1 device of the IP address provided. Access to the PLC networks is not in scope for this project.

Budget, Timeline, Access, and Scope

The budget for this project is $45,000.00. We expect engagements like this to be priced on a fixed fee approach, not hourly rates. GUC prefers an all-remote engagement to reduce costs, and all remote workers and scans should originate from sites in the USA. If a vendor prefers to have some portion of the work to take place on site, travel costs should be included in the total cost of the project. All systems in scope can be reached from a central network point.

This project does not have a mandatory start date, but it must be concluded prior to the end of the fiscal year on June 30, 2024. Consequently, all work must be completed and invoiced by June 15, 2024. Payment will be made prior to June 30, 2024.

GUC will provide the external IP address ranges for conducting the external penetration test. Further, GUC will provide the selected vendor with a generic AD user account with general user privileges for you to use to attempt to exploit and gain access to workstations, servers or systems in a non-obtrusive and non-destructive manner.

We expect to negotiate a formal Statement of Work (SOW) with the selected vendor and rules of engagement will be detailed at that time, including the requirement of no impact

on production systems. Any work that has any potential of negative impact should be performed from 6 a.m. to 6 p.m. Monday-Friday, Eastern Standard Time. Also note that all scans should originate from sites in the USA, as most other countries are blocked. Any further details will be specified in the SOW negotiated with the selected vendor.

The following items are NOT in scope for this project:

1. Review of standards, policies, and procedures.
2. Phishing or social engineering
3. PLC's, valves and sensors in the SCADA networks
4. Any exploit that might be disruptive to our production networks

SCADA systems testing

For our SCADA networks, the first goal is to determine if the vendor can gain remote access into a SCADA network. Second, we will provide the IP address of a single device in each SCADA network, and the vendor should determine if that device can be compromised. PLC's, valves and sensors are not in scope.

Application Testing

One on-premise enterprise application will be in scope for application penetration testing, with details to be provided in the SOW to be negotiated with the selected vendor.

Miscellaneous

- GUC is responsible for the management and administration of our SCADA and corporate networks.
- Reporting on the SCADA networks should be a subsection in the single report for GUC, not broken out into separate reports. Specific findings per network or device should be delineated within the single report.