# Request For Proposal

**by the**

## Village of Hoffman Estates

**for services related to**

# Cybersecurity Assessment

Proposal Release Date: May 28, 2024

Proposal Due Date: July 5, 2024

## 1. Intent

The Village of Hoffman Estates is conducting this request for proposals to evaluate options for consultation services from qualified, non-product affiliated cybersecurity consulting firms to conduct a comprehensive cybersecurity assessment. The response to this RFP should include a vendor's best proposal to provide the services described within this document.

## 2. Village Contacts

Vendors may contact the Village of Hoffman Estates for questions related to this RFP. Telephone calls are permitted, however are not preferred. Verbal communications are not binding and should not be relied upon until confirmed in writing.

- Darek Raszka, IT Director
  - PH: (847) 781-4875
  - E: darek.raszka@vohe.org
- Jon Pape, Assistant Village Manager
  - PH: (847) 781-2609
  - E: jon.pape@vohe.org

## 3. Schedule

The Village anticipates the following schedule, which is subject to change.

| **Dates** | **Activity** |
|---|---|
| **May 28, 2024** | **RFP Released** |
| **June 14, 2024** | Vendor Questions Due |
| **June 21, 2024** | Response to Vendor Questions Provided |
| **July 5, 2024** | **Vendor Responses Due** |
| **Week of July 15, 2024** | Vendor Interviews, if necessary |
| **July 2024** | Vendor Selection |
| **August-November 2024** | **Anticipated Work Period** |

## 4. Instructions to Vendors

Vendors who intend to respond to this RFP shall indicate as such in writing via email to RFP@vohe.org.

The Village will accept Vendor Questions that seek clarification or additional information regarding this RFP. Vendor Questions must be submitted in writing via email to RFP@vohe.org, no later than June 14, 2024. Written responses to all questions will be furnished to all potential proposers.

Responses to the RFP shall only be submitted electronically. Vendors are solely responsible for ensuring timely receipt of their responses. Proposals received after the response due date may not be considered. Deliver an electronic copy to: RFP@vohe.org

The Village of Hoffman Estates reserves the right to accept or reject any and all proposals, or any part of any proposal, without penalty. The Village of Hoffman Estates may award a contract to a single contractor for all elements of the entire project or may award any of the elements separately. In addition, the Village of Hoffman Estates reserves the right to fund (and proceed with project or purchase), not to fund the project, or to partially fund the project. Any allowance for oversight, omission, error, or mistake by the proposer made after receipt of the proposal will be at the sole discretion of the Village of Hoffman Estates.

## 5. Municipality Description

The Village of Hoffman Estates is a full-service, home rule municipality that strives to continually improve the quality of life of its residents and businesses by delivering responsive and efficient municipal services. With a population approaching 55,000, Hoffman Estates is a mid-size, suburban community. The Village's location provides excellent access to all major attractions within the Chicagoland area and the Midwest. Accommodations to suit all requirements, a variety of top-quality restaurants, good shopping, and many other attractions – both natural and man-made – have resulted in Hoffman Estates becoming one of the premier suburban communities in the state of Illinois. The Village has made major strides in the areas of business and economic development, inter-agency cooperation, and growth management. With an expanding population base in the region, the Village of Hoffman Estates is poised for future growth, both commercially and residentially. The Village also offers good employment prospects, excellent educational amenities, and a modern infrastructure.

## 6. Scope of Work

The Village requires a qualified professional with proven experience in the cybersecurity field to perform a cybersecurity assessment and make specific privacy and security compliance enhancement recommendations.

### 6.a Mandatory Scope of Work

The selected vendor shall perform an in-depth cybersecurity vulnerability assessment that provides security guidance information that is credible and fully aligned with industry standards and best practices such as the U.S. National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (NIST CSF) and the Center for Internet Security Critical Security Controls (CIS), while also considering HIPPA and/or CJIS compliance requirements. The mandatory scope of work includes a cybersecurity vulnerability assessment and penetration testing of the Village's Information infrastructure including:

i. External Network – all external public-facing systems and network flow control from external to internal/demilitarized (DMZ) zones.

ii. Internal Network – all internal systems including, but not limited to, servers, workstations, mobile units, switching/routing devices, storage and virtualization infrastructure, dedicated function appliances.

iii. Assess VoIP network system components for security vulnerabilities, validating system-specific configurations and reviewing for known exploits.

iv. Office 365 – Review of security and best practices of the Office 365 environment including all applications.

v. Wireless Network – wireless systems to include access points from all Service Set Identifiers (SSID's) and their encryption levels.

vi. Access Controls – perform an active directory security assessment, including but not limited to, operational processes, privileged accounts and groups, audit levels, policies etc.

vii. Industry standards compliance – evaluate Payment Card Industry (PCI), Health Insurance Portability and Accountability Act (HIPAA) and Criminal Justice Information Services (CJIS) compliance.

viii. Physical Access - review and testing of physical access controls to IT infrastructure.

ix. Remote Access – assess remote access and security to and from Village resources.

x. Internet Access – assess URL/web and email filtering and access restrictions.

xi. Social engineering – perform social engineering efforts to verify the existence and effectiveness of procedural controls to prevent unauthorized access or changes to the Village's IT infrastructure. Tests should not be designed to target a specific individual rather overall culture.

xii. Connections to External Partners – review Village connections and security stance with external partners via wide area networks (WAN), virtual private networks (VPN) and other methods.

xiii. Advanced Persistent Threat (APT) Assessment – perform a holistic assessment and identify weaknesses that could be used in targeted and/or advanced attack. Assess the current environment for indications of an existing breach.

xiv. Backup and Disaster Recovery – examination of current backup infrastructure and retention for security best practices.

xv. Development of a Data Policy, including data loss prevention, data retention review and policy specific to PII and PHI

xvi. Assess the Village's Supervisory Control and Data Acquisition (SCADA) water system for security vulnerabilities and best practices.

Assessment Reporting Deliverables

- Executive Summary – A report developed for a non-technical audience summarizing the scope, approach, findings, recommendations, estimated timeline, and estimated cost to implement the recommendations.
- Technical Review – A comprehensive overview of each item that was tested or assessed. Graphs, tables, and visuals can be used to summarize results.
- Detailed Findings – In depth analysis of all testing and results. Explanation of vulnerabilities to be explained along with detection methods, risks, and recommended remediation.
- Assessment Remediation Plan - A multi-year roadmap consisting of:
    - Item to be improved on/remediated.
    - Recommended action(s) to take to remediate deficiency.
    - Priority level of item to be remediated (low, medium, or high)
    - Pricing estimates (low to high)
    - Estimated time to implement remediation in multi-year road map.
- The report should also include the following:
    - The company name and the names of the testers with their credentials
    - List of all software and tools used in assessment.
    - Detail the duration of the tests performed.
    - All evidence gathered as proof of successful access, compromises, or exploitations.
    - Details of external, internal, and wireless penetration tests
    - Details of any social engineering tests

## 6.b. Optional Item Pricing

The items listed below are considered optional but should also be included in the proposal identified as optional, with timeline and pricing. If any optional items are included in a proposal's base mandatory cybersecurity assessment, identify those items, and ensure an option price is provided.

- Development of a Cybersecurity Incident Response Plan
- Development of a Disaster Recovery Plan

## 7. Information Technology Environment

The below information is intended to provide perspective vendors with a summary of the Village of Hoffman Estates Information Technology environment. Detailed information, including key network information and network topology will be provided to the selected vendor if requested.

| **Equipment Type** | **Approximate Quantity** |
|---|---|
| Desktop PC's | 236 |
| Mobile PC's | 176 |
| Mobile Devices | 294 |
| Virtual Servers | 20 |
| Physical Servers | 16 |
| Storage Arrays | 4 |
| Printers | 55 |
| Network Switches | 75 |
| Firewalls | 13 |
| Wireless Access Points | 41 |
| Wireless SSID's | 7 |
| Public IP Addresses | 80 |

The Village's IT infrastructure is spread across nine main buildings and also includes various equipment in water towers and lift stations. All buildings are connected by combination of single mode/multimode fiber, high speed microwave, cellular and ethernet links. The Village predominantly uses Microsoft Windows Operating Systems and Fortinet switching. The Village has a mix of on-premise and cloud hosted SaaS applications.

## 8. Evaluation Criteria and Selection Process

The Village of Hoffman Estates will evaluate the responses based on multiple criteria and will select the best overall solution to fit its needs. The Village of Hoffman Estates is not obligated to select the lowest price bidder. The Village will evaluate proposals in a fair, consistent, and objective manner. Selection of the vendor shall be based on response to questions or requirements identified in this RFP and possible vendor interviews. The final recommendation will be made by a Village staff RFP review committee for Village Board consideration and approval. The Village staff RFP review committee will consider all RFP responses. The Village reserves the right to reject all proposals and to re-publish a new RFP for the project contemplated herein. All responses will be evaluated in the following areas:

Evaluation Criteria:

- Completeness of Proposal
- Conformance to RFP Requirements
- Qualifications and Experience
- Ability to Meet the Village's Needs
- Client References
- Public Sector Experience
- Cost Proposal
- Finalist Vendor Interviews (if applicable)

## 9. Proposal Format and Requirements

The best RFP responses specifically address the Village of Hoffman Estates' particular requirements and demonstrate a fit between those requirements and the vendor's strengths. Proposals should be prepared simply, providing a straightforward, concise description of the proposer's capabilities to perform the services identified in this RFP. Promotional material is not desired. Emphasis should be on completeness and clarity of content.

The following summarizes the desired Proposal Format.

A. RFP cover letter – a signed letter briefly stating the proposer's understanding of the work to be done in compliance with this RFP, a statement regarding why the firm believes itself to be the best qualified firm to perform the service, and a statement that the proposal is a firm and irrevocable offer for 120 days. The cover letter must be signed by an authorized representative of the firm.

B. Statement as to the Vendor's particular abilities and qualifications to include, but not limited to:
   - i. Brief history of the company
   - ii. Product and service offerings
   - iii. Description of core competencies
   - iv. History of Vendor, including the number of years the Vendor has been in business and quantity of similar work completed.
   - v. Primary corporate location's address
   - vi. The geographical area of operations and professional affiliations
   - vii. Size and composition of the organization
   - viii. Disclosure of all information concerning any suits filed, judgments entered, or claims made against the Vendor during the last five years with respect to services provided by the Vendor or any declaration of default or termination for cause against the Vendor with respect to such services. In addition, state if during the past five years the Vendor has been suspended from entering into any government contract.

C. Provide a detailed work plan describing services performed in the cybersecurity assessment, including estimated timelines.

D. At a minimum, provide samples for the following deliverables for like services at a client similar to the Village. Sensitive customer information may be redacted if necessary.
   - i. Executive Summary
   - ii. Technical Review
   - iii. Assessment Remediation Plan

E. The cost of services to be provided and an explanation of the basis on which fees are determined. All potential services and associated pricing must be disclosed. The cost proposal must include a not-to-exceed amount for mandatory services and a separate not-to-exceed amount for optional services.

F. Resume(s) of staff to be assigned to this project.

G. Minimum of three professional references for similar size municipal projects. Provide contact name, email, and phone number for each reference and a brief description of a similar project.

## 10. Pricing

The vendor shall provide a detailed cost proposal. Pricing shall be good for a minimum of 120 days after submission.

## 11. Conditions

The vendor agrees to the Village's standard terms and conditions attached hereto or shall provide a copy of their general terms and conditions. The vendor shall provide a copy of their SLA terms and conditions.

## Addendum 1

## Response to Vendor Questions

The Village of Hoffman Estates appreciates the interest from all vendors in response to this Request For Proposals. Below you will find a comprehensive list of all questions received by the Village prior to the due date of June 14, 2024. The Village has responded to select questions to the best of its ability, including summarizing duplicative questions. Questions that have not been responded to are those that the Village is unwilling to answer at this time in this format and can be revisited with the selected vendor.

Please note: Section 11 of the RFP titled, "Conditions", states that, "The vendor agrees to the Village's standard terms and conditions attached hereto or shall provide a copy of their general terms and conditions. The vendor shall provide a copy of their SLA terms and conditions." The Village recognizes that no general terms and conditions were attached to the original RFP. The Village welcomes Vendors to submit their terms and conditions, which will be reviewed by the Village's Legal Department.

1. Is there an approximate budget for this project on the core services (excluding the optional services) that you can share?
    a. The Village does not have a predetermined budget for this project but is committed and able to support the needs for these services.
2. Is the Village of Hoffman Estates requiring companies to have a Facility Clearance at the Secret or Top-Secret level?
    a. No. However, the Village will complete background checks and vetting on all personnel working on the project.
3. Will this contract be executed exclusively at the place of performance, in a hybrid format, or through telework?
    a. The Village will work to accommodate remote work as much as possible but anticipates some work will require onsite interactions.
4. Will the Village of Hoffman Estates provide Government Furnished Equipment (GFE) such as laptops, desks, etc., as part of this task?
    a. Yes, as needed.
5. What is the expected Period Performance for this task, or is this an open evaluation from the Vendor's side?
    a. The Village does not have a specific timeline and will work with the selected vendor to accommodate an appropriate work period.
6. Have you performed this scope of work before?
    a. No, the Village has not completed a comprehensive project like this before.
7. Is there an incumbent?
    a. No.
8. Is this multi-year award?
    a. No. However, the Village recognizes the possibility of some work continuing into 2025.
9. Could you please clarify the PCI requirement, whether the requested service is for the vendor to perform an actual PCI assessment or if it is just tracking/verifying compliance activities and controls?
    a. The Village is interested in tracking and recording PCI issues within the Village's procedures and making recommendations for improvements.

10. Will multiple bidders be selected?
    a. The Village anticipates selecting one vendor.
11. If a bidder does not bid on all project components, will the bid be rejected?
    a. Bids will not be rejected based solely on this factor. However, the Village prefers a vendor that can complete all aspects of the scope.
12. Is there a timeline for completion of the overall project?
    a. No, but the Village is interested in accelerating this project for a completion as near term as reasonable.
13. For external pen testing – which approach black, gray, white hat?
    a. The Village will work with the vendor to select the appropriate level of testing recommended that can accommodate Village schedules and interruptions.
14. Is there a current vulnerability management program in production?
    a. Yes. The Village uses an internal vulnerability scanner. The Village expects that the selected vendor will examine our environment and provide recommendations.
15. For internal vulnerability assessment, credentialed or non-credentialed?
    a. The Village is open to both and will follow best practices and take the recommendation of the selected vendor.
16. Is there an ISO or CISO, and/or CTO on staff?
    a. The Village does not have a dedicated staff member for these tasks.
17. Can an org chart be provided?
    a. Yes.
18. Is there accessible documented policies, standards, and operation procedures in place?
    a. Yes, however, the Village seeks recommendations to improve these documents.
19. What type of VOIP system is used?
    a. Cloud-based.
20. How many wireless SSIDs at how many locations needs to be tested?
    a. 6 SSIDs at 8 locations.
21. How many facilities are included in the physical access assessment?
    a. The Village has 8 populated physical locations plus 32 SCADA specific equipment locations.
22. Social engineering is worded very broadly. It notes not to target specific individuals. To price this we need to know more information. E.g. If phishing campaigns are used, how many campaigns and how many people to phish, if vishing is requested, how many individuals to contact?, if smishing is requested, how many individuals to text? If USB drop is requested, how many USBs to provide?
    a. The Village maintains an active phishing test campaign. The Village has approximately 350 employees and welcomes the selected vendor to assess and make recommendations on phishing, vishing, smishing, and USB drops.
23. Are there any managed service providers involved? E.g. outsourced device management, help desk, etc
    a. The Village utilizes an MSP as needed for capacity on project assistance.
24. Is this a new contract? If not, please provide the incumbent details, and previous spending.
    a. Yes, this is a new contract.

25. Request you to kindly wave off the following requirement “Minimum of three professional references for similar size municipal projects.”, and kindly allow us to provide three professional references with similar size project.
    a. The Village prefers vendors who can demonstrate work with similarly sized municipal organization but welcomes vendors to submit the references they feel most applicable to the project.
26. Is there any local preference to award a vendor?
    a. Yes, though the Village is committed to finding the best partner for this project. The Village welcomes and values supporting local vendors.
27. Do you allow offshore staff to work remotely and perform assessment?
    a. No.
28. Any limitations on number of pages for submission of responses on proposal format?
    a. No. The Village prefers responses that are concise and efficient.
29. Is there any limitation on below sample and preferred format (e.g. PPT or PDF) for D. At a minimum, provide samples for the following deliverables for like services at a client similar to the Village. Sensitive customer information may be redacted, if necessary, i. Executive Summary ii. Technical Review iii. Assessment Remediation Plan
    a. The Village prefers proposals to be submitted as a single PDF document.
30. Will there be a pre-bid conference call?
    a. No.
31. Will the contractor(s) use their own laptop or Client issued laptop? Any security requirements to update the contractor's personal laptop?
    a. The Village is able and prefers to supply hardware needed but understands that some vendors may have specialty equipment that needs to be used.
32. Will the contractor(s) save project information on their own laptop or on the Client's repository? Will it be SharePoint? Other?
    a. The Village prefers that project information be stored on the Village’s resources and can make a SharePoint or other available.
33. Does the Client require any specific certifications?
    a. No. However, the Village will rely on the performance of past engagements and will review any certifications if applicable.
34. Are there any issues with subcontracting, if necessary?
    a. The Village prefers that work be completed by the selected vendor. Any proposed subcontracting should be clearly stated in the proposal and will be vetted through the same process.
35. Is a business continuity or disaster recovery plan review in scope?
    a. Yes.
36. Does the Client have preference of a previous vendor to perform the assessment?
    a. No.
37. How many departments/locations are in scope?
    a. The Village has 8 populated physical locations plus 32 SCADA specific equipment locations.
38. Do all departments/locations use the same technology stack?
    a. Yes.
39. Is IT fully centralized or are there departments who manage their own IT infrastructure? If there are departments who manage their own IT infrastructure, please provide a high-level description of the departmental IT infrastructure.

a. IT Is fully centralized and provides services to a full-service municipality.

40. Is any in-house custom software development being performed? If so, please describe the nature of the software development being performed, the languages being developed in (e.g., .NET, PHP), and the business use of the software being developed.
    a. No.
41. Are there any web applications in scope for the penetration testing? If so, how many and do you require any role-based testing?
    a. Yes. One web application would be included in the testing.
42. Can all penetration testing activities occur during business hours, or do you require after hour testing?
    a. The Village anticipates that some testing will be required after regular business hours to minimize interruptions to the organization.
43. Wireless AP. Are all 41 Wireless AP managed from a central service or is each of the 41 Aps individually managed and configured? Is it possible to perform this review remotely, or is physical onsite required?
    a. They are centrally managed.
44. Physical access. Is the intent to perform a physical and environmental access review on sight? This would include data centers, network closets, etc...
    a. Yes.
45. Development of data policy, is the intent to review the data policy or create a detailed data policy? If created, is the intent to develop a data categorization policy, this would be extensive and require meeting with the business offices etc... Not a problem, we have done this, but clarification is important to estimate the level of effort.
    a. The intent is to create a detailed data categorization policy.
46. In the scope, mobile devices are mentioned. What type are they?
    a. Apple products.
47. The RFP lists 20 virtual servers. Are these servers located in a physical location or cloud hosted service, such as Microsoft Azure?
    a. They are not cloud hosted.
48. Social Engineering - does the Village require a certain number of targets, or should we propose our recommend number and type of social engineering attack?
    a. The Village welcomes proposals that recommend the number and type.
49. RFP - vii. Industry standards compliance – evaluate Payment Card Industry (PCI), Health Insurance Portability and Accountability Act (HIPAA) and Criminal Justice Information Services (CJIS) compliance. Question – These are three different compliance standards and require three different evaluations. Is VOHE okay with this being multiple assessments/projects?
    a. Yes.
50. Can all internal network systems be tested from a central location?
    a. The Village can accommodate certain access changes to accommodate the ease of testing.
51. Is there a formal disaster recovery policy in place?
    a. Yes.
52. Although the RFP requires alignment with recognized cybersecurity standards and best practices, the list of mandatory in-scope activities doesn’t include the performance of a full-scale framework-based cybersecurity assessment that would span all cybersecurity policies, procedures, and practices. Is this activity implied, based on the other in-scope items, or is the scope limited to the focus areas listed?

   a. The Village wishes to conduct a full-scale assessment.

53. What level of involvement and support can we expect from Village's Internal staff during the engagement?
    a. The Village's internal IT staff will be involved and available to participate in the assessment throughout.
54. Would you assist in whitelisting IP addresses for phishing campaign should the emails get held in Spam?
    a. Yes.
55. Please confirm the following standards are part of the scope assessment: NIST CSF 2.0, CIS, HITRUST, CJIS, AWIA, and PCI.
    a. Yes.
56. Are you looking for configuration reviews of O365 vs a specific set of standards such as CIS, or are you looking to perform a penetration test on O365 elements such as passwords and some configurations?
    a. Both.
57. Are you full cloud, on-premises, or hybrid environment?
    a. Hybrid.
58. Would an Azure / Entra review be included in the scope?
    a. Yes.
59. Is there a procedure in place to report unauthorized devices attempting to access village resources or would the Firm be drafting a new one?
    a. The Village welcomes the selected vendor to review what the current Village practices are and make recommendations for improvements.
60. Are there currently any email protection tools or mechanisms that can filter common cyber threats?
    a. Yes. The selected vendor is expected to review current practices and make recommendations based on findings.
61. Are access restrictions currently in place for applicable URLs/websites?
    a. Yes. The selected vendor is expected to review current practices and make recommendations based on findings.
62. Does village leadership understand the importance of having an up-to-date Disaster Recovery Plan?
    a. Yes.
63. Is the Microsoft O365 a GCC or Commercial Tenant?
    a. GCC.
64. What Licensing Model are you currently utilizing, i.e. O365 E3 Vs M365 E3?
    a. O365 G1, G3, and G5.
65. What is the total number of licensed Users?
    a. Approximately 450.
66. Provide network topology diagrams which show detail on the stack type and layering
    a. This can be provided to the selected vendor.
67. Do you have an MPLS network? If so, please provide internal and external traffic flow diagram.
    a. No.
68. Do you own all in-scope IPs and assets (including web servers and external IPs)? If not, please provide detail.
    a. Yes.
69. Are all systems in your environment regularly patched and updated?
    a. The Village welcomes the selected vendor to assess current Village practices and make recommendations.

70. Are there mission-critical systems we should be careful about interacting with?
    a. Yes, which can be discussed with the selected vendor.
71. Do users have local administrative rights to their computers?
    a. The Village welcomes the selected vendor to review and scrutinize all configuration aspects and based on findings, make recommendations.
72. Is there an Active Directory Domain or another Identity Management service?
    a. Yes.
73. What is the preferred method of software deployment and patching? Is there an RMM tool in place?
    a. Yes, the Village uses an RMM tool.
74. Is there a possibility for an extension of the due date for this RFP?
    a. No.

## ALL QUESTIONS RECEIVED (in no particular order):

1. Is there an approximate budget for this project on the core services (excluding the optional services) that you can share?
2. Is the Village of Hoffman Estates requiring companies to have a Facility Clearance at the Secret or Top-Secret level?
3. Will this contract be executed exclusively at the place of performance, in a hybrid format, or through telework?
4. Will the Village of Hoffman Estates provide Government Furnished Equipment (GFE) such as laptops, desks, etc., as part of this task?
5. What is the expected Period Performance for this task, or is this an open evaluation from the Vendor's side?
6. What is your budget?
7. Have you performed this scope of work before?
8. Is there an incumbent?
9. Is this multi-year award?
10. Could you please clarify the PCI requirement, whether the requested service is for the vendor to perform an actual PCI assessment or if it is just tracking/verifying compliance activities and controls?
11. Will multiple bidders be selected?
12. If a bidder does not bid on all project components, will the bid be rejected?
13. Is there a timeline for completion of the overall project?
14. For external pen testing – which approach black, gray, white hat?
15. When was the last external pen test?
16. Is there a current vulnerability management program in production?
17. For internal vulnerability assessment, credentialed or non-credentialed?
18. Does the Village perform vulnerability scans internally? If so, how often and using what tools?
19. Is there an ISO or CISO, and/or CTO on staff?
20. Can an org chart be provided?
21. Is there accessible documented policies, standards, and operation procedures in place?
22. Is change control formally implemented?
23. What type of VOIP system is used?
24. What wireless is in place (vendor)?
25. How many wireless SSIDs at how many locations needs to be tested?
26. How many facilities are included in the physical access assessment?
27. Social engineering is worded very broadly. It notes not to target specific individuals. To price this we need to know more information. E.g. If phishing campaigns are used, how many campaigns and how many people to phish, if vishing is requested, how many individuals to contact?, if smishing is requested, how many individuals to text? If USB drop is requested, how many USBs to provide?
28. SCADA – is the network air-gapped from the main network or segmented? How many devices require testing?
29. Is there a SIEM used? If so what and is it managed by a third-party?
30. How is the network monitored?
31. Are there any managed service providers involved? E.g. outsourced device management, help desk, etc

32. Please provide the estimated budget for this contract.
33. Is this a new contract? If not, please provide the incumbent details, and previous spending.
34. Request you to kindly wave off the following requirement “Minimum of three professional references for similar size municipal projects.”, and kindly allow us to provide three professional references with similar size project.
35. Is there any local preference to award a vendor?
36. What' the budget allocated to this RFP?
37. Do vendor staff needs to be onsite for assessment?
38. Do you allow offshore staff to work remotely and perform assessment?
39. If we awarded contract, at the times if proposed staff personnel not available with us, do you allow us to replaced personnel with similar skills and experience?
40. Any limitations on number of pages for submission of responses on proposal format?
41. Is there any limitation on below sample and preferred format (e.g. PPT or PDF) for D. At a minimum, provide samples for the following deliverables for like services at a client similar to the Village. Sensitive customer information may be redacted if necessary i. Executive Summary ii. Technical Review iii. Assessment Remediation Plan
42. We do not have municipal experience; however we do have experience working federal compliance requirements and assessing state governments. Is the municipal specific experience a strong factor?
43. Will there be a pre-bid conference call?
44. What type of VOIP system does the Village use?
45. Is there a local preference? We are (redacted) based, though it appears most if not all items can be performed remotely.
46. Is there an approved budget that you can share?
47. Will the contractor(s) use their own laptop or Client issued laptop? Any security requirements to update the contractor's personal laptop?
48. Will the contractor(s) save project information on their own laptop or on the Client's repository? Will it be SharePoint? Other?
49. In the RFP - Is the Scope different than a Statement of Work? Is there a separate Statement of Work?
50. Does the Client require any specific certifications?
51. How frequently will onsite work occur? Is there any remote work? What does the remote to onsite mix look like?
52. Are on-site meetings and testing are required, or if a primarily remote assessment approach would be acceptable?
53. Are there any issues with subcontracting, if necessary?
54. Is a business continuity or disaster recovery plan review in scope?
55. Does the Client have preference of a previous vendor to perform the assessment?
56. Is the organization currently using compliance software to assist with their documentation and tracking of current security posture?
57. For the compliance software/security assistance question, what is the name of the compliance software in use?
58. How many departments/locations are in scope?
59. Do all departments/locations use the same technology stack?

60. Is IT fully centralized or are there departments who manage their own IT infrastructure? If there are departments who manage their own IT infrastructure, please provide a high-level description of the departmental IT infrastructure.
61. Do all other departments or locations in scope rely on centralized IT? If not, which, or how many, departments have their own IT functions?
62. Is the organization looking for a thorough inspection into policies and technical security configurations settings or more of a simpler policy review?
63. Is any in-house custom software development being performed? If so, please describe the nature of the software development being performed, the languages being developed in (e.g., .NET, PHP), and the business use of the software being developed.
64. Are any IT functions outsourced? (e.g., server administration, helpdesk, data center hosting, security monitoring, etc.)
65. For the outsourced question, are these included in the assessment?
66. Are any other critical IT assets outside of server rooms (e.g., holding location for hard drives to be destroyed, safe used to store backup tapes, co-location data center)? If so, how many and where are they located?
67. Any critical document storage locations (e.g., warehouse for archived paper file storage)? If so, where are these located?
68. Can you provide a list of physical locations where the servers reside?
69. Could you provide the number of cloud-hosted servers and a general description including what services and hosting provider
70. Is there any equipment currently in storage?
71. How many employees have an IT role?
72. What IT sub-teams do you have? ☐ Server admins ☐ Network admins ☐ Desktop support ☐ Application admins ☐ Other
73. Are we including Business Associate Agreements in scope for security assessment?
74. How many Business Associate Agreements are in scope?
75. The intended depth and rigor of the penetration test - whether a passive assessment, moderate active testing, or full-scale evaluation is desired? Is this dependent on the initial assessment?
76. Is AI used for information security management or analysis? If 'yes', is there a written AI policy?
77. Has the Client had a previous security assessment performed?
78. When was the last previous security assessment performed?
79. Penetration Testing - 1) Will the Bidder/Vendor need to have access to all systems? 2) Is there one central log in for all systems or independent log ins?
80. In-scope departments: What happens if during the assessment interviews we find a department(s) tied to overlapping/in-scope department processes and/or security? Do we turn this into Change Management for Scope change?
81. Are there any web applications in scope for the penetration testing? If so, how many and do you require any role based testing?
82. Do you want a black, gray, or white box penetration test approach?
83. Can all penetration testing activities occur during business hours or do you require after hour testing?
84. Is the SCADA environment in scope for any vulnerability scanning or penetration testing? If so, how many systems reside on the SCADA network?
85. Does the Village perform any software development on any systems in scope?

86. What types of social engineering does the Village require; email, phone, physical? For any email or phone social engineering attacks, how many employees should be targeted? How many physical sites are included in any physical social engineering?
87. How many policies and procedures need to be reviewed as part of the assessment? What industry standards are current policies and procedures based on?
88. How many IT and information security personnel are there?
89. Are any outsourced IT vendors used to support any services?
90. How many systems and departments handle payment card information for PCI compliance?
91. How many systems and departments handle protected health information for HIPAA compliance?
92. Do you require all testing and results of the assessment to be completed by a certain date?
93. Has the Village undergone similar testing in the past? If so, will the results of prior work be available to review to assess remediation done?
94. Does the Village have a budget approved for the work?
95. Wireless AP. Are all 41 Wireless AP managed from a central service or is each of the 41 Aps individually managed and configured? Is it possible to perform this review remotely, or is physical onsite required?
96. Physical access. Is the intent to perform a physical and environmental access review on sight? This would include data centers, network closets, etc...
97. Development of data policy, is the intent to review the data policy or create a detailed data policy? If created, is the intent to develop a data categorization policy, this would be extensive and require meeting with the business offices etc... Not a problem, we have done this, but clarification is important to estimate the level of effort.
98. How many personnel will be targeted for social engineering? What type of social engineering tests would you like to see? Phishing, smishing, vishing?
99. For physical access, how many locations are in scope?
100. Are you looking for black, grey or white box penetration testing?
101. How many external and internal IP addresses are in scope for penetration testing?
102. Are there any IoT devices that are in scope?
103. In the scope, mobile devices are mentioned. What type are they?
104. Has a cybersecurity assessment of this type been accomplished before?
105. Who is the incumbent?
106. What has been the previous pricing for these cybersecurity services?
107. The RFP lists 20 virtual servers. Are these servers located in a physical location or cloud hosted service, such as Microsoft Azure?
108. Are assets, both mobile and workstation/server, managed through a Mobile Device Management solution? If yes, which solution?
109. Does the Village have a comprehensive asset inventory that identifies systems/applications and criticality to the overall infrastructure?
110. Has a business impact analysis been performed on systems/applications?
111. Is the Village beholden to any state mandates regarding incident response activities, such as reporting or coordinating with a State SOC?
112. What types of audits and assessments - PCI, HIPAA, CJIS, etc. - has the Village completed in the past 5 years?
113. How many SCADA or OT assets are in scope for the assessment?

114. How many VOIP assets are in scope for the assessment?
115. Social Engineering - does the Village require a certain number of targets, or should we propose our recommend number and type of social engineering attack?
116. Budget - is this assessment budgeted, can you share a rough order of magnitude for the budget?
117. Scope of Assessment - the current description (Mandatory Scope of Work) specifically 6.a.vii, but generally across all sections - how detailed does the Village want/need the assessment to get. The work could be completed at a high level for less than 100 hours whereas a very detailed assessment will be 600+ hours. Could you provide some additional guidance on the level of detail, evidence review, etc., you are seeking?
118. RFP - vii. Industry standards compliance – evaluate Payment Card Industry (PCI), Health Insurance Portability and Accountability Act (HIPAA) and Criminal Justice Information Services (CJIS) compliance. Question – These are three different compliance standards and require three different evaluations. Is VOHE okay with this being multiple assessments/projects?
119. RFP - xiii. Advanced Persistent Threat (APT) Assessment – perform a holistic assessment and identify weaknesses that could be used in targeted and/or advanced attack. Assess the current environment for indications of an existing breach. Question – This is currently not an (redacted) offering. Is VOHE okay with this not being part of the scope that we offer?
120. RFP - xvi. Assess the Village's Supervisory Control and Data Acquisition (SCADA) water system for security vulnerabilities and best practices. Question – This is currently not an (redacted) offering. Is VOHE okay with this not being part of the scope that we offer?
121. Can all internal network systems be tested from a central location?
122. Is there a process for data classification in place?
123. Is there a formal disaster recovery policy in place?
124. Are detailed configuration reviews of workstations in scope? If so, are all workstations running Windows 10/11?
125. Does the Village require a cost proposal separate from the technical proposal?
126. What is the Village's budget for this project?
127. How many locations are in scope for the physical access assessment?
128. Are web applications in scope for testing? If so, how many?
129. Is the wireless network controller-based or access-point-based?
130. Regarding social engineering, in what type of testing is the Village interested (e.g., email phishing, vishing, smishing, tail-gating)? How many targets/physical locations are anticipated for each type of testing?
131. Does the Village have formal HIPAA policies | procedures | forms?
132. Which departments should be included in the HIPAA Privacy Rule Compliance Assessment, and what is the number of locations per department?
133. Is Breach Notification included in the scope?
134. Is the Village's network adequately segmented for PCI?
135. Regarding the SCADA network assessment: Can the entire ICS | SCADA network be tested from a single location? If there are more than one location to be tested, how many sites are there? How far apart are the sites in scope? Are detailed firewall configuration reviews in scope? If so, is a sampling approach acceptable? Are detailed configuration reviews of routers/switches in scope? Are detailed server configuration reviews in scope, and if so, how many unique operating system brands/versions or builds are there? Are security policies and procedures aligned with a best practice framework? If so, which one?
136. Although the RFP requires alignment with recognized cybersecurity standards and best practices, the list of mandatory in-scope activities doesn't include the performance of a full-scale framework-based

cybersecurity assessment that would span all cybersecurity policies, procedures, and practices. Is this activity implied, based on the other in-scope items, or is the scope limited to the focus areas listed?

137. The RFP mentions that the assessment should result in both privacy and cybersecurity compliance enhancement recommendations. In terms of developing privacy recommendations, would it be appropriate to perform a comprehensive privacy assessment or is this limited to privacy findings associated with the data protection components of the cybersecurity assessment?
138. How much of the testing is anticipated to be performed on-site? Would off-site vulnerability and penetration testing be acceptable?
139. How many public facing systems will be included in the penetration test?
140. How many active hosts are on the internal network?
141. How many internal Windows domains will be in scope?
142. Assess VoIP network system components How many systems components will be in scope?
143. Wireless Network How many physical locations will be in scope?
144. How many SSIDs at each physical location will be in scope?
145. Is access controlled exclusively using Active Directory across the environment?
146. How many windows domains will be in scope?
147. Physical Access How many physical locations will be in scope?
148. Will this be an assessment and a penetration test, or just one or the other?
149. Social engineering What types of social engineering tests will be performed? Phishing, Vishing, in-person, pretexting?
150. How many end users will be in scope for each test?
151. Connections to External Partners Does the village rely on cloud-hosted infrastructure or remote monitoring/ operational support to manage their IT environment?
152. Does the village rely on API architecture to communicate with external partners?
153. Advanced Persistent Threat (APT) Assessment Has the village deployed a Managed Detection and Response (MDR) solution that can be used to identify malware?
154. Are there any specific systems or applications that the Village does not want to be tested, or that require special handling?
155. What is your organization's current compliance status, and when was the last assessment conducted?
156. What is the current level of cybersecurity expertise among your staff, and what training have they undergone?
157. How is your security personnel structured, and do you have dedicated teams for different aspects of cybersecurity?
158. Are there any budgetary constraints or resource limitations that we should consider when developing the roadmap?
159. Can you provide a brief summary of the timeline required for the work?
160. Does Village have any preference in terms of aspects of the work being performed onsite versus remotely?
161. Is there a budget that has been allocated for these assessments?
162. Are there any particular tools or software that Village expects us to use during the assessment process?
163. What level of involvement and support can we expect from Village’s Internal staff during the engagement?
164. What type of defensive cybersecurity technologies are currently in place?

165. Are there any requirements for the penetration testers to undergo background checks or other pre-vetting? If so, please provide details.
166. Are any of the IPs in scope hosted on cloud providers like AWS?
167. Are there any 3rd party hosted IPS/ranges included in the scope?
168. Do you have any outsourced IT functions?
169. Can you provide an approximate number of external/public IP address ranges in scope for the testing?
170. How large are the external ranges?
171. What is the population of live devices in these external IP ranges?
172. Are devices hosted in cloud environments? Is it multi-tenant?
173. Are there any IPs we should refrain from scanning?
174. Can a full scope Internal Pentest work be completed remotely or is an on-site presence mandatory?
175. Approximately how many physical locations are in scope for onsite visits?
176. How many data centers do you have? Are any hosted by 3rd party?
177. What is the breakdown of the number of each internally facing device that is in scope?
178. What kind of IoT devices are setup within the environment?
179. Is the entire in scope internal network accessible from one logical connection?
180. Is the network segmented? How many VLANs are there?
181. Are wireless networks covered as a part of this scope? If yes, provide the number of separate facilities/buildings with separate wireless networks.
182. Will you approve conducting wireless pentest remotely using a Pentest Box? If yes, would you be willing to assist with any network connectivity issues while moving the box within its different wireless range?
183. How many access points in scope?
184. How many SSIDs in scope?
185. How many physical locations to test the wireless network? Where are the physical locations/departments?
186. Provide details on the number of email IDs to be targeted for phishing assessments.
187. How many phishing scenarios are in scope?
188. Provide details on the number of locations in scope for physical impersonation or piggybacking assessments.
189. Would you assist in whitelisting IP addresses for phishing campaign should the emails get held in Spam?
190. Are phone calls or pretext assessments in scope?
191. Are testing of applications required for regulatory compliance programs? If yes, please specify the programs.
192. Has the organization conducted a third-party network vulnerability assessment previously? If yes, provide the assessment date.
193. How does your organization manage and evaluate IT vendors and contractors?
194. Are there specific challenges or compliance requirements for vendor management that need to be addressed in our review?
195. Can you walk us through your current disaster recovery plan and its last test scenario? What were the key learnings and identified areas for improvement?
196. How critical is system uptime to your operations, and what are the current recovery time objectives (RTO) and recovery point objectives (RPO)?
197. Could you detail the current configurations of your VoIP systems, including any custom settings or integrations with other IT systems? What VoIP security assessments have been conducted in the past?

198. What level of evaluation do you expect for the industry standards compliance evaluation?
199. Microsoft 365 How many tenants?
200. Are we able to get Global Administration credential?
201. Are we able to utilize 3rd party applications and PowerShell scripts to assist us in log gathering for the reports?
202. Does *"including all applications"* only include M365 applications that have an admin portal? (Meaning this excludes third party applications that may be integrated)
203. Active Directory Security Assessment How many tenants? How many Domain Controllers? How many Users, Groups, Objects?
204. Are we able to utilize 3rd party applications to assist us in assessing the permissions and security controls?
205. APT Is this a tool they would like reviewed such as Microsoft Defender ATP? What environment is Village referring to?
206. Please confirm the following standards are part of the scope assessment: NIST CSF 2.0, CIS, HITRUST, CJIS, AWIA, and PCI.
207. PCI requirement: Is the requested service for the vendor to perform an actual PCI assessment, or is it just tracking/verifying compliance activities and controls?
208. How mature is the cyber program? Are there any documented policies and procedures?
209. Can the Village provide a list of cloud-hosted SaaS applications?
210. Has an assessment of this magnitude been performed in the past?
211. Can the Village provide the number of water utility site locations?
212. Is there a U.S. citizenship requirement?
213. Can any tasks be completed offshore?
214. Does the Village currently have a cybersecurity program in place? How does it rate its cybersecurity maturity?
215. Will the Village allow remote access to the network for tools, or will it provide information from/access to tools currently used within the environment?
216. For social engineering penetration testing, does the Village want phishing and/or impersonation exercises conducted?
217. Does the Village currently utilize phishing capabilities within the environment?
218. Is the wireless network controller-based or access-point based?
219. What SCADA and Historian vendors are in use?
220. Are there any standalone physically remote networks that are not connected through MPLS? If so, are they 3G/4G/5G or Radio or connected through MPLS?
221. Would the offeror like optional pricing for remediation activities?
222. Are you expecting one price or fixed pricing for each scope activity?
223. If a NIST CSF assessment is performed, would it be 1.1 or 2.0?
224. Is the Village able to share the allocated budget for the requested Scope of Work?
225. Does the district utilize additional IT Cloud providers, excluding Microsoft O365 as mentioned in the RFP (i.e., Google Cloud, AWS, etc.) that will be considered in-scope for the assessment?
226. Is the village expecting the SCADA environment to be included within the Internal Penetration Assessment or the Cybersecurity Assessment, or both?
227. Are all internal target systems and network segments accessible from a single location at the Village or will site visits or physically moving our testing device be necessary?

228. Will the internal penetration assessment include physical security awareness testing? If so, please list out the number of locations to be tested.
229. How many externally facing systems (anything with an IP address) will be in scope for testing?
230. How many web services (e.g., HTTP/HTTPS) are externally exposed?
231. How many websites that are externally accessible will be reviewed that require authenticated testing?
232. Will the external penetration assessment include authenticated web application testing? If so, please list out the total number of applications and roles to be tested.
233. Will the external penetration assessment include email and/or phone social (phishing attacks)?
234. As a result of the Cybersecurity Assessment that includes the review industry standard compliance requirements (HIPAA, PCI-DSS, CJIS), are you looking for a gap assessment, attestation of controls, or report on compliance?
235. Is the intent of the Village to award all work to one vendor? Or to award the work to multiple vendors?
236. Do vendors have to bid on all work or can they bid on a portion of the work to be performed?
237. Are you looking for configuration reviews of O365 vs a specific set of standards such as CIS, or are you looking to perform a penetration test on O365 elements such as passwords and some configurations?
238. Are you looking to run gap analysis reports against each of PCI, HIPAA, and CJIS? Or are you looking to run against just one of the frameworks?
239. Are you looking for a review of the VPN configurations or penetration testing against them for “xii. Connections to External Partners”?
240. How many users are in scope for Social Engineering exercises?
241. How many SCADA devices are in scope?
242. For “viii Physical Access“– Are you looking to review configurations on various security equipment, a walkthrough identifying security vulnerabilities, or a physical penetration test where testers are trying to gain unauthorized access?
243. Has the village ever performed the requested testing in the past? If yes, when was the winning bid and what was the total?
244. Is there a planned budget for this project?
245. Will the village provide all questions and answers asked by vendors to all participants in the RFP process?
246. Pen Testing – How many active IPs on the external network will be in scope?
247. Pen Testing – Are there web applications that are expected to be tested during this engagement?
248. Pen Testing – How many active IPs on the internal network are in scope?
249. Pen Testing – How many internal Windows Domains will be in scope?
250. Pen Testing – Which perspective would the internal penetration test be performed from (e.g., authenticated, unauthenticated)?
251. Vulnerability Scanning – How many active VoIP network system components exist on the network?
252. What type of applications are they - custom, third party, etc.
253. Are these enterprise applications within Azure/Entra?
254. Are you full cloud, on-premises, or hybrid environment?
255. Would an Azure / Entra review be included in the scope?
256. Pen Testing – How many physical locations will be tested?
257. Pen Testing – How many SSIDs will be tested?
258. Pen Testing – Are there guest networks or other segmented networks that need to be tested?
259. Pen Testing – How many active directory domains/forests are there?

260. Do you know the number of debit / credit card transactions that you process on an annual basis across all payment channels?
261. What payment channels do you use to process credit / debit card payments e.g., over the phone, online, customer present etc.
262. How many physical locations where card payment processing activity may take place e.g., contact center, offices, any other locations.
263. How have you been reporting compliance to your acquiring bank to date e.g., type of Self-assessment questionnaire or Report on Compliance.
264. Do you outsource any card payment processing activity?
265. Pen Testing – How many physical locations need to be tested?
266. Pen Testing – Will testing be a covert penetration test, assessment of controls or both?
267. Is there a procedure in place to report unauthorized devices attempting to access village resources or would the Firm be drafting a new one?
268. What tools are utilized, if any, to monitor remote access?
269. Are there currently any URL/web protection tools or mechanisms that can filter common cyber threats?
270. Are there currently any email protection tools or mechanisms that can filter common cyber threats?
271. Are access restrictions currently in place for applicable URLs/websites?
272. Pen Testing – How many users will be included in the social engineering exercise?
273. Pen Testing – What types of social engineering tests are required (e.g., Phishing, Vishing)?
274. Are WANs used when connecting and communicating with external partners? If yes, how are they secured?
275. Is a Virtual Private Network (VPN) required when connecting with external partners?
276. Has an Advanced Persistent Threat Assessment previously been conducted by the village? If yes, how recently?
277. Has the village experienced any previous security breaches in the past? If yes, where and how was the breach remediated?
278. In the event of a breach is there a formal or informal process the village follows to deal with the situation (e.g., informing relevant team members, looking to management for guidance)?
279. Is there a current Disaster Recovery Plan in place or will the Firm be drafting a new one?
280. Has the village ever conducted a risk assessment on its security posture? If yes, how recently?
281. Does village leadership understand the importance of having an up-to-date Disaster Recovery Plan?
282. Has the village ever had an occasion to enact the Disaster Recovery Plan? If so, can you provide more information such as the impact to the village and how things were improved by using the plan?
283. Is there currently a formal Data Policy on handling PII and PHI in place or will the Firm be drafting a new one?
284. Are any tools used for Data Loss prevention? If yes, what is currently in use?
285. Is data retention currently implemented for PII and/or PHI? If yes, where is said data stored and long is said data retained for?
286. How often is the data retention policy reviewed and/or updated?
287. Pen Testing – What SCADA systems are in use?
288. Pen Testing – How many SCADA components need to be tested?
289. Pen Testing – Will this be more of a vulnerability assessment or a covert penetration test?
290. The RFP Document mentions there are standard terms and conditions that should be attached but I do not see them. Is there another document for this?

291. Is the Village looking for an evaluation against these standards? “Payment Card Industry (PCI), Health Insurance Portability and Accountability Act (HIPAA) and Criminal Justice Information Services (CJIS) compliance”
292. How many SCADA devices? “Assess the Village’s Supervisory Control and Data Acquisition (SCADA) water system for security vulnerabilities and best practices. “
293. Are all 80 of the public facing IP’s active?
294. Is the Microsoft O365 a GCC or Commercial Tenant?
295. What Licensing Model are you currently utilizing, i.e. O365 E3 Vs M365 E3?
296. What is the total number of licensed Users?
297. How many are unlicensed?
298. Are you Hybrid AD today?
299. Are you Hybrid Exchange today?
300. What kind of vulnerability scanning are you looking for the listed devices?
301. Is there a single leader defined and responsible for cybersecurity within the organization?
302. Is there a single leader defined and responsible for OT (Operational IT) within the organization?
303. What is the number of & roles of the internal employees responsible for IT?
304. What is the number of & roles of the internal employees responsible for Cybersecurity?
305. What is the company and number of resources & roles of the 3rd Party Employees responsible for IT?
306. What is the company and number of resources & roles of the 3rd Party Employees responsible for Cybersecurity?
307. Have prior risk audits been performed? Were they performed by an external party (if so, are the results available for review)?
308. Provide network topology diagrams which show detail on the stack type and layering
309. Do you have an MPLS network? If so, please provide internal and external traffic flow diagram.
310. How do you define and adjust your IT & cybersecurity budgets?
311. Does your organization have an annual cybersecurity budget? If so, is it separate from your operational IT budget?
312. What proprietary information or intellectual property is critical to your business? How is this data currently secured?
313. Do you regularly use any security tools or scripts to assess risks in your organization?
314. Do you own all in-scope IPs and assets (including web servers and external IPs)? If not, please provide detail.
315. Are any assets such as printers or firewalls being audited or managed by a third-party? If so, please provide detail.
316. Are there any in-scope systems which will require additional approval to test?
317. How many third-parties have direct access to your data and/or infrastructure? Please provide a list with brief explanation(s).
318. Do you have an audit process for third-party vendors (if so, please describe the process)?
319. What do users in your organization do when they need IT Operations support?
320. What do users in your organization do when they need IT Security support?
321. What security policies do you have in place (Acceptable Use/Privacy/Change/etc.)?
322. Do you have a Security Awareness Training solution in place? If so, which solution and when does it renew?
323. Do you feel that the users in your organization are well-informed about online risks?

324. Are you aware of any past breaches of your organization's data?
325. Do you have a breach/dark web monitoring system in place? If so, which solution and when does it renew?
326. Do you use a password manager? If so, which solution and when does it renew?
327. What password length and complexity policy is in place and how is it enforced?
328. Are there any account lockout policies in place?
329. How many failed login attempts within what timespan trigger lockout?
330. How long are accounts locked out for?
331. Do you use any Multi-Factor Authentication (MFA) practices (if so, please explain)?
332. Do you have a spam filter? If so, which solution and when does it renew?
333. Which email server solution (not client) do you use?
334. Has your organization ever been adversely affected by phishing attacks?
335. Does your organization send or receive encrypted email (if so, please explain process)?
336. What sort of SaaS solutions are you leveraging at this time (O365/G Suite/Dropbox/etc.)
337. Do you have a backup solution in place for SaaS systems?
338. What are you currently using as a BDR solution? Which solution and when does it renew?
339. Does the BDR solution have offsite replicas?
340. Are your backups password-protected and/or encrypted?
341. Do you have a backup and restore testing procedure which you have performed recently?
342. Do you have a DLP solution in place? If so, which solution and when does it renew?
343. Do you have any strategy or product in place to prevent sensitive data loss (DLP)?
344. Has your organization classified data into groups according to sensitivity?
345. Do you have antivirus/antimalware solutions in place? If so, which solutions (please provide details on type/versions) and when do they renew?
346. Do you have issues with current antivirus solutions (coverage/visibility/reporting)?
347. Who handles antivirus detection incidents for you?
348. What capabilities do you use with your current antivirus solution(s)?
349. Do you have a Persistence/Threat Hunting solution in place? If so, which solution and when does it renew?
350. Do users or third-parties remotely access internal resources (if so, please explain method)?
351. Does your environment contain a DMZ or Reverse Proxy (if so, please explain)?
352. Does your local environment contain any publicly-accessible systems (if so, please explain)?
353. Quantify the bandwidth at each site between switches & firewall (gbps)
354. Identify the cable types at each site between switches & firewall (e.g. Fiber, Twinax)
355. List servers including physical site location, make & models
356. List firewalls including physical site location, make & models
357. List WAPs including physical site location, make & models
358. List switches including physical site location, make & models
359. Do you have any endpoint DNS protection solutions deployed? If so, which solution and when does it renew?
360. Do you have any DNS content filtering solutions in place? If so, which solution and when does it renew?
361. Do you currently have any issues or concerns regarding DNS in your environment?
362. Do you have a vulnerability scanning and/or management solution in place? If so, which solution and when does it renew?

363. Are all systems in your environment regularly patched and updated?
364. In the event you were audited by a 3rd party, would you have the ability to provide documentation of all applications and patch levels (both OS and Apps)?
365. Are you running any software which is unsupported or end of life? If so, which software and what is it's function?
366. Do you have a development environment for all internally developed applications?
367. Are there mission-critical systems we should be careful about interacting with?
368. Do you have a NDR (packet capture/analysis) solution in place? If so, which solution and when does it renew?
369. Do you have a SIEM (log monitoring/analysis) solution in place? If so, which solution and when does it renew?
370. Do you have an existing syslog server or event log monitor (if so, please explain)?
371. Do you have an account review policy to confirm user permissions (if so, please explain)?
372. Do users have local administrative rights to their computers?
373. Do you have any systems in place which back up website/WebApp files and databases?
374. Are there architecture/network/data documents we can review for all in-scope WebApps?
375. Is it possible for us to get a walkthrough of each in-scope WebApp?
376. How often are WebApp backups performed and how often are they verified and tested?
377. How often are webservers you manage scanned for malicious content?
378. Are webservers which host your in-scope WebApps dedicated or shared?
379. Are all in-scope WebApps locally hosted?
380. Are there any requirements we need to follow for testing externally-hosted WebApps?
381. Do in-scope WebApps have Test/Dev/Staging/QA environments into addition to Production?
382. Are we authorized to scan all in-scope WebApp components (server/application/API/DB)?
383. Are there any users that would be impacted by in-scope WebApp testing?
384. Are there any times which are best to avoid in relation to in-scope WebApp testing?
385. Will you provide us with logins for all in-scope WebApps?
386. Can we audit in-scope WebApps using both standard and admin credentials?
387. Are databases used for in-scope WebApps shared with other systems or applications?
388. Do any regulatory, state, or industry requirements or standards apply to in-scope WebApps?
389. Have in-scope WebApps been tested before?
390. Do you have Web Application Firewalls protecting all websites and WebApps you manage? If so, which solution and when does it renew?
391. Can you provide us with a full list of all websites/WebApps/domains/subdomains you own?
392. What public WebApps (including WAN IPs/URLs/descriptions) do you use?
393. Who will be the main contact(s) for compliance-specific interviews?
394. Who will be the main contact for the onsite walkthrough/visit?
395. Who should we send a secure folder link to for policy/procedure upload?
396. Do you have drive encryption enabled on all devices within the organization?
397. Have you had a compliance audit/gap analysis in the past (if so, when)?
398. Were there any significant findings resulting from prior compliance audits?
399. Do you feel that top compliance risks have been properly identified/addressed (if so, how)?
400. Who is in charge of compliance in your organization?
401. Are you familiar with key compliance policies and procedure for transactions and activities?

402. Do you have adequate compliance resources (personnel/budget/training/expertise/etc.)?
403. Is there compliance messaging (posters/email notifications/etc.) available in your office/location?
404. How does the organization communicate its compliance program values/initiatives/requirements?
405. Is job-specific compliance training provided to all users in the organization (if so, when and how)?
406. Is there a well-defined process for reporting compliance issues and is it effective?
407. Is senior management notified about compliance issues (if so, how frequently)?
408. Do you have Business Associate Agreements with all vendors who have access to sensitive data?
409. What is the desired start date of this assessment/audit?
410. What is driving the need for this assessment/audit?
411. Does the organization have Cyber Insurance? If so, who is the provider and when does it renew?
412. Who are the main stakeholders related to IT & cybersecurity decisions and managing those partnerships?
413. Describe the process and timeline of onboarding a new vendor/partner
414. Is the organization trying to align with ITIL, MITRE ATT&K?
415. Are there compliance requirements or goals to align to the type of compliances (HIPPA, CMMC, ISO, etc.) for the organization?
416. What do you view as the largest risks and threats to your organization?
417. What functions and/or processes are critical to the day-to-day operations of the organization?
418. Is there a feeling that the users in the organization are security-conscious?
419. What would a 24-hour outage cost the organization (revenue loss, employees wagers/productivity, etc.)?
420. Is there an Active Directory Domain or another Identity Management service?
421. What is the preferred method of software deployment and patching?  Is there an RMM tool in place?
422. How does the organization manage software and operating system licensing (M365, AV, server OS, etc.)? Do they carry inventory?
423. Does the organization utilize a ticketing system?
424. Dedicated Full Time Operational IT Staff?
425. Dedicated Full Time Cybersecurity Staff?
426. Dedicated Full Time Application Development Staff?
427. Physical Site Locations? (If multiple sites, gather information on connectivity between them)
428. Users? (delineate knowledge workers vs. total employees)
429. Mailboxes?
430. Workstations? (delineate PC vs. MAC counts)
431. Phones? (delineate Cell vs. Desk)
432. How many servers in the cloud, how many of the physical servers are on-premise at the Village? Is there a hypervisor? If so, VMWare or Hyper-V?
433. Additional connected IoT Devices? (what is in the watertowers, etc and what are the types of all the devices)
434. Total Internal IP Addresses? (servers/workstations/printers/phones/IoT devices/etc.):
435. Total Web Apps?
436. Are there in-house or external compliance experts to address compliance needs?
437. What system(s) are currently being used to manage compliance requirements?
438. Organization Shipping Address:
439. Full CIDR notation for all in-scope LAN IP ranges
440. Full URLs for all in-scope WebApps
441. Are there any internal devices/IPs/subnets/WebApps which should not be in scope? Why?

442. Describe how the scoping interview data was collected and your perceived level of accuracy:
443. Would you please share any questions/ answers from other vendors?
444. Is there a current budget allotment for this project and if so, what is it?
445. Is there a possibility for an extension of the due date for this RFP?
446. How many of the 80 IPs have open ports facing the internet?
447. How many networks does the village have?
448. How frequently do you want the external penetration tests done? Monthly? Quarterly? Semi-annually? Annually?
449. How frequently do you want the Vulnerability Assessment done? Continuously (i.e. weekly – to stay on top of things at all times)? 1 time only?
450. PCI, HIPAA, CJIS - are they looking for formal audit/attestation of compliance, or are they comfortable with an assessment that does not provide attestation of compliance?