PROVIDENCE HOUSING AUTHORITY
FACILITIES MANAGEMENT DEPARTMENT
40 LAUREL HILL AVENUE
PROVIDENCE, RI 02909

EQUAL HOUSING OPPORTUNITY

ADDENDUM NO. 01

PROJECT:	RFP TO PROVIDE CYBER SECURITY SERVICES
OWNER:	PROVIDENCE HOUSING AUTHORITY 100 BROAD STREET PROVIDENCE, RI 02909
DATE:	FEBRUARY 14, 2023

TO ALL BIDDERS OF RECORD:

A. This Addendum forms a part of the Contract Documents.

B. This Addendum includes answers to the questions received from vendors.

C. Network Diagram

Questions and Answers

1. **Does all traffic flow through the data center?**
   All data is stored at the two data centers and the remote locations connect to the data centers.

2. **Are all the amps communicating with the data center. Is the water (ISP) coming into the data center and feeding each amp through a spigot (Bridgewave)?**
   AMP's 001, 003, 004, 005, 007 and 009 use a Bridgewave to connect and communicate to the data centers – Verizon is backup at these locations.

   AMP's 002 (two Verizon connections – CC and RW), 006 and 007 use Verizon to connect and communicate to the data centers – Cox is backup at these locations.

3. **What are the points of egress and ingress so we know where we need to land NID?**
   Verizon is a primary network connection at 4 AMP's and backup at 6 AMP's, Cox has a connection at one AMP and backup at 4 AMP's.

4. **Is everything hosted in the data center?**
   Yes.

5. **Is AMP007 Primary the Bridgewave or the Verizon wireless?**
   Bridgewave is primary and Verizon the backup.

6. **The Verizon primary accounts, do they have their own firewalls?**
   Each AMP has a Fortinet firewall.

7. **Do all Bridgewave AMPs have their own firewalls or is there just 1 in the data center to support that entire wireless network?**
   Each AMP has a Fortinet firewall.

8. **How many people are on the IT team? Is there a dedicated cybersecurity team?**
   3 and no dedicated cybersecurity team.

9. **How many firewalls are in scope?**
   Ten

10. **Could PHA please clarify the scope of the application and cloud readiness assessment?**
    Simply assist with yearly reviews as needed to see what is on premise, and can it go to cloud, and what is in cloud already and is it protected, backed up.

11. **How many web and enterprise applications are in scope?**
    None

12. **Please clarify the two following bullet points under the scope of services.**
    - **Monthly social engineering & security awareness testing**
    - **Quarterly social engineering & security awareness training**

    Security awareness training, can be lunch learn, do some phishing, calls into staff, USB drop or other ways to test users besides web delivered training.

13. **How many targets are in scope for testing for each?**
    167.

14. **Does PHA currently use SentinelOne for endpoint protection?**
    No (Sophos XDR) expires 4/15/2024.

15. **Are there existing firewalls in each AMP? I'd like to understand better whether or not I'd have to supply firewalls or if they currently exist. If so, what are they? We use a span port from the firewall to feed our XDR system. We need to know what we're looking at.**
    There are firewalls installed at each AMP; AMP 003 and 005 have a Fortinet Fortigate 100F installed and the remaining AMP's have Fortinet Fortigate 60F installed.

16. **Do all computers currently have Anti-Virus running? If so, which one? Anti-Ransomware?**
    Yes, computers have Sophos installed.

    Products

Core Agent	2022.4.1.1
Sophos Intercept X	2022.1.3.3

17. **How many servers exist in the environment, and which operating systems?**
    No physical servers, we have the VM's listed on page 6 of the RFP.

18. **Which of the following services are you interested in? (select all that apply)**
    a. SIEM (Security Incident and Event Management)
       Yes, especially for cloud 365, domain controllers and firewalls at min
    b. VMS (Vulnerability Management System)
       Yes (but don't need some enterprise expensive system, ideally a web based such as intruder.io for example)
    c. EDR (Endpoint Detection and Response)
       When Sophos expires. replace with theirs PHA decision

19. **Do you have an incident response plan?**
    Currently no, working on creating one – will need assistance

20. **Do you have an Endpoint Detection and Response (EDR) tool? If so, which product are you using?**
    Sophos.

21. **Is the EDR tool deployed to 100% of your environment?**
    Yes X No ☐

22. **What cloud environments do you currently utilize? (select all that apply)**
    - Amazon Web Services ☐
    - Microsoft Azure ☐
    - Google Cloud Platform ☐
    - Other (please specify): M365

23. **Please provide an estimated total number of EPS (Event Per Second) or GB/day of logs generated (if known).**
    Not known, don't want a SIEM or log management that charges per GB that old, Splunk like and gets expensive. Newer pricing models are based on devices, or some flat fee per month.

24. **What is your preferred delivery model for the SIEM?**
    - Consumption/as-a-Service *__preferred__
    - Own the SIEM platform

25. **With a question deadline of 02/13, there is a short time for PHA to provide answers and for offerors to apply them before shipping their responses. Would PHA consider extending the due date?**
    Not currently.

26. **Would PHA accept Managed Detection and Response, and Endpoint Detection and Response services delivered from Canada?**
    As stated in the RFP, page 11 – Offeror offices must reside withing the United States

External Network Vulnerability Assessment / Penetration Testing

- **Confirm total number of public facing / external network IP addresses to be tested (If providing an IP range, please indicate the estimated number of live IPs).**
  19 – Cox 9 and Verizon 10.
- **Are the external systems hosted by a third-party provider?**
  Yes
- **Does your organization own and manage the network equipment at your external perimeter?**
  We own the Bridgewave and Fortinet's, not Verizon or Cox equipment.
- **Are 3rd Parties required to comply with or be aware of and agreeable to the Penetration Testing?**
  No
- **Number of Web based applications/ services to test (dynamic pieces of websites that users or other application authenticate to – client portal, sales quote system).**
  None
- **VPN, Terminal Services, Remote Desktop, FTP, and other remote services to be tested?**
  Select staff uses GoToMyPc to connect to their pc from outside the agency.
- **Is an objective of this test to also assess the Company's intrusion detection capabilities?**
  If perform routine monthly quarterly scans for Pen and Vuln, then a quick scan should suffice and every 12-16 months** run a full scenario to break in. if MSSP feels after first one or two that can extend time between, that is fine and should be discussed internally for risk, liability.
- **How deep should testing go in the event of successful network penetration (i.e. just validation of vulnerability; network administrator access; server access, etc.)?**
  For the monthly quarterly scans, vuln level. For the larger 12-16 month.

Internal Network Vulnerability Assessment / Penetration Testing

- **Confirm total number of internal network IP addresses to be tested (If providing an IP range, please indicate the estimated number of live IPs).**
  20 subnets (HVAC and Data)
- **How deep should testing go in the event of successful network penetration (i.e., just validation of vulnerability; network administrator access; server access, etc.)?**
  Vulnerability for basic scans, and similar to External, might want to go all the way every few years.
- **Are internal web-based applications / services in scope, if so, please provide an indication as to the anticipated number of web-based applications/services that may need to be assessed.**
  None (if all is in m365 azure AD etc., then there are just camera NVR, maybe server or two running HVAC, Access Control and HAB)
- **Is it desired to evaluate the strength of mobility environments (iPhones, BlackBerry, home VPN access)?**
  Not currently
- **Are corporate build / configuration standards in place for various platforms (network devices, operating systems, etc.) and if so, is it desirable to evaluate against those standards, etc. This will determine the amount of time required to perform additional analysis and tuning of evaluation criteria.**
  Yes, our Firewalls. (also could use CIS control suite for hardened win10,11 and other devices, I think it might be free for you guys, but also all Win OS will run local firewall)

- **Can remote internal networks be scanned via a primary location, or would it be necessary to perform field visits to each in-scope location?**
  Can be scanned via a primary location.

- **Are any of the internal applications a third-party provider?**
  Our Authority Wide housing, Camera and HVAC software are third-party software.

Wireless Security Assessment

- **Will Wi-Fi testing be conducted at each location? If so, how many SSIDs and which locations?**
  No, Wi-Fi devices are not connected to the network. (just weigh risk if something happens what could be the outcomes, I recall these are all local to a small group of computers with no access to anything on main networks. Might want to have them checked once, but maybe down road to save some cost

- **Please provide an estimate of the types of Wireless in use (microwave, 802.11x, proprietary, cell phone, blackberry, iPhone, Bluetooth, Point-to-Point, etc.).**
  Wireless Antenna's - refer to page 5 of the RFP.
  T-Mobile tablets = 14
  Verizon tablets = 24

- **Are formal wireless security policies in place?**
  MFA is setup when vendor's connect to our network.

Mobile

- **What Mobile Platforms are in scope?**
  None currently

- **How are Mobile devices being used for, e.g. email, two-way comms, application interfaces, GPS, mobile applications?**
  PHA and personal cell phones are used for email, we have Verizon and T-Mobile iPad's and Tablets used for our Mobile Work Order and Mobile Inspections.

External War Dialing Exercise with Modem Penetration Test

- **Please provide an estimate of the number of telephone numbers that are in scope.**
  None, our phone system is not connected to the network and not part of this project.

- **Please provide an indication of acceptable dialing times or special requirements around when it is acceptable to dial phone numbers (e.g., are business hours off limits?).**
  Not included in this project

- **Is dictionary-based password guessing an acceptable procedure for identified modems and voice mail boxes?**
  Not included in this project

- **Please provide an estimate of the number of modems.**
  Not included in this project

Facility Breach

- **Number of Facilities in scope?**
  We have 10 locations; the 5 Family sites have multiple buildings, and the 5 Elderly buildings have one building.

- **To what level should the unauthorized access be demonstrated? (access to paper files, office areas, network access, obtaining equipment, etc.)?**
  Currently only network access.

Remote Social Engineering

Types of Social Engineering approaches:

- **Impersonation: If there is a person within the company you would like us to impersonate in order to gain access to information, please indicate who this should be. Otherwise, we will decide based on factors including tenure, position, and possible influence.**
  Yes, will can discuss when project awarded.
- **Important User: We may make references to known associates or important users in order to influence someone's decision to provide us with information on their behalf. Please indicate who this 'important user' should be. Otherwise, we will decide based on factors including tenure, position, and possible influence.**
- Yes, will can discuss when project awarded.
- **Third-party Authorization: We may make claims that permission has already been granted by another associate for information.**
  Yes.
- **SPAM: Do you wish for us to generate false advertisements in hopes of detecting users who decide to click on ads and hyperlinks?**
  Yes.
- **Spear Phishing: Through the process of sending an e-mail to users and falsely claiming to be a legitimate enterprise, we can potentially coerce a user into disclosing private information. Please indicate if this is a required assessment.**
  Yes.
- **Will USB drops be included as part of the exercise? If so, how many USB would you like to deploy and how many locations?**
  Yes, 3 USB that can be move to different locations.
- **Will Physical Facility Breach be included as part of the exercise? If so, how many locations will be in scope?**
  No.
- **Can employees log into webmail remotely? If so, what is the webmail URL?**
  We use M365.
- **Is email hosted internally? If not, who hosts the email services?**
  We use M365.

Firewall Rule Set Reviews

- **Please provide the number of in scope firewalls to be reviewed.**
  10.
- **Are there Company firewall policies / standards in place that the assessment will test against for compliance, in addition to best practices?**
  There isn't anything specific in place, it's more of a written policy than the firewall configuration.
- **Please provide firewall make and model for in-scope devices.**
  2 Fortinet Fortigate 100F and 8 Fortinet Fortigate 60F.

VoIP Security Assessment

- **Please provide an indication as to the number of centralized management consoles for VoIP systems.**

Three IT staff log into the Cox website to manage our phone system, our VOIP is not part of this project.

- **Please provide an indication as to the degree of separateness the VoIP network has from the data network or are they two converged?**
  VOIP is not connected to the business network and not included in this project.
- **To what degree of security is the VoIP assessment desired? For example, if it can be shown that the testing team is capable of intercepting voice mails or eavesdropping on phone calls, would that be of value?**
  Please list as a separate line item and cost.
- **Are soft VoIP phones in use?**
  Yes, 9 of our Leased Housing staff is using Cox WebEx
- **Is it desired to identify abuses of the VoIP system (fraudulent calls, excessive long distance, etc.)?**
  No
- **Is voicemail box penetration testing an acceptable procedure?**
  Not, currently

DMZ Architecture Review

- **Number of systems and devices in the DMZ architecture to be reviewed**
  None.
- **Are updated network diagrams available?**
  Yes
- **How recent is the DMZ architecture documentation (diagrams, etc.)**
  We've been using the network diagram
- **Would it be necessary to verify physical connections in data centers or other locations, if so, please provide estimate of the number of physical locations to visit to identify potentially unauthorized physical links that may bypass firewall protections (e.g., dual homed hosts).**
  Not currently

Cloud Services Administration Review

- **What services are provided by a cloud provider (AWS, Google, Microsoft, etc.)**
  M365.
- **Do you manage your cloud services yourself? If so, which functions are performed in-house versus by the cloud provider?**
  Administration only for M365
- **Do you have an architecture diagram of you cloud environment(s)? If yes, can you provide?**
  Not have currently

SCADA Security Assessment

- **Are there specific security standards the Village would like this SCADA assessment to align with?**
  Not using SCADA
- **Is the SCADA environment formally documented?**
- **Has there been previous SCADA assessment preformed?**

- **Is the SCADA review just observational (interviews/document reviews) or include scanning us a vulnerability assessment tool on the network?**
- **Total number of SCADA endpoints?**
- **Is the entire SCADA network accessible from a single location?**
    - **If not, how many locations will need to visited?**
- **How many Villages SCADA subject matter experts will need to be interviewed?**

Database Security Review

- **How many databases are in scope for this review?**
  None.

- **What type of database systems are in scope?**
  None

Backup Security Review

- **How many backup systems are in scope for this review?**
  None currently

- **What type of backup systems are in scope?**
  None currently

Type of Security Monitoring Service(s); what is the client's expectation / requirement of the service.

1. **Monitoring Triage & Notification**
   24 x 7 | off-hours | hybrid | custom monitoring coverage
   24X7 365 Network monitoring, management and resolve all cyber security incidents authority wide

2. **Log Collection & Storage (some level of collection/storage will be required to support Analysis and Response)**
   Firewalls, End point security, 365 to start. (when fully mature might collect from each workstation and server and switch.)

3. **Vulnerability Identification (Scanning)**
   Monthly external scan

4. **Intrusion Detection**
   Network / Host
   Firewall might be enabled already, host if built into EDR,

5. **Asset Identification**
   Not at this time

6. **Compliance Reporting**
   Not at this time

7. **Endpoint Detection & Response (workstations)**
   Currently have Sophos xdr, put date when subscription ends and if want vendor to provide service provide QTY

8. **Cloud Services Monitoring**
   365, any other cloud services

9. **Server & Services Availability Monitoring & Alerts**
   I would list current setup and that planning to move to azure service and keep x,y,z onsite

10. **Security Response and Remediation Support**
    You want them to own this and provide updates and communicate to you if need onsite assistance.

Number of Hosts to be Monitored

1. **Number of Firewalls and each make/model?**
   2 Fortinet Fortigate 100F and 8 Fortinet Fortigate 60F

2. **Any Web Application Firewalls?**
   No

3. **DNS Server (Microsoft, BIND, etc.)?**
   Yes, 1

4. **Any Netflow capabilities?**
   No

5. **Number of Infrastructure devices (routers, switches, etc…) and each make/model?**
   1 - Adtran 1224ST
   5 - Adtran 1234 PoE
   1 - Adtran 1238P
   1 - Adtran 1531
   48 - Adtran 1531P

2 - Adtran 1534
2 - Adtran 1534G2
3 - Adtran 1534PG2.1
1 - Adtran 1544
7 - Adtran 1550
5 - D-Link DGS-1216T
2 - D-Link DGS-3612G
3 - HP 2520-8-PoE
32 - NetVanta 1560-08-150W
1 - NetVanta 1560-24-370W
3 - NetVanta 1560-24-740W
3 - NetVanta 1560-48-370W
4 - NetVanta 1560-48-370W

6. **Number of Servers and each make/model/OS?**
   No physical servers, our VM's run on a VxRail with Windows Server 2016 and 1 VM running 2012

Product Version:	4.7.515-26640584
VxRail Manager Version:	4.7.515-16804010
vCenter Version:	6.7.0 build-16709110

7. **Number of Active Directory or Ldap Servers?**
   2 Active Directory servers

8. **Number of and any specific files, if file integrity monitoring is an objective**
   None

9. **Number of endpoints (workstations) and each make/model/OS**
   Two Dell laptops connect to our network; Latitude 3500 and Latitude 3520
   All 167 computers are Dell except the Mini PC and Misc.
   5250 = 30
   7400 = 44
   5260 = 7
   7470 = 9
   7450 = 23
   3240 – 11
   7440 = 10
   3630 = 3
   90100 = 6
   9020 = 2
   9030 = 2
   7490 = 6
   7780 = 2
   390 = 1
   3650 = 1
   3510 = 1
   Mini PC = 1
   Misc. = 8

10. **Does the Client have a virtual environment that can host the SIEM sensor virtual image?**
    *no should be able to run a small device like mini PC or its own version.

11. **Number of Virtual Services and make and model?**
    Number of VM's Please refer to page 6 of the RFP, Our Virtual Environment run on 2 VxRail's, one at each Data Center

Product Version:	4.7.515-26640584
VxRail Manager Version:	4.7.515-16804010
vCenter Version:	6.7.0 build-16709110

12. **What, if any, cloud environment would be in-scope (AWS, Azure, O365, etc.)?**
    Currently using M365 and within the year most likely Azure Services not VM's
13. **Can you share your network diagrams?**
    If you are the selected vendor for this project
14. **Can you share an asset inventory for in-scope devices by asset type?**
    If you are the selected vendor for this project
15. **How many locations are in-scope for collection and monitoring? Are these locations reachable from a single site; are these sites independent / segmented?**
    All 10 sites, they are accessible form a central location and segmented
16. **How many isolated network segments exist across the network?**
    We have 3 VLAN's (data, camera and HVAC devices)

How many employees/contractors/vendors/interns have access to the network that will be monitored?

All 167 network users and our Network Management, Virtual Environment Management and Authority Wide Software vendors

17. **Do you know your current Events Per Second (EPS) for in-scope networks?**
    No
18. **Do you know your current number of logs to be monitored for in-scope networks?**
    No
19. **What other security controls do you have in place (IDS, EndPoint / EDR, Proxies, etc.)?**
    Sophos XDR, Door Access, MFA, computer time restrictions, required password change every 180 days, password minimum length of 13 and computer locks after 10 minutes of inactivity.
20. **For user data enrichment, we typically connect to either Active Directory or an HR system to add employee name, org, supervisor, etc. to data analysis. Does your AD have additional information, Full Name, Title, Department, Supervisor, Location, etc? Alternatively, is there an HR or other system you would like us to connect with to add that information?**
    Our AD does not have all that information listed above and our HR system is not part of the project.

Internet

1. **Number and location of Internet ingress/egress points**
   Verizon is primary network connection at 4 AMP's and backup at 6 AMP's, Cox is backup at 4 AMP's.
2. **Internet Pipe size at each ingress/egress**
   Verizon Wireless – 2 sites 500 Mbps, 7 sites 300 Mbps and 1 site 150 Mbps
3. **List of remote/branch sites if applicable**
   Chad Brown/Admiral Terrace/Sunset Village - 300 Mbps
   Codding Court – 300 Mbps
   Roger Williams - 150 Mbps
   Hartford Park - 500 Mbps
   Manton Heights - 300 Mbps
   Dexter Manor - 500 Mbps

Dominica Manor - 300 Mbps
Carroll Towers - 300 Mbps
Kilmartin Plaza - 300 Mbps
Parenti Villa - 300 Mbps

Green – 1Gb P2P Wireless
Blue – "Spoke" VPN
Red – "Hub" VPN