Connecticut Lottery Corporation (CLC)

Request for Proposal #CLC202001 – Network Security Penetration Testing

April 22, 2020

Addendum 3

Proposal Submission Due Date Extended

RFP Clarifications

Proposer Questions and CLC Responses

Revision to RFP Schedule:

The Proposal Submission Date is extended a third time to provide prospective Proposers the full fourteen-day period to respond to RFP #CLC202001. This extension is due to the additional time that the CLC needed to provide full and accurate answers to the large volume of Proposer questions received and the current challenges created by the Coronavirus pandemic.

The remaining Schedule, as revised, is as follows:

Proposal Submission Date	*05/07/2020; 2:00 PM Eastern Time Proposals must be submitted by email only to Purchasing Officer Suzanne Colley at Suzanne.Colley@ctlottery.org
CLC Preliminary Notice of Award	06/03/2020

Dates bearing an asterisk (*) are firm dates and times. All other dates are subject to change.

The CLC's Addendum 2 to RFP #CLC202001, dated April 15, 2020, is amended as highlighted in yellow below.

Part IV, Sections A.1 and A.2 and Part C of RFP #CLC202001 concerning Delivery of Submissions, Package Labeling, and Content Requirements are amended as follows:

1. Proposals must be submitted by email only to Suzanne.Colley@ctlottery.org with "Network Security Penetration Testing, RFP #CLC202001, 05/07/2020" in the Subject Line. Proposals must be signed; however, original, ink signed Proposals do not need to be submitted.

2. Proposers must submit an electronic "searchable" PDF/Word version of their full Proposals. If a Proposal contains Proposer Confidential Information, then the Proposer must also provide a PDF copy of its complete Proposal (including pricing) with Proposer Confidential Information redacted and clearly labeled as the "Public Copy."

3. In lieu of numerical section tabs, Proposers must insert title pages that clearly identify the beginning of each section of their Proposals. For example, a page titled "References" should be

inserted to identify the beginning of the References section.

The CLC has suspended all public bid openings until further notice. Proposers responding to RFP #CLC202001 may request the List of Proposers after the scheduled Proposal Submission Date.

All other terms and conditions of RFP #CLC202001 and its Addenda not expressly amended herein shall remain in full force and effect.

RFP Clarifications:

1. REQUIREMENTS AND SPECIFICATIONS

RFP References – Part I.G.8, Page 4; and Part III, Page 6

Due to the continuing and evolving challenges of the Coronavirus pandemic, the CLC will work with the Successful Proposer to schedule the on-site Network Penetration Testing phase of the engagement for a time that works best for both parties and allows for everyone involved to perform the necessary tasks in a safe environment. This is an unprecedented time for all of us, and the CLC will remain fluid in its decision-making as the current environment changes. The Successful Proposer's cooperation and flexibility is paramount and appreciated.

As of the issuance of this Addendum, the CLC expects to perform all three phases of the RFP – Network Penetration Testing, Network Configuration Review, and New IDS/IPS Appliance Installation – but may change the approach and/or order in which these phases are completed to accommodate a safe time to perform on-site portions of the engagement. For example, Network Configuration Review can be performed with video conference calls, network diagrams, and exported configurations of the routers and switches. Based on that information, the Successful Proposer should be able to recommend appropriate IDS/IPS devices for the CLC.

Proposer Questions:

Vendor #1

1. Do you have a budget for this project
   The CLC has set a budget in FY20 for this purchase. However, the CLC is not prepared to disclose this information to Proposers at this stage of the procurement process. Proposers are expected to submit their best pricing to accommodate a response that will fulfill all the obligations of this RFP.

2. Is it an ongoing project? 1 year? 2 year?
   This is a one-time project.

3. Was there an issue that occurred to bring about the RFP?
   No.

Vendor #2

1. In light of the current pandemic, it might become necessary for all of our staff to work from home. To accommodate this, is it possible for bidders to submit proposals via email rather than hard copy?

   Due to the Coronavirus pandemic, the CLC has extended the Proposal Submission Date and will accept Proposals by email in accordance with the "Revision to RFP Schedule" section of this Addendum (page 1). In light of potential difficulties related to electronic submission of documents (i.e. documents in excess of 25MB), the CLC recommends sending a separate email to Purchasing Officer Suzanne Colley at Suzanne.Colley@ctlottery.org or calling her to confirm receipt of a Proposal.

Vendor #3

1. After reviewing, the attached RFP our firm [Company X] has a question. We notice the project work is broken into three sections;
   a. Network Security Penetration Testing
   b. Network Configuration Review
   c. New IDS/IPS Appliance Installation

   Do interested bidders need to be able to provide all three services? [Company X] for instance can't install and configure new IDS/IPS appliances but we are very capable in the areas of Penetration Testing and Network Configuration Review. Would you consider an RFP response for just 2 of the 3 services listed above?

   Proposers are required to perform all three phases of the RFP.

Vendor #4

1. Do we need to audit the PC's and laptops for compliance?

   The RFP is concerned with security vulnerabilities, not compliance.

2. We understand that WebApp Scanning, Code Scan, Database Scan is not part of the scope, is this true?

   Scanning applications, code reviews and database table/data configurations are not within the scope of this RFP. However, database connection/security vulnerabilities are included.

3. We understand that social engineering is not part of the scope, is that true?

   Social engineering is not within scope of this RFP.

4. Please provide us the device count by Network Device type that are in scope (Firewall, Router, Switches, IDS/IPS etc)

   All CLC controlled equipment is within scope of this RFP. Breakdown of systems/devices:

   20 Firewalls
   170 PCs
   31 Windows Servers
   15 Linux Servers
   15 Networked printers
   36 Switches
   6 Routers
   3 IDS/IPS
   2 VPNs
   13 Active External Internet Addresses split across 3 different connections

5. Please provide count of servers, would sampling be ok for servers.

   All CLC controlled equipment is within scope of this RFP.

6. For Physical security, do all 3 locations need to be assessed or if the processes are the same across all can we take a sample set.
   Physical security is outside the scope of this RFP.

7. For IDS/IPS installation, we are assuming the devices will be provided by the CLC and we will only provide installation support?
   The Successful Proposer must recommend IDS/IPS devices that it has experience with that will meet the needs of the CLC. The Successful Proposer may, but is not required to, submit pricing for the purchase of the IDS/IPS appliances. It is a requirement that the devices are installed and configured by the Successful Proposer, and that CLC IT staff is trained on how to use them.

8. For IDS/IPS installation, we are assuming it's going to be a HA pair, is that true?
   After a thorough review of the current CLC network, the Successful Proposer must submit what it believes to be the best implementation for the CLC's existing network infrastructure.

9. For IDS/IPS installation, it requires learning phase which will be determined based on conversation with the CLC staff that could add some more time to deployment in production, than the 90 day timeframe requested.
   The installation and initial configuration must be completed within 90 calendar days of the CLC receiving the IDS/IPS appliances. If the Proposer determines it is necessary to continue to configure/tweak the devices after installation, then this should be included as a deviation in its Proposal.

10. For IDS/IPS installation, does the CLC have Log monitoring in place where the IDS/IPS logs need to be routed, is this part of scope?
    The CLC employs log monitoring on an internal server.

11. Due to Coronavirus, do you anticipate any changes in submission and selection dates?
    Yes, the CLC has revised the remaining RFP Schedule due to the Coronavirus pandemic. Refer to the "Revision to RFP Schedule" section of this Addendum (page 1). Please monitor the CLC's website ctlottery.org for any further changes to the RFP, including its Schedule.

Vendor #5

1. Do you anticipate extending the bid due date?
   Yes, the CLC has revised the remaining RFP Schedule due to the Coronavirus pandemic. Refer to the "Revision to RFP Schedule" section of this Addendum (page 1).. Please monitor the CLC's website ctlottery.org for any further changes to the RFP, including its Schedule.

2. What additional details are you willing to provide, if any, beyond what is stated in bid documents concerning how you will identify the winning bid?
   None. Evaluation will be in accordance with the RFP.

3. Was this bid posted to the nationwide free bid notification website at www.mygovwatch.com?
   No, the RFP was posted to CT Biznet and the CLC websites.

4. Other than your own website, where was this bid posted?
   Notification sent to: Greater New England Minority Supplier Development Council and Center for Women & Enterprises.

.**Vendor #6**

1. Where does your infrastructure reside in? Your data center, a public cloud, a virtualized private cloud, or a combination?
   Cloud services are beyond the scope of this engagement. All systems in scope are on premise under direct control of the CLC.

2. What do you use today to detect cyber threats that have breached or are attempting to breach your organization?
   The CLC is not prepared to disclose this information to Proposers at this stage of the procurement process. Information regarding the CLC's existing IT infrastructure relevant to the engagement will be shared with the Successful Proposer after contract execution.

3. What environments are you looking to monitor (Cloud AWS/Azure, OnPrem Hyper-V or Vmware, Both)?
   Cloud services are beyond the scope of this engagement. All systems in scope are on premise under direct control of the CLC.

4. If you have a cloud infrastructure, how is secured today?
   Cloud services are beyond the scope of this engagement. All systems in scope are on premise under direct control of the CLC.

5. Are you running VMware or Hyper-V on-prem?
   The CLC utilizes virtualization for the majority of servers. The CLC is not prepared to disclose this information to Proposers at this stage of the procurement process. Information regarding the CLC's existing IT infrastructure relevant to the engagement will be shared with the Successful Proposer after contract execution.

6. How many Servers do you have within your Environment?
   See response to Vendor #4 – Question 4.

7. How many Firewalls do you have within your Environment? Are they all the same make & model?
   See response to Vendor #4 – Question 4.

8. How important is Security Compliance to you and your organization?
   The CLC is an extremely sensitive enterprise and its success depends on maintaining the public trust and confidence. As stated in the RFP, the CLC's overall objective is to ensure that appropriate security controls are implemented within the CLC's networks, servers, applications, and computing platforms to preserve integrity, confidentiality, and availability of the data that the CLC is responsible for. This engagement is also intended to ensure that security controls are effectively implemented to aid in the prevention of unauthorized, accidental, or deliberate disruption of CLC systems and data.

9. How many total devices would you want to manage/co-manage with a SIEM?
   See response to Vendor #4 – Question 4.

10. How many physical network locations do you have?
    Three physical locations within 15 miles of each other. The CLC's headquarters is located in Rocky Hill, CT.

11. Do you have current IDS/IPS solutions in place and if yes, what are they? If not, what products/requirements are you looking into?
    The CLC is not prepared to disclose this information to Proposers at this stage of the procurement process. Information regarding the CLC's existing IT infrastructure relevant to the engagement will be shared with the Successful Proposer after contract execution.

The Successful Proposer must recommend IDS/IPS devices that it has experience with that will meet the needs of the CLC. The Successful Proposer may, but is not required to, submit pricing for the purchase of the IDS/IPS appliances. It is a requirement that the devices are installed and configured by the Successful Proposer, and that CLC IT staff is trained on how to use them.

12. Is there a specified budget for each of the phases?
    The CLC has set a budget in FY20 for this purchase. However, the CLC is not prepared to disclose this information to Proposers at this stage of the procurement process. Proposers are expected to submit their best pricing to accommodate a response that will fulfill all the obligations of this RFP.

Vendor #7

1. How large is the IP space to be assessed (i.e., range size, how many class Cs, Class Bs, etc.)? Please provide the subnets/IP addresses.
    a. 350 live IP addresses on 15 subnets total are on the network. What is total possible number of IP addresses possible on the external network?
        See response to Vendor #4 – Question 4.

2. How may hosts are in scope as part of this assessment (i.e., how many hosts are expected to be live out of the IP space in question 3)?
    a. 350 live IP addresses on 15 subnets total are on the network. What is total number of live IP addresses in use on the external network?
        See response to Vendor #4 – Question 4.

3. Are any systems or devices in scope hosted by a third party?
    Third-party networks are beyond the scope of this engagement. All systems in scope are on premise under direct control of the CLC.

4. 350 live IP addresses on 15 subnets total are on the network. What is total possible number of IP addresses possible on the external network?
    See response to Vendor #4 – Question 4.

5. How may hosts are in scope as part of this assessment (i.e., how many hosts are expected to be live out of the IP space in question 3)?
    a. 350 live IP addresses on 15 subnets total are on the network. What is total number of live IP addresses in use on the external network?
        See response to Vendor #4 – Question 4.

6. How many of them contain or are data centers?
    All three locations contain servers or firewalls. However, the majority of systems are located at the CLC's headquarters.

    a. Name of city and state for each of the data center locations.
        Three physical locations within 15 miles of each other. The CLC's headquarters is located in Rocky Hill, CT.
    b. Size of each data center (i.e., number of network devices, size of server farm, etc.)
        See response to Vendor #4 – Question 4.

7. Number and locations of MAN/Campus/Branch networks in scope.
    See response to Vendor #4 – Question 4.

8. Approx. number of users/IP hosts per location.
   See response to Vendor #4 – Question 4.

9. Please describe the existing IDS/IPS installation in terms of the number, type and geographical location of consoles and endpoint detection/prevention systems. If any current whitelists are configured on the IDS/IPS systems today, how large are those lists?
   The CLC is not prepared to disclose this information to Proposers at this stage of the procurement process. Information regarding the CLC's existing IT infrastructure relevant to the engagement will be shared with the Successful Proposer after contract execution.

10. How many networks and systems are protected by IDS/IPS systems today?
    The CLC is not prepared to disclose this information to Proposers at this stage of the procurement process. Information regarding the CLC's existing IT infrastructure relevant to the engagement will be shared with the Successful Proposer after contract execution.

11. How many IT personnel are currently designated to respond to IDS/IPS events?
    The CLC is not prepared to disclose this information to Proposers at this stage of the procurement process. Information regarding pertinent CLC IT staff will be shared with the Successful Proposer after contract execution.

12. Does CLC have a SIEM platform implemented?
    The CLC is not prepared to disclose this information to Proposers at this stage of the procurement process. Information regarding the CLC's existing IT infrastructure relevant to the engagement will be shared with the Successful Proposer after contract execution.

13. Does CLC have a documented security incident response plan?
    The CLC is not prepared to disclose this information to Proposers at this stage of the procurement process. Information regarding the CLC's existing IT infrastructure relevant to the engagement will be shared with the Successful Proposer after contract execution.

14. Does CLC have a test lab environment set up and configured for IDS/IPS testing?
    The CLC does not have a separate lab environment setup for IDS/IPS testing.

Vendor #8

1. Are web applications in-scope and if so approximately how many web applications are in scope?
   Web applications are not within the scope of this RFP. However, the Successful Proposer should not exclude the webservers themselves from the penetration testing process.

   a. Web applications typically consist of static web pages, dynamic pages, component and database objects. The main interactions are typically static links, dynamic links and code call/return. Which of the preceding elements apply to the web applications? Roughly how many inter-application interactions occur?
      Not Applicable.

2. Internal network penetration testing requires a sampling approach. What is the value of the sampling? (e.g. 10%, 20%?). Or are we expected to do the whole internal network?
   Each Proposer must determine its own methods for performing the testing services required in the RFP.

Vendor #9

1. This RFP seems to have three stages (Network Penetration Testing, Network Configuration Review and New IDS/IPS Appliance Installation). Would we be allowed to submit a partial bid for this RFP? Specifically, we would like to submit a bid on the first two stages (Network Penetration Testing, Network Configuration Review), as we do not have expertise or resources for the third stage (New IDS/IPS Appliance Installation).
   Proposers are required to perform all three phases of the RFP.

Vendor #10

1. Is there a current incumbent party supplying the requirements for this RFP? If so, is there any weight to the incumbent concerning the award of the RFP?
   There is no incumbent party.

2. Is the requirements for this RFP an annual budgeted item and if so is the budget amount available to the responders of the RFP prior to the due date?
   The CLC has set a budget in FY20 for this purchase. However, the CLC is not prepared to disclose this information to Proposers at this stage of the procurement process. Proposers are expected to submit their best pricing to accommodate a response that will fulfill all the obligations of this RFP.

3. Concerning MUSL, is there a requirement to provide additional testing/assessments?
   No

4. Concerning 3rd party vendors with access to data, is there a requirement to provide additional testing/assessments?
   The CLC's proprietary computer gaming system and third-party vendor networks are excluded from this engagement.

5. Concerning satellite technologies/communications, is there a requirement to provide additional testing/assessments?
   The CLC does not utilize any satellite technology/communications.

Vendor #11

1. Due to the current pandemic, staff are currently working from home. To accommodate this:
   a. Is it possible for bidders to submit proposals via email rather than hard copy (Part I, Section A. Schedule, Page 1)?
      See response to Vendor #2 – Question 1.

   b. Similarly, given the pandemic, may we submit signed and notarized Attachment A – Proposer's Affidavit, Pages 18-19 and Attachment B – Consulting Agreement Affidavit, Page 20 when our social isolation directives are relaxed?
      Due to the Coronavirus pandemic, the CLC will accept signed forms in lieu of notarized forms. Proposers may be asked to provide notarized forms at a later date.

2. When was your last assessment of this nature performed?
   The CLC performs different forms of testing and assessments of its information technology and IT infrastructure periodically as part of its ongoing risk management program.

3. Part III. Requirements & Specifications, Page 5, states in relevant part, "The Proposer must also provide the CLC a sample penetration test report for review and a statement of work that includes all timeframes for this project." Please confirm whether the CLC is asking for a sample SOW to accompany the sample report or a sample SOW for the CLC project?

The CLC is interested in a statement of work for the upcoming CLC project, which will be reviewed for methodology and timeframes, as well as a separate sample penetration test report.

4. Regarding the new IDS/IPS appliance installation, Part III. Requirements & Specifications, Page 6, states in relevant part: "Work with CLC IT Department staff to configure and install the new IDS/IPS appliances within ninety (90) days of the CLC receiving the recommended IDS/IPS appliances. This will include knowledge transfer to the CLC IT department on daily usage of the IDS/IPS appliances including reporting and responding to alerts from the devices." May we assume that the awarded vendor performing the assessment will not be responsible for installing and configuring the appliances?

   CLC IT staff will work directly with the Successful Proposer; however, the CLC is relying solely on the expertise of the Successful Proposer for installation and configuration. This collaboration will aid the process by allowing the outside technicians the ability to ask questions directly from the CLC IT staff during the setup/configuration.

5. Regarding the network configuration review, Part III. Requirements & Specifications, Page 6, states in relevant part: "review current network configurations, including routers, switches and firewalls":
   a. Of the approximate 350 devices/IP addresses, how many of each type of device are in scope for the network configuration review? We need to know the quantity of each device type for accurate pricing.

      See response to Vendor #4 – Question 4.

6. Is web application testing in scope (Part III. Requirements & Specifications, Pages 5-6)?

   Web applications are not within the scope of this RFP. However, the Successful Proposer should not exclude the webservers themselves from the penetration testing process.

   a. If so, what is the number of URLs to be tested?

      Not Applicable.
   b. How many applications are included?

      Not Applicable.

7. Is there a wireless network assessment in scope (Part III. Requirements & Specifications, Pages 5-6)?

   The CLC does not utilize any wireless connections in the production network, so they are not a requirement of this RFP.

   a. If so, how many locations?

      Not Applicable.
   b. How many controllers are in scope?

      Not Applicable.
   c. If not controller based, please provide the number of WAPs.

      Not Applicable.

Vendor #12

1. Page 5, Part III. Requirements and Specifications: You mention 350 devices. Is that all servers, workstations, networking equipment, SCADA devices located in the 3 locations?

   See response to Vendor #4 – Question 4.

   a. This does not include any devices used to process lottery purchases at customer sites (i.e. Gas stations), correct?

The terminals and communications at retail outlets are not under the direct control of the CLC. The CLC's proprietary computer gaming system and third-party vendor networks are excluded from this engagement.

2. Network Penetration testing is specified. Is there any need to do application penetration testing?
   Web applications are not within the scope of this RFP. However, the Successful Proposer should not exclude the webservers themselves from the penetration testing process.

   a. If application penetration testing is desired, can you provide a list of applications that would be in scope?
      Not Applicable.

3. What is the timeframe, from contract award, that CT Lottery wants the penetration test concluded?
   The CLC will work with the Successful Proposer to schedule the on-site Network Penetration Testing phase of the engagement for a time that works best for both parties and allows for everyone involved to perform the necessary tasks in a safe environment.

   a. Will the penetration test occur prior to the possible implementation of the new IDS/IPS or after?
      The CLC will work with the Successful Proposer to schedule the on-site Network Penetration Testing phase of the engagement for a time that works best for both parties and allows for everyone involved to perform the necessary tasks in a safe environment.

4. Vulnerability assessments are often a suggested first step (in our opinion) before a penetration test. Has the CT Lottery done a vulnerability assessment already?
   The CLC has previously enlisted a third-party vendor to perform a vulnerability assessment.

   a. If yes, can the vulnerability assessment be provided?
      No

5. Page 6, Part III. Requirements and Specifications, Section: Network Configuration Review: There is an IDS/IPS system already in place. Can you provide clarity on the vendor/product you currently have?
   The CLC is not prepared to disclose this information to Proposers at this stage of the procurement process. Information regarding the CLC's existing IT infrastructure relevant to the engagement will be shared with the Successful Proposer after contract execution.

6. Page 6, Part III. Requirements and Specifications, Section: New IDS/IPS Appliance Installation: Is there a hardware vendor that CT Lottery is considering for the IDS/IPS replacement or does that decision need to be made?
   The Successful Proposer must recommend IDS/IPS devices that it has experience with that will meet the needs of the CLC. The Successful Proposer may, but is not required to, submit pricing for the purchase of the IDS/IPS appliances. It is a requirement that the devices are installed and configured by the Successful Proposer, and that CLC IT staff is trained on how to use them.

   a. If it has been selected can you provide the vendor/product chosen?
      Not Applicable.

Vendor #13

1. Does the Lottery want a black, grey, or white box pen test approach?
   White box. This is a collaborative effort.

2. Can all internal testing be conducted at the Rocky Hill facility or will travel to the other locations be required?
   All networks can be accessed via a connection at the CLC's Rocky Hill facility.

3. Of the 350 IP addresses in scope, how many are external-facing vs internal facing?
   See response to Vendor #4 – Question 4.

4. Are any of your publicly accessible systems in scope hosted by a third party or a cloud service provider, such as Rackspace or AWS?
   Cloud services are beyond the scope of this engagement. All systems in scope are on premise under direct control of the CLC.

5. Will pen testing also include web applications? If so,
   Web applications are not within the scope of this RFP. However, the Successful Proposer should not exclude the webservers themselves from the penetration testing process.

   a. How many web applications are in scope?
      Not Applicable.

   b. How many API endpoints?
      Not Applicable.

   c. How many static vs dynamic pages?
      Not Applicable.
   d. Are any of these custom-developed by the Lottery?
      Not Applicable.

6. Is targeted Denial of Service testing required?
   This is not a requirement.

7. Can vulnerability scans and penetration tests be performed during working hours, or do they need to be performed after hours?
   External penetration testing/scans can be performed anytime. Internal vulnerability scans and penetration tests will be performed during normal business hours (8:30am-4:30pm M-F, excluding holidays). The CLC will aid in selecting secondary servers to start with that will not impact the production environment. Based on the level of disruption to the network/systems it may be necessary to schedule specific times.

8. For the network configuration reviews, how many devices are in scope?
   6 routers and 36 switches

9. Does the Lottery currently know how many IDS/IPS devices will be purchased or required to be installed/configured by consultant?
   The Successful Proposer must recommend IDS/IPS devices that it has experience with that will meet the needs of the CLC. The Successful Proposer may, but is not required to, submit pricing for the purchase of the IDS/IPS appliances. It is a requirement that the devices are installed and configured by the Successful Proposer, and that CLC IT staff is trained on how to use them.

10. Is there a date that the Lottery would like all work to be completed by?
    The CLC will finalize the scope of work and goals and objectives with the Successful Proposer prior to contract execution.

11. Does the Lottery require a presentation to management once all testing is done?

This is not a requirement of the RFP. However, if Proposers customarily include such presentations as part of their services at no additional cost or expense, then they should say so in their Proposals.

12. The state in which we work (Washington) is under order requiring non-essential workers and businesses to stay home (currently in effect from March 24 to April 10). For this reason, we'd like to request that you accept electronic submission of proposals in a PDF or similar format. Firm-wide, [Company X] employees are currently working remotely from home offices under shelter-in-place orders. We're concerned that the complex logistics of producing and shipping hard copies would require us to violate legal restrictions and risk the health and safety of our employees and communities—as well as yours. We're committed to a safe and ethical work environment for our employees and our clients and hope that our uncertain and quickly changing situation will allow for this accommodation. This link provides more information on the type of restrictions we are under: https://medium.com/wagovernor.
    See response to Vendor #2 – Question #1.

Vendor #14

1. How many IP Addresses will be in-scope for the external penetration test?
    See response to Vendor #4 – Question 4.

2. Will the CLC provide the external IP Addresses that are in scope for the external penetration test?
    The CLC will provide a list of external IP address to the Successful Proposer following contract execution.

3. Will the CLC whitelist the penetration tester on their IPS systems for the external penetration test?
    No

4. Internal penetration test:
    a. Will the penetration tester be positioned on the network or placed within a VLAN that has access to all subnets?
        All networks can be accessed via a connection at the CLC's Rocky Hill facility.

    b. If not, will the CLC be able to move the penetration tester to adjacent subnets if they cannot achieve lateral movement through a compromised vector?
        No

5. Will we be given access credentials for all network devices? if not, what is the plan?
    Exported router and switch configurations will be given to the Successful Proposer after contract execution.

6. How many firewalls?
    See response to Vendor #4 – Question 4.

7. How many routers?
    See response to Vendor #4 – Question 4.

8. How many switches?
    See response to Vendor #4 – Question 4.

9. Wireless access points?

The CLC does not utilize any wireless connections in the production network, so they are not a requirement of this RFP.

10. Any other devices?
    See response to Vendor #4 – Question 4.

11. Do they use voip?
    The CLC is not prepared to disclose this information to Proposers at this stage of the procurement process. Information regarding the CLC's existing IT infrastructure relevant to the engagement will be shared with the Successful Proposer after contract execution.

12. Identify specific devices- servers, routers, gateways, etc. quantity and OS version.
    See response to Vendor #4 – Question 4.

13. Number of phones and models.
    The CLC is not prepared to disclose this information to Proposers at this stage of the procurement process. Information regarding the CLC's existing IT infrastructure relevant to the engagement will be shared with the Successful Proposer after contract execution.

14. How many site to site vpn's?
    The CLC is not prepared to disclose this information to Proposers at this stage of the procurement process. Information regarding the CLC's existing IT infrastructure relevant to the engagement will be shared with the Successful Proposer after contract execution.

15. How many users access a vpn to their site?
    The CLC is not prepared to disclose this information to Proposers at this stage of the procurement process. Information regarding the CLC's existing IT infrastructure relevant to the engagement will be shared with the Successful Proposer after contract execution.

16. How do they manage users? Radius or Active Directory or other?
    The CLC is not prepared to disclose this information to Proposers at this stage of the procurement process. Information regarding the CLC's existing IT infrastructure relevant to the engagement will be shared with the Successful Proposer after contract execution.

17. What user vpn software do they use?
    The CLC is not prepared to disclose this information to Proposers at this stage of the procurement process. Information regarding the CLC's existing IT infrastructure relevant to the engagement will be with the Successful Proposer after contract execution.

18. How many outside vendors are allowed to access internal resources?
    The CLC is not prepared to disclose this information to Proposers at this stage of the procurement process. Information regarding the CLC's existing IT infrastructure relevant to the engagement will be shared with the Successful Proposer after contract execution.

    a. What is the nature of those resources?

19. What policies are applied to outside vendors?
    The CLC is not prepared to disclose this information to Proposers at this stage of the procurement process. Information regarding the CLC's existing IT infrastructure relevant to the engagement will be shared with the Successful Proposer after contract execution.

20. What type of devices connect to their network?

The CLC is not prepared to disclose this information to Proposers at this stage of the procurement process. Information regarding the CLC's existing IT infrastructure relevant to the engagement will be shared with the Successful Proposer after contract execution.

21. For business owned devices:

    a. hardware make/model/year purchased
    b. what operating systems?

        The CLC is not prepared to disclose this information to Proposers at this stage of the procurement process. Information regarding the CLC's existing IT infrastructure relevant to the engagement will be shared with the Successful Proposer after contract execution.

22. Can you describe any infrastructure in place that is used to apply updates to business owned systems?

    The CLC is not prepared to disclose this information to Proposers at this stage of the procurement process. Information regarding the CLC's existing IT infrastructure relevant to the engagement will be shared with the Successful Proposer after contract execution.

23. How do desktop and server operating systems get updates?

    The CLC is not prepared to disclose this information to Proposers at this stage of the procurement process. Information regarding the CLC's existing IT infrastructure relevant to the engagement will be shared with the Successful Proposer after contract execution.

24. How do desktop and server applications get updates?

    The CLC is not prepared to disclose this information to Proposers at this stage of the procurement process. Information regarding the CLC's existing IT infrastructure relevant to the engagement will be shared with the Successful Proposer after contract execution.

25. What federal regulations apply to their network (PCI, GLB, etc.?)

    The CLC's objectives and goals of the engagement are stated in Part III of the RFP.

26. What state regulations apply to their network?

    The CLC's objectives and goals of the engagement are stated in Part III of the RFP.

27. What business policies apply to their network?

    The CLC's objectives and goals of the engagement are stated in Part III of the RFP.

28. Do they implement any type of cloud computing? Azure, Amazon, etc?

    a. Will this be part of the network review?

        Cloud services are beyond the scope of this engagement. All systems in scope are on premise under direct control of the CLC.

29. What technology (WAN, ELAN, L1?) interconnects the sites?

    The CLC utilizes a fiber primary connection between sites and backup T1s.

30. How many Internet connections are in use?

    See response to Vendor #4 – Question 4.

31. Is BGP in use and if so what architecture is used with the ISP(s)?

The CLC is not prepared to disclose this information to Proposers at this stage of the procurement process. Information regarding the CLC's existing IT infrastructure relevant to the engagement will be shared with the Successful Proposer after contract execution.

32. Does any device run the ASA image or the FTD (Firepower Threat Defense) image?
    The CLC is not prepared to disclose this information to Proposers at this stage of the procurement process. Information regarding the CLC's existing IT infrastructure relevant to the engagement will be shared with the Successful Proposer after contract execution.

33. What Cisco cloud services connect to the network devices?
    Cloud services are beyond the scope of this engagement. All systems in scope are on premise under direct control of the CLC.

34. Does any device run in a failover pair? (Act/Stby or Act/Act)?
    The CLC is not prepared to disclose this information to Proposers at this stage of the procurement process. Information regarding the CLC's existing IT infrastructure relevant to the engagement will be shared with the Successful Proposer after contract execution.

35. How many lines long is the current config?
    The CLC is not prepared to disclose this information to Proposers at this stage of the procurement process. Information regarding the CLC's existing IT infrastructure relevant to the engagement will be shared with the Successful Proposer after contract execution.

36. Does the config include remote access VPN, site to site VPN, or SSL VPN services?
    The CLC is not prepared to disclose this information to Proposers at this stage of the procurement process. Information regarding the CLC's existing IT infrastructure relevant to the engagement will be shared with the Successful Proposer after contract execution.

37. Would CT Lottery be willing to sign an NDA prior to bidding so that we can submit financial records with our bid? If no, will CT Lottery accept only our D&B number (15-138-2793) and upon award an NDA will need to be executed and financials will be provided then.
    Proposers must provide financials pursuant to Part IV, Section C of the RFP to confirm their financial soundness and stability. The CLC is subject to the Freedom of Information Act and, therefore, is unable to sign an NDA. Please refer to Part IV, Section B of the RFP concerning marking and submitting Proposer Confidential Information.

Vendor #15

Questions 1-4 relate to external penetration testing. Questions 5-13 relate to internal penetration testing.

1. Within the in-scope IP addresses, approximately how many active nodes are there exposed to the internet?
   See response to Vendor #4 – Question 4.

2. Will you need to limit testing to outside of business hours?
   External penetration testing/scans can be performed anytime. Internal vulnerability scans and penetration tests will be performed during normal business hours (8:30am-4:30pm M-F, excluding holidays). The CLC will aid in selecting secondary servers to start with that will not impact the production environment. Based on the level of disruption to the network/systems it may be necessary to schedule specific times.

3. After the report is delivered, would you like to have your remediation efforts validated*? Note: The standard retesting window is 30 days.*
    a. If 30 days is insufficient, what is an acceptable remediation lifecycle for your organization?

       The CLC will review the Successful Proposer's re-remediation testing terms, if offered, prior to contract execution.

4. Are any in-scope nodes hosted with a third-party cloud provider? If so, which provider(s)? Cloud services are beyond the scope of this engagement. All systems in scope are on premise under direct control of the CLC.
    a. Are stand-alone nodes (e.g. VMs, VPCs, EC2, etc.) used or is it a server-less architecture?

       The CLC is not prepared to disclose this information to Proposers at this stage of the procurement process. Information regarding the CLC's existing IT infrastructure relevant to the engagement will be shared with the Successful Proposer after contract execution.

    b. Are any in-scope assets located outside of the United States? If so, which countries?

       All assets are in the United States.

    c. What level of information sharing would you like to use during this project? (Pick one)
        i. Full-Disclosure (if a collaborative or "Purple Team" assessment is desired)
        ii. Semi-Blind (provide IP ranges and hostnames only)
        iii. Blind (have partner identify target ranges)
        iv. Hybrid (have partner identify target ranges and fill in any gaps prior to the assessment)

       Full-Disclosure

    d. What level of evasiveness would you like partner to employ for this engagement? (Pick one)
        i. Non-Evasive
        ii. Evasive
        iii. Hybrid-Evasive (start evasive and slowly become "louder" until continuing non-evasively)

       Non-Evasive

5. Can access be provided such that all in-scope systems are reachable from a single network location? If not, please describe.

   All networks can be accessed via a connection at the CLC's Rocky Hill facility.

6. Would you like the assessment to include segmentation/isolation testing as required by the PCI-DSS? If so, please describe the number of perspectives necessary to fully validate all potential ingress/egress points.

   The CLC does not require testing to follow any specific requirements. It is up to each Proposer to determine the best course of action for testing and network review.

7. With regards to the IPS, there is no mention of the specific number of locations that will require IPS/IDS inspection. Is that up to the overall evaluation of the design during part II – network configuration and review of the engagement?

   The Successful Proposer must recommend IDS/IPS devices that it has experience with that will meet the needs of the CLC. The Successful Proposer may, but is not required to,

submit pricing for the purchase of the IDS/IPS appliances. It is a requirement that the devices are installed and configured by the Successful Proposer, and that CLC IT staff is trained on how to use them.

8. If we determine after the configuration review that additional segmentation and network access control are required, the assumptions will be that we make those recommendations of part II along with a scope of remediation (to be provided in addition to this work) to remedy these findings?

   All findings/suggestions/recommendations will be provided by the Successful Proposer in its written report after completing the network reviews and testing.

9. Regarding the Penetration testing and results – will the proposer be permitted to participate in the remediation activity in a separate scope of work for closing any vulnerabilities, etc.?

   Proposers are welcome to provide information and pricing for remediation support services for consideration by the CLC.

Vendor #16

1. PART IV. SUBMISSION REQUIREMENTS & PROPOSAL CONTENTS
   a. SUBMISSION REQUIREMENTS
      i. Delivery of Submissions
         1. Proposers must submit an original and four (4) printed copies of their full Proposals. Proposers must also submit an electronic "searchable" PDF/Word (on CD/DVD/USB Stick) version of their full Proposals (See 7 Part IV, Section B for instructions on submitting a second electronic version of Proposals redacted to exclude Proposer Confidential Information).

            See response to Vendor #2 – Question 1.

Vendor #17

1. Our company is looking to Partner for this RFP response, and I was wondering if the external and internal penetration testing can only be done remotely while my company does the remaining onsite work?

   Refer to the "Clarifications" section of this document (page 1). This is a collaborative effort. The CLC will accommodate the Successful Proposer with a workstation and network connection at the Rocky Hill facility after Connecticut's "Shelter-In-Place" order expires and the CLC has lifted public access restrictions to its headquarters. When appropriate, the Successful Proposer will be required to physically plug into the network at the CLC's Rocky Hill facility and attempt to gain access to systems, files and data mimicking an attacker with internal network access with no credentials. This testing must be performed on-site per RFP section Part III. REQUIREMENTS & SPECIFICATIONS. All networks can be accessed via a connection at the CLC's Rocky Hill facility.

Vendor #18

1. Page 2, Proposal Submission Date. It is stated that proposals must be submitted by mail or in-person. In light of everything that is going on with COVID-19 would you please consider allowing us to submit our proposal via email only?

   See response to Vendor #2 – Question 1.

2. We are a privately held corporation and do not release detailed financial statements. In lieu of financial statements, will you accept a Credit Advisory Report from Dun and Bradstreet?
   Proposers must provide financials pursuant to Part IV, Section C of the RFP to confirm their financial soundness and stability. Please refer to Part IV, Section B of the RFP concerning marking and submitting Proposer Confidential Information.

3. What is the budget for this project?
   The CLC has set a budget in FY20 for this purchase. However, the CLC is not prepared to disclose this information to Proposers at this stage of the procurement process. Proposers are expected to submit their best pricing to accommodate a response that will fulfill all the obligations of this RFP.

4. Page 7, B. Freedom of Information Act. Will you accept a separate redacted proposal?
   Proposers must submit a complete version of their Proposals. If a Proposal contains information that the Proposer claims should not be public, then the Proposer should follow the instructions in Part IV, Section B of the RFP and also provide a Public Copy of its Proposal.

5. Page 5, Part III, Requirement and Specifications. Will you require on-site presence or (in light of current circumstances) will remote work be possible beyond the assessment tasks? How will the physical plug into the network occur?
   Refer to the "Clarifications" section of this document (page 1). This is a collaborative effort. The CLC will accommodate the Successful Proposer with a workstation and network connection at the Rocky Hill facility after Connecticut's "Shelter-In-Place" order expires and the CLC has lifted public access restrictions to its headquarters. When appropriate, the Successful Proposer will be required to physically plug into the network at the CLC's Rocky Hill facility and attempt to gain access to systems, files and data mimicking an attacker with internal network access with no credentials. This testing must be performed on-site per RFP section Part III. REQUIREMENTS & SPECIFICATIONS. All networks can be accessed via a connection at the Rocky Hill facility.

6. Page 6, New IDS/IPS Appliance Installation. How should we present pricing for installation of a product/solution when that is an unknown?
   The Successful Proposer must recommend IDS/IPS devices that it has experience with that will meet the needs of the CLC. The Successful Proposer may, but is not required to, submit pricing for the purchase of the IDS/IPS appliances. It is a requirement that the devices are installed and configured by the Successful Proposer, and that CLC IT staff is trained on how to use them.

Vendor #19

1. As part of Network Penetration Testing, list of External devices/ IP addresses to be tested remotely
   See response to Vendor #4 – Question 4.

2. As part of Network Penetration Testing, list of Internal devices/ IP addresses to be tested Onsite
   See response to Vendor #4 – Question 4.

3. As part of Network Penetration Testing, is the service provider expected to visit all 3 physical locations in scope or systems, files and data can be accessed from a central location?
   All networks can be accessed via a connection at the Rocky Hill facility.

4. As part of Network Configuration review, please specify the number of routers, switches & firewalls along with make & model for each device.
   See response to Vendor #4 – Question 4.

5. When is the project likely to start?
   The CLC will finalize the scope of work and goals and objectives with the Successful Proposer prior to contract execution.

6. Also, is there an empanelment process and how can we be on the list of RFP recipients/notifications?

   Please visit ctlottery.org (About Us/Procurement/Contact Us).

Vendor #20

1. How many Internal IP's?
   See response to Vendor #4 – Question 4.

2. How Many External IP's
   See response to Vendor #4 – Question 4.

3. How many firewalls?
   See response to Vendor #4 – Question 4.

4. How many network switches?
   See response to Vendor #4 – Question 4.

5. How many Wireless networks and Access Points?
   Wireless networks are not within the scope of this RFP.

6. Does Scope include any website, if so how many and what are they?
   Web applications are not within the scope of this RFP. However, the Successful Proposer should not exclude the webservers themselves from the penetration testing process.

7. How many cloud based applications?
   Cloud services are beyond the scope of this engagement. All systems in scope are on premise under direct control of the CLC.

8. What IDS/IPS is being used?
   The CLC is not prepared to disclose this information to Proposers at this stage of the procurement process. Information regarding the CLC's existing IT infrastructure relevant to the engagement will be shared with the Successful Proposer after contract execution.

Vendor #21

1. Are you asking the winner of the proposal to recommend the IDS/IPS or will you determine that?
   The Successful Proposer must recommend IDS/IPS devices that it has experience with that will meet the needs of the CLC. The Successful Proposer may, but is not required to, submit pricing for the purchase of the IDS/IPS appliances. It is a requirement that the

devices are installed and configured by the Successful Proposer, and that CLC IT staff is trained on how to use them.

2. What kind of user management systems, Active Directory, etc. is currently used?
   The CLC is not prepared to disclose this information to Proposers at this stage of the procurement process. Information regarding the CLC's existing IT infrastructure relevant to the engagement will be shared with the Successful Proposer after contract execution.

3. Are the three locations internetworked and if so, how?
   The CLC utilizes a fiber primary connection between sites and backup T1s.

4. What 3rd party appliances are involved in the networks?
   Third-party networks are beyond the scope of this engagement. All systems in scope are on premise under direct control of the CLC.

5. Are there any required certifications for this contract?
   The Successful Proposer and its Key Persons are required to be separately licensed by the Connecticut Department of Consumer Protection as stated in Part VI, Section E of the RFP. While the CLC does not require Proposers to possess specific certifications, the CLC expects Proposers to possess minimum certifications and licenses required to conduct their businesses in compliance with applicable federal, state, or local laws.

Vendor #22

1. Can you categorize the 350 endpoints as to the number of servers, PC's appliances, etc?
   See response to Vendor #4 – Question 4.

2. Has the CLC made an affirmative decision to replace the current IDS/IPS systems?
   The Successful Proposer must recommend IDS/IPS devices that it has experience with that will meet the needs of the CLC. The Successful Proposer may, but is not required to, submit pricing for the purchase of the IDS/IPS appliances. It is a requirement that the devices are installed and configured by the Successful Proposer, and that CLC IT staff is trained on how to use them.

3. What hardware and software comprise the current IDS/IPS systems and when were they installed?
   The CLC is not prepared to disclose this information to Proposers at this stage of the procurement process. Information regarding the CLC's existing IT infrastructure relevant to the engagement will be shared with the Successful Proposer after contract execution.

4. In PART VI SPECIAL PROVISIONS, SECTION G GENERAL INDEMNIFICATIONS, "defend the CLC and the State of Connecticut, and each of their respective directors, officers, employees, and representatives (collectively, Indemnified Parties), from and against any and all claims, losses, or liabilities of any kind (including attorney's fees and costs) (Claims) **arising out of, resulting from, or related to the contract** or any of its (or any its subcontractor's) malfeasance, misconduct, negligence (or more culpable act or omission), tortious acts, or violations of applicable law or intellectual or proprietary rights of any person or entity while performing or failing to perform the contract." Commercial contracts do not include unlimited liability – otherwise the pricing would be too high to be affordable. Can this provision be modified to limit the liability?
   No

Vendor #23

1. How many external IP's do you have, that need to be tested?
   See response to Vendor #4 – Question 4.

2. What are behind those external IP's. ?
   The CLC is not prepared to disclose this information to Proposers at this stage of the procurement process. Information regarding the CLC's existing IT infrastructure relevant to the engagement will be shared with the Successful Proposer after contract execution.

3. How many servers do you have?
   See response to Vendor #4 – Question 4.

4. Where are the Servers located?
   Three physical locations within 15 miles of each other. The CLC's headquarters is located in Rocky Hill, CT.

5. What are the key reasons for performing a Penetration Test Risk Assessment?
   The CLC's objectives and goals of the engagement are stated in Part III of the RFP.

6. What are you trying to achieve by performing this assessment?
   The CLC's objectives and goals of the engagement are stated in Part III of the RFP.

7. List any other milestones/tasks you would like to see accomplished during the assessment.
   The CLC will finalize the scope of work and its goals and objectives with the Successful Proposer prior to contract execution.

8. What is your estimated timeline for making a final decision?
   Refer to the "Revision to RFP Schedule" section of this Addendum (page 1).. Please monitor the CLC's website ctlottery.org for any further changes to the RFP, including its Schedule.

9. How long does it take to provision access for consultants (for example, account access if required, badges, space)?
   The Connecticut Department of Consumer Protection is responsible for vendor licensing. The Successful Proposer is advised to submit all required licensing paperwork to the DCP as soon as possible following receipt of preliminary award.

10. When does your project need to be completed?
    We are flexible given the challenges presented by the Coronavirus. We will work with the Successful Proposer on a mutually agreeable completion date.

11. What are your internal deadlines?
    The CLC's deadlines are based on the schedule outlined in the RFP. We are flexible given the challenges presented by the Coronavirus. We will work with the Successful Proposer on a mutually agreeable completion date.

    INTERNAL: Number of network subnets and sizes to be scanned:
    See response to Vendor #4 – Question 4.

12. Total Number of Active IPs
    See response to Vendor #4 – Question 4.

13. Can all IP addresses be accessed from one location/assigned IP address? If not, how many locations are required?
    All networks can be accessed via a connection at the Rocky Hill facility

14. Can all the tests be performed remotely using a virtual scanner (Travel is Not Allowed during Covid Shelter in Place)
    Refer to the "Clarifications" section of this document (page 1). This is a collaborative effort. The CLC will accommodate the Successful Proposer with a workstation and network connection at the Rocky Hill facility after Connecticut's "Shelter-In-Place" order expires and the CLC has lifted public access restrictions to its headquarters. When appropriate the Successful Proposer will be required to physically plug into the network at the CLC's Rocky Hill facility and attempt to gain access to systems, files and data mimicking an attacker with internal network access with no credentials. This testing must be performed on-site per RFP section Part III. REQUIREMENTS & SPECIFICATIONS. All networks can be accessed via a connection at the Rocky Hill facility.

15. Can one sensor scan all assets in scope? (Must have bandwidth and port accessibility)
    Each Proposer must determine its own methods for performing the testing services required in the RFP.

16. Can a sensor be installed in the CLC environment? (Physical or Virtual) (Travel is Not Allowed during Covid 19 Shelter in Place)
    Under no circumstances is any device or software to be installed in the CLC network.

17. IPS Models to be reviewed Are they unique or the same model IPS at the three CLC locations? we'd be interested in understanding if the configurations are "cookie-cutter: (similar), or unique?
    IPS configuration review is not in the scope of this RFP, as they will be replaced.

18. Will active countermeasures be in place during testing?
    Yes

19. Can testing source IP's be white-listed from active countermeasures (shunning, HIDS, HIPS, NAC)?
    No

20. Are any third parties (service providers) in scope? (e.g., Azure, AWS, Remote Data Center)
    The CLC's proprietary computer gaming system and third-party vendor networks are excluded from this engagement.

21. Is PCI DSS Segmentation Testing Required? (e.g., CDE)
    No

22. Is work required to be performed after hours?
    External penetration testing/scans can be performed anytime. Internal vulnerability scans and penetration tests will be performed during normal business hours (8:30am-4:30pm M-F, excluding holidays). The CLC will aid in selecting secondary servers to start with that will not impact the production environment. Based on the level of disruption to the network/systems it may be necessary to schedule specific times.

23. Do you need presentations from onsite
    EXTERNAL: Number of network subnets and sizes to be scanned:
    See response to Vendor #4 – Question 4.

24. Is Network Discovery Required (Need to Find Active IPs)
    This is a collaborative effort, however each Proposer must determine its own methods for performing the testing services required in the RFP,

25. Will active countermeasures be in place during testing?
    Yes

26. Can testing source IP's be white-listed from active countermeasures (shunning, HIDS, HIPS)?
    No

27. Are any third parties (service providers) in scope? (e.g., Azure, AWS, Remote Data Center)
    The CLC's proprietary computer gaming system and third-party vendor networks are excluded from this engagement.

28. Is work required to be performed after hours?
    External penetration testing/scans can be performed anytime. Internal vulnerability scans and penetration tests will be performed during normal business hours (8:30am-4:30pm M-F, excluding holidays). The CLC will aid in selecting secondary servers to start with that will not impact the production environment. Based on the level of disruption to the network/systems it may be necessary to schedule specific times.

29. Do you need presentations from onsite
    CONFIGURATION REVIEW: Please identify the numbers for samples of the following that will be considering in the scope of the review.
    See response to Vendor #4 – Question 4. Each Proposer must determine its own methods for performing the testing services required in the RFP

30. What types of data is available for the network documentation review
    Network diagrams, exported router and switch configurations will be given to the Successful Proposer after contract execution.

31. Number of routers, in scope :
    See response to Vendor #4 – Question 4.

32. Number of switches, in scope:
    See response to Vendor #4 – Question 4.

33. Number of security devices (Firewall/IDS), in scope:
    See response to Vendor #4 – Question 4.

34. Can all the configurations be provided for review off-site (Travel is Not Allowed during Covid 19 Shelter in Place)
    IDS/IPS REVIEW
    Configurations can be reviewed off-site. Refer to the "Clarifications" section of this document (page 1). This is a collaborative effort. The CLC will accommodate the Successful Proposer with a workstation and network connection at the Rocky Hill facility after Connecticut's "Shelter-In-Place" order expires and the CLC has lifted public access restrictions to its headquarters. When appropriate, the Successful Proposer will be required to physically plug into the network at the CLC's Rocky Hill facility and attempt to gain access to systems, files and data mimicking an attacker with internal network access with no credentials. This testing must be performed on-site per RFP section Part III. REQUIREMENTS & SPECIFICATIONS. All networks can be accessed via a connection at the Rocky Hill facility.

35. Will requirements for the IDS be provided
    The CLC is not prepared to disclose this information to Proposers at this stage of the procurement process. Information regarding the CLC's existing IT infrastructure relevant to the engagement will be shared with the Successful Proposer after contract execution.

36. Is the IDS required to be a stand-alone solution or integrated into the firewalls
    The Successful Proposer must recommend IDS/IPS devices that it has experience with that will meet the needs of the CLC. The Successful Proposer may, but is not required to, submit pricing for the purchase of the IDS/IPS appliances. It is a requirement that the devices are installed and configured by the Successful Proposer, and that CLC IT staff is trained on how to use them.

37. How many IDS/IPS are required?
    The Successful Proposer must recommend IDS/IPS devices that it has experience with that will meet the needs of the CLC. The Successful Proposer may, but is not required to, submit pricing for the purchase of the IDS/IPS appliances. It is a requirement that the devices are installed and configured by the Successful Proposer, and that CLC IT staff is trained on how to use them.

38. Why is the current IDS/IPS being considered for replacement
    NEW IDS/IPS APPLIANCE INSTALLATION
    The CLC is not prepared to disclose this information to Proposers at this stage of the procurement process. Information regarding the CLC's existing IT infrastructure relevant to the engagement will be shared with the Successful Proposer after contract execution.

39. Can all physical plugging of the IDS/IPS be performed by CLC and configuration be performed remotely. (Travel is Not Allowed during Covid Shelter in Place)
    Refer to the "Clarifications" section of this document (page 1). This is a collaborative effort. The CLC will accommodate the Successful Proposer with a workstation and network connection at the Rocky Hill facility after Connecticut's "Shelter-In-Place" order expires and the CLC has lifted public access restrictions to its headquarters. When appropriate, the Successful Vendor will be required to physically plug into the network at the CLC's Rocky Hill facility and attempt to gain access to systems, files and data mimicking an attacker with internal network access with no credentials. This testing must be performed on-site per RFP section Part III. REQUIREMENTS & SPECIFICATIONS. All networks can be accessed via a connection at the Rocky Hill facility

40. Does the request for an optional penetration test after new IDS/IPS is installed mean that Red Team testing is being requested or that IP addressed are not going to be whitelisted in protection measures
    No whitelisting will be used during any phase of the testing.

Vendor #24

1. May I please know if this is a new contract?
   This is a new contract.

2. If this old contract, may I please know how many incumbents were and could you please share the names of the incumbents?
   Not Applicable.

3. Could you please share the estimated budget for this contract?
   The CLC has set a budget in FY20 for this purchase. However, the CLC is not prepared to disclose this information to Proposers at this stage of the procurement process. Proposers are expected to submit their best pricing to accommodate a response that will fulfill all the obligations of this RFP.

Vendor #25

1. Page 5, Part III, “The CLC’s network consists of: " - Of the 300+ IP's and multiple subnets, what is the estimate of network devices?
   See response to Vendor #4 – Question 4.

2. Page 5, Part III, “The CLC’s network consists of: " - What vendors are the existing network devices?
   The CLC is not prepared to disclose this information to Proposers at this stage of the procurement process. Information regarding the CLC’s existing IT infrastructure relevant to the engagement will be shared with the Successful Proposer after contract execution.

3. Page 5, Part III, “The CLC’s network consists of: " - Can we get a hardware/software list if available?
   The CLC is not prepared to disclose this information to Proposers at this stage of the procurement process. Information regarding the CLC’s existing IT infrastructure relevant to the engagement will be shared with the Successful Proposer after contract execution.

4. Page 6, Part III, “Network Penetration Testing: ” - During the onsite assessment, are we to assume we are granted access to the facility to physically plug into the network at the CLC’s Rocky Hill facility. Or, do we “attempt” to gain access into the CLC Rocky Hills facility to physically plug into the network?
   Refer to the “Clarifications” section of this document (page 1). This is a collaborative effort. The CLC will accommodate the Successful Proposer with a workstation and network connection at the Rocky Hill facility after Connecticut’s “Shelter-In-Place” order expires and the CLC has lifted public access restrictions to its headquarters. When appropriate, the Successful Proposer will be required to physically plug into the network at the CLC’s Rocky Hill facility and attempt to gain access to systems, files and data mimicking an attacker with internal network access with no credentials. This testing must be performed on-site per RFP section Part III. REQUIREMENTS & SPECIFICATIONS. All networks can be accessed via a connection at the Rocky Hill facility.

5. Page 6, Part III, “Network Configuration Review:” - Are there existing IDS/IPS requiring integration with recommended systems?
   The existing IDS/IPS solution will be replaced with the new solution. The Successful Proposer must recommend IDS/IPS devices that it has experience with that will meet the needs of the CLC. The Successful Proposer may, but is not required to, submit pricing for the purchase of the IDS/IPS appliances. It is a requirement that the devices are installed and configured by the Successful Proposer, and that CLC IT staff is trained on how to use them.

6. General question - Are there any specific compliance regulations/policies mandated by City/County/State/Federal/Tribal?
   The CLC’s objectives and goals of the engagement are stated in Part III of the RFP.

Vendor #26

Part III. REQUIREMENTS & SPECIFICATIONS, pp 5 - 6

1. What Standard or Law does CLC need this Vulnerability Assessment/Pen Test to comply with? (I.E. NIST SP800-53, PCI-DSS, HIPAA, and/or State Privacy Laws etc.)
   No specific risk assessment methodology is prescribed for this engagement.

2. (p. 6) Is the CLC RFP purely just a Vulnerability Assessment and Penetration Test to document Known Vulnerabilities, and Exploits, and prove without a doubt that an Exploit could be used to Penetrate the CLC Network?

The CLC's objectives and goals of the engagement are stated in Part III of the RFP. The CLC takes data and system security very seriously and continuously strives to improve its security posture.

3. (p. 5) Are the 350 devices/IP addresses Internal or External?
   See response to Vendor #4 – Question 4.

4. (p.5) Of the Three Internet Connections, how many External IP Addresses are exposed to the Public Internet?
   See response to Vendor #4 – Question 4.

5. Are we testing any cloud environments such as AWS or Azure for CLC
   Cloud services are beyond the scope of this engagement. All systems in scope are on premise under direct control of the CLC.

6. (p. 5) On the 15 Subnets are we pen testing Desktops, Laptops, Servers, Virtualized Servers, Switches, Router/Firewalls, load balancers, spam filters etc.?
   See response to Vendor #4 – Question 4.

7. Are we Pen Testing the CLC Website?
   The ctlottery.org website is not within the scope of this RFP.

8. Are we Pen Testing any Web Applications CLC has?
   Web applications are not within the scope of this RFP. However the Successful Proposer should not exclude the webservers themselves from the penetration testing process.

9. (p. 5) In the RFP CLC mentions "ensure that appropriate security controls are implemented" is CLC referring to Technical IT Controls Only or as part of this engagement are we to include Administrative IT Controls, and Physical Controls in place, as well as perform a Risk Assessment of all IT Controls in place?
   This RFP is solely concerned with the technical details of the CLC networks and to validate the configuration/security of the CLC infrastructure.

10. (p. 6) Is the network configuration review a review of current documentation CLC possesses?
    The network configuration review is focused on the actual running configurations of routers and switches within the network, as well as the overall design of the CLC network.

11. (p. 6) Does part of the network configuration review include documenting in detail the CLC network?
    No

12. (p. 6) What is CLC currently using for IDS/IPS monitoring? (Hardware, or SAAS)
    The CLC is not prepared to disclose this information to Proposers at this stage of the procurement process. Information regarding the CLC's existing IT infrastructure relevant to the engagement will be shared with the Successful Proposer after contract execution.

13. (p. 6) Does the installation of a new IDS/IPS solution consider the services needed to properly tune such an environment over say a years' time to dial it in properly?

    The installation and initial configuration must be completed within 90 calendar days of the CLC receiving the IDS/IPS appliances. If the Successful Proposer determines it is necessary to continue to configure/tweak the devices after installation, then this should be included in the submission.

Part VI. Special Provisions, Section E. CT DCP LICENSING; INVESTIGATION OF PROPOSERS. Pps 14-15

14. What is the process for obtaining CT DCP licensing?

    The Successful Proposer will be provided the contact information for the Connecticut Department of Consumer Protection to begin the licensing process following preliminary award. As part of this process, the DCP will perform a fiduciary and security background check of the Successful Proposer and its Key Persons performing the contract.

15. Does the licensing need to be in place prior to the bid?

    No

16. How can we determine if the licensing is already in place?

    To check the status of DCP licenses, visit https://www.elicense.ct.gov/Lookup/LicenseLookup.aspx.

C. CONTENT REQUIREMENTS. Tab 2: References. P. 8-9

17. If proposer utilizes a sub-contractor can the proposer reference and the subcontractor reference be for the same company?

    No

C. CONTENT REQUIREMENTS. Tab 9: Affidavits and Certifications. P. 12

18. If the OPM Ethics Form 5 is completed on Biznet is that sufficient or does CLC require the document be provided as part of the submission? It appears to the latter but wanted to double-check.

    Proposers must complete and submit all required forms with their submissions.

Vendor #27

External Infrastructure

1. Please tell us about your environment. The more contextual information that you provide the better.

   See response to Vendor #4 – Question 4.

2. How many hosts are accessible from the internet?

   See response to Vendor #4 – Question 4.

3. How many Carriers are in use?

   Two.

Internal Infrastructure

4. Please tell us about your environment. The more contextual information that you provide the better.
   See response to Vendor #4 – Question 4.

5. How many physical locations require attendance?
   All networks can be accessed via a connection at the Rocky Hill facility.

6. How many VLANs are in scope?
   See response to Vendor #4 – Question 4.

7. How many clients (i.e. desktops, laptops) are there in total?
   See response to Vendor #4 – Question 4.

8. How many servers, including physical and virtual, are in scope?
   See response to Vendor #4 – Question 4.

Firewall and Router Security Configuration Reviews

9. Number of Firewalls, routers and switches including brands/models
   See response to Vendor #4 – Question 4.

10. Is the requirement for a full firewall configuration review and/or a rulebase review?
    The network configuration review is focused on the actual running configurations of routers and switches within the network, as well as the overall design of the CLC network.

11. Number of rules per rulebase (per firewall in scope)
    Not Applicable.

12. Please specify whether it will be sufficient to assess one Firewall in a pair, where applicable.
    Not Applicable.
13. Please confirm that we can gain access to the Firewall console to assess the configuration
    Not Applicable.

<u>Vendor #28</u>

Internal Network

1. How many hosts are present? (Workstations, servers, network printers, etc.)
   See response to Vendor #4 – Question 4.

2. How many network devices are present? (Routers, switches, multiplexers, etc.)
   See response to Vendor #4 – Question 4.

3. Do you have any BMS/ICS devices present? (This would include building management systems, HVAC system type of devices?
   The computer room HVAC systems are networked to provide SNMP monitoring.

4. How many asseets/systems/data are in scope to be assessed?
   See answrer to Vendor #4 – Question 4.

5. Is network access control (NAC) used?

   The CLC is not prepared to disclose this information to Proposers at this stage of the procurement process. Information regarding the CLC's existing IT infrastructure relevant to the engagement will be shared with the Successful Proposer after contract execution.

6. Network protection – Are there any network based firewalls and other security devices or services?

   See response to Vendor #4 – Question 4.

7. Host protection – Any host-based security such as firewalls, antivirus, IPS, etc.

   The CLC is not prepared to disclose this information to Proposers at this stage of the procurement process. Information regarding the CLC's existing IT infrastructure relevant to the engagement will be shared with the Successful Proposer after contract execution.

8. What do you consider as the most safeguarded data? (This could be your intellectual property, financial data, build on materials?

   The CLC is not prepared to disclose this information to Proposers at this stage of the procurement process. Information regarding the CLC's existing IT infrastructure relevant to the engagement will be shared with the Successful Proposer after contract execution.

9. Target sensitivity – Are there any legacy or other sensitive hosts that the consultant should be aware of?

   The CLC is not prepared to disclose this information to Proposers at this stage of the procurement process. Information regarding the CLC's existing IT infrastructure relevant to the engagement will be shared with the Successful Proposer after contract execution.

10. Maintenance windows - Are there any periods the consultant should be aware of such as patching windows, etc.?

    The CLC performs patching of all systems/equipment at scheduled periods. The CLC will suspend any patching/upgrades during the network scanning/testing.

11. Does the network segmentation exist? – Please describe the segmentation.

    The CLC is not prepared to disclose this information to Proposers at this stage of the procurement process. Information regarding the CLC's existing IT infrastructure relevant to the engagement will be shared with the Successful Proposer after contract execution.

12. Do you require a consultant to be on site? Recommend hotel, dress code and location.

    The Successful Proposer will need representation on-site at the Rocky Hill facility per the conditions set out in the RFP Part III. REQUIREMENTS & SPECIFICATIONS.

    a. If not, can you import a remote testing VM?

       Under no circumstances is any device or software to be installed in the CLC network.

    b. Please specify which hypervisor you are using. (ESXi, etc.)

       The CLC is not prepared to disclose this information to Proposers at this stage of the procurement process. Information regarding the CLC's existing IT infrastructure relevant to the engagement will be shared with the Successful Proposer after contract execution.

13. If not, we will need a shipping address and PoC to ship our remote testing hardware.

    Not Applicable.

14. Is there any additional information that the consultants should know prior to testing?
    The CLC will finalize the scope of work and goals and objectives with the Successful Proposer prior to contract execution.

External Network

15. How many internet facing live hosts are in scope? (Provide individual IPs, host names, domains, and/or ranges)
    See response to Vendor #4 – Question 4.

16. What times would you like the assessments to take place? (Business hours are preferred, however afterhours can be accommodated.)
    External penetration testing/scans can be performed anytime. Internal vulnerability scans and penetration tests will be performed during normal business hours (8:30am-4:30pm M-F, excluding holidays). The CLC will aid in selecting secondary servers to start with that will not impact the production environment. Based on the level of disruption to the network/systems it may be necessary to schedule specific times.

17. Are any of these systems hosted by 3rd parties? (Amazon AWS or similar)
    Cloud services are beyond the scope of this engagement. All systems in scope are on premise under direct control of the CLC.

18. What goals should the consultant consider? (i.e. obtain access to the internal network, or access to a user database, etc.)
    The CLC defers targets/goals of a penetration test to the Proposer. All testing must be done without damaging or destroying CLC systems or data and where all remote system scanning, and attempts to exploit vulnerabilities or escalate privileges are conducted with proper care to avoid any disruption of service. In the event that a system is breached, a screenshot with a listing of files or database tables will be considered adequate evidence of access. Under no circumstances is the Successful Proposer to remove, copy, alter, or compromise any data of any kind from CLC's systems.

19. What testing, if any, is off limits? (such as accessing the internal network)
    All testing must be done without damaging or destroying CLC systems or data and where all remote system scanning, and attempts to exploit vulnerabilities or escalate privileges are conducted with proper care to avoid any disruption of service. In the event that a system is breached, a screenshot with a listing of files or database tables will be considered adequate evidence of access. Under no circumstances is the Successful Proposer to remove, copy, alter, or compromise any data of any kind from CLC's systems.

20. Is the network part of a production environment?
    The testing will be done on the production environment.

21. If the network is in a Dev environment, should the consultant validate it against the production environment?
    Not Applicable.

22. Is there any additional information that the consultant(s) should know prior to testing?

The CLC will finalize the scope of work and goals and objectives with the Successful Proposer prior to contract execution

Vendor #29

General

1. Have you previously performed penetration assessments in the past?
   The CLC has previously enlisted third-party vendors to perform different types of security scans/assessments.

   a. Describe the type of penetration assessments that were performed.
      The CLC is not prepared to disclose this information to Proposers at this stage of the procurement process. Information regarding the CLC's existing IT infrastructure relevant to the engagement will be shared with the Successful Proposer after contract execution.

   b. When was the assessment last conducted?
      The CLC is not prepared to disclose this information to Proposers at this stage of the procurement process. Information regarding the CLC's existing IT infrastructure relevant to the engagement will be shared with the Successful Proposer after contract execution.

2. The RFP states that portions of the engagement have to be performed onsite at the Rocky Hill location. Given the current environment, is it an option to utilize tools to perform internal testing from a remote location?
   Refer to the "Clarifications" section of this document (page 1). This is a collaborative effort. The CLC will accommodate the Successful Proposer with a workstation and network connection at the Rocky Hill facility after Connecticut's "Shelter-In-Place" order expires and the CLC has lifted public access restrictions to its headquarters. When appropriate, the Successful Proposer will be required to physically plug into the network at the CLC's Rocky Hill facility and attempt to gain access to systems, files and data mimicking an attacker with internal network access with no credentials. This testing must be performed on-site per RFP section Part III. REQUIREMENTS & SPECIFICATIONS. All networks can be accessed via a connection at the Rocky Hill facility.

Internal Penetration Assessment

3. Approximately how many of the 350 total devices mentioned within the RFP will be tested as part of the internal penetration testing?
   a. Approximately how many of these devices are internal servers, workstations, and/or networking devices?
      See response to Vendor #4 – Question 4.

4. Will onsite physical security testing be in scope for this engagement?
   Physical security is outside the scope of this RFP.

External Penetration Assessment

5. Approximately how many of the 350 total devices mentioned within the RFP will be tested as part of the external penetration testing?
   See response to Vendor #4 – Question 4.

a. How many of these externally facing targets are running web services (HTTP and HTTPS)?

The CLC is not prepared to disclose this information to Proposers at this stage of the procurement process. Information regarding the CLC's existing IT infrastructure relevant to the engagement will be shared with the Successful Proposer after contract execution

Are any of the external systems in scope hosted by a third party?

No

6. Are both authenticated and un-authenticated (anonymous) web application testing requested?

Web applications are not within the scope of this RFP. However, the Successful Proposer should not exclude the servers hosting the web services from the penetration testing process.

7. Is email/phone security awareness testing in scope for this assessment?

Email/phone security is outside the scope of this RFP. However, the Successful Proposer should not exclude the servers hosting email/phone services from the penetration testing process.

New IDS/IPS Appliance Installation

8. Is there an IDS / IPS already in place? If so, what solution is being used?

The existing IDS/IPS solution will be replaced with the new solution.

9. Does the CLC already have a preferred IDS / IPS solution, and if so, what is the solution? If there is no preferred solution, how does the CLC prefer vendors approach scoping and pricing this section as the recommended approach for implementation may vary based on the recommended solution?

The Successful Proposer must recommend IDS/IPS devices that it has experience with that will meet the needs of the CLC. The Successful Proposer may, but is not required to, submit pricing for the purchase of the IDS/IPS appliances. It is a requirement that the devices are installed and configured by the Successful Proposer, and that CLC IT staff is trained on how to use them.

10. The RFP states that "The CLC's procurement of appliances is not included in this RFP…" Does this mean the CLC will be responsible for procuring the recommended IDS / IPS appliance?

The Successful Proposer must recommend IDS/IPS devices that it has experience with that will meet the needs of the CLC. The Successful Proposer may, but is not required to, submit pricing for the purchase of the IDS/IPS appliances. It is a requirement that the devices are installed and configured by the Successful Proposer, and that CLC IT staff is trained on how to use them.

a. The RFP asks for quotes for the installation of a new IDS / IPS appliance "…within ninety (90) days of the CLC receiving the recommended IDS/IPS appliances." How long does the CLC anticipate the procurement process for licensing the recommended tool taking?

Procurement of new IDS/IPS appliances could take several weeks, depending on the total price of the devices, as well as the availability of the devices themselves.