NYeC
NEW YORK eHEALTH COLLABORATIVE

NYeC

HITRUST & HIPAA Security Assessments RFP

Questions & Answers

HITRUST

For the HITRUST Assessments—to be submitted by 10/22/2023

1. How many, if any, Corrective Action Plans (CAPs) did NYeC have coming out of its 2022 Validated Assessment?
    - We have not yet received the final report for our 2022 assessment, but we expect less than 20 CAPs.
2. How many control statements were in the scope of NYeC's 2022 Validated Assessment?
    - Approximately 1,000
3. Are there any planned material changes to the scoped environment, either prior to or after, the HITRUST Interim Assessment in 2023?
    - Yes
4. Will NYeC be open to using the recently announced HITRUST version 11?
    - We anticipate that NYS DOH will require that NYeC use HITRUST version 11, but that has not yet been confirmed.
5. Are measured and managed scoring utilized in your current HITRUST assessment?
    - No
6. Is the assessment option "include privacy controls" marked as "yes" or "no"?
    - No
7. Is there just the one HIE platform/system in-scope per the "scope of the assessment" within MyCSF?
    - Yes
8. How many facilities are listed in MyCSF as in-scope locations?
    - Two locations
9. Could you provide an output from the "Factors" page in your MyCSF Validated Assessment so that we might confirm the # of requirements and view them within our sandbox?
    - NYeC will provide this information to the winning bidder.

10. How many requirement statements were in scope during the last HITURST validated assessment?
    - See Question 2
11. How many corrective action plans were identified during the last validated assessment?
    - See Question 1
12. How many facilities\locations are in scope for HITRUST?
    - See Question 8
13. Are cloud providers, such as AWS, Azure, or others in scope for the assessment?
    - Not for now, but it will be part of the next full assessment.
14. Does NYeC think the DOH will require certification against version 11 (being released soon) of MyCSF for the next validated assessment?
    - See Question 4.
15. Are we just bidding on the 2023 Interim Assessment Services?
    - The winning bidder would enter into a Master Services Agreement (MSA) with NYeC, and the 2023 services would be covered by a Statement of Work under that MSA. If the engagement extends beyond 2023 (based on, for example, factors such as performance), additional Statements of Work would be negotiated under that MSA.
16. If so, how many CAPs were issued in 2022 for 2023 Interim Assessment?
    - See Question 1.
17. How many requirements are in current HITRUST certification scope?
    - See Question 2.
18. What are all scoping factors?
    - For information on scoping requirements for NYeC's 2022 HITRUST assessment, please see Appendix A to the RFP.
19. How many locations are in-scope?
    - See Question 8

HIPAA

For the HIPAA Security Assessments—to be completed by 09/15/2023

1. How many internal hosts does NYeC have?
    - Approximately 200
2. How many live external IPs does NYeC have?

- Less than 20

3. For the external penetration test, would NYeC like a second round of confirmatory testing to ensure any vulnerabilities found in the initial test have been remediated?
    - Yes
4. For the internal and external vulnerability assessment, does NYeC require just vulnerability scans of the environments or a more detailed review?
    - NYeC seeks a more detailed review with remediation guidelines and comparative reporting to measure the progress.
5. Are wireless networks in scope for internal testing?
    - Yes
6. How many systems/IPs are in scope for vulnerability scanning and penetration testing activities?
    - Approximately 200
7. For internal testing, can all testing be conducted at one location, or will multiple locations need to be tested?
    - NYeC's Data Center and Cloud location must be tested.
8. For any external-facing web applications or API's, please provide the following:
    - Number of web applications in scope
        - Less than 10
    - How many static and dynamic pages will be assessed:
        - Less than 20 pages
    - How many API endpoints:
        - Less than 10
    - Do user roles need to be tested? If so, how many:
        - Approximately 150 domain users
9. Are any of these systems custom/in-house developed applications?
    - Approximately 5
10. Will a production or non-production environment be used for testing?
    - A non-production environment can be used for testing
11. Does NYeC require any social engineering tests, such as email, phone, or physical access testing?
    - No

NYeC
NEW YORK eHEALTH COLLABORATIVE

12. Can vulnerability scans and penetration tests be performed during working hours, or do they need to be performed after hours?
    - After hours is preferred
13. Does NYeC require a risk assessment that covers the HIPAA Privacy, Security or Breach Notification Rules?
    - Please see RFP for details. NYeC requires a HIPAA Security Risk Assessment
14. Provide details about the HIE platform, such as number and type of servers and databases, physical or virtual systems, or cloud-based
    - N/A
15. If physical systems are used, where are they hosted or how many data centers are used?
    - 2 (NJ, TX)
16. How many systems acquire, process, transmit, or store PHI?
    - Less than 20
17. How many IT, security, and compliance staff would be involved in meetings and walkthroughs?
    - Approximately 5-10
18. What is meant by validation testing report due by March 31, 2024 on page 5 of the RFP?
    - NYeC seeks validation testing several months after the original pen test to help to track the progress if all findings have been remediated from the last scan.
19. Does NYeC wish to conduct a full Risk Analysis as described in §164.308(a)(1)(ii)(A) or is the scope limited to the technical assessment of vulnerabilities and penetration testing?
    - NYeC is interested in proposals that cover the requirements described in the RFP. Additional or expanded services may be the subject of negotiation with the winning bidder.
20. Does NYeC wish to include a gap assessment to review the organization's written policies, procedures, practices, and enforcement of the requirements of the Security Rule?
    - NYeC is interested in proposals that cover the requirements described in the RFP. Additional or expanded services may be the subject of negotiation with the winning bidder.
21. Does NYeC wish to include an assessment of the HIPAA Privacy and Breach Notification Rules?
    - NYeC is interested in proposals that cover the requirements described in the RFP. Additional or expanded services may be the subject of negotiation with the winning bidder.
22. What is the approximate number of IP addresses to be included in the scope of the internal vulnerability assessment?

- Less than 200

23. What is the approximate number of IP addresses to be included in the scope of the external vulnerability assessment?
    - Less than 20
24. What is the approximate number of IP addresses to be included in the scope of the penetration test?
    - Less than 220
25. Does NYeC wish to perform authenticated vulnerability scanning?
    - Yes
26. Does NYeC wish for the penetration test to be black box or white box?
    - External test should be Black Box test while internal test might be mixed.
27. Are there any web applications to be included in the penetration test? If yes, how many?
    - Less than 5
28. Does NYeC wish to include wireless network testing as part of the penetration test?
    - Yes, at corporate environment
29. Does NYeC wish to include social engineering as part of the penetration test?
    - No
30. Is there a preference to have the work completed on-site or remotely?
    - This is a factor that NYeC will negotiate with the winning bidder based on the circumstances in existence at the time of the assessment (e.g., COVID restrictions, etc.).
31. If on-site work is desired, how many physical locations are in scope?
    - NYeC has two corporate locations but see Question 30.
32. Would you prefer the vuln scanning and pen testing services separate from the actual risk assessment portion of the service?
    - Yes
33. Please see attached scoping questionnaire (see folder for document)
    - NYeC will discuss scoping details with the winning bidder.

SECURITY RISK

For the Security Risk Assessment on the HIE Platform based on NIST SP 800-30—to be completed by 07/15/2023

1. What is the IT infrastructure used to deliver your services? Please specify details if you can. - N/A
    - Network
    - Operating System
    - Database
    - Applications
2. Are you hosted on-prem, or in the cloud? If it is a hybrid model (most likely), please share the rough split.
    - Mostly on-prem, and in process of migrating some applications and DR site to cloud within couple of months.
3. How many IT assets does NYeC have?
    - Approximately 350
4. Is the HIE Platform a single application? If so, could you specify the number of user roles and dynamic pages?
    - N/A

34. Is the platform hosted internally or with a third party?
    - Internally
35. Please elaborate on NYeC's expectations for validation testing.
    - NYeC seeks validation testing by March 31, 2024 (several months after the initial testing) to confirm/test NYeC's remediation efforts.
36. Is NIST SP 800-30 the preferred risk assessment framework to be used for this portion of the project? We can use any of the standard risk assessment frameworks you prefer.
    - Yes, please see RFP for details.
37. Please see attached scoping questionnaire
    - NYeC will discuss scoping details with the winning bidder.

OTHER

1. In section VI, the last date says, "Validation testing—Results/reports due to NYeC by March 31, 2024." What is this referring to?
    - NYeC seeks validation testing by March 31, 2024 (several months after the initial testing) to confirm/test NYeC's remediation efforts.

2. The Security Assessment tasks need to be done annually to maintain HITRUST. Would you like us to include "Option B" pricing for two years, 2023 and 2024?

- The winning bidder would enter into a Master Services Agreement (MSA) with NYeC, and the 2023 services would be covered by a Statement of Work under that MSA. If the engagement extends beyond 2023 (based on, for example, on factors such as performance), additional Statements of Work would be negotiated under that MSA.

3. Can you please provide the following information so we can more accurately quote the network testing services you've requested?
    - How many external IPs, domains or subdomains are in scope?
        - Less than 20
    - Will the selected firm be added to any perimeter allow lists?
        - Yes, for internal scanning
    - Will the external vulnerability assessment be completed at the same time as the external network penetration test?
        - Yes
    - How many internal subnets will be in scope?
        - N/A
    - Will the selected firm be provided domain credentials for scanning?
        - Yes
    - Can the internal assessment be done remotely?
        - Yes

4. Should the HIE Platform Assessment also be performed under the HHS Risk Analysis Guidelines? www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html
    - The assessment should be performed using a standard risk assessment framework such as NIST SP 800-30 NIST Risk management.

5. Regarding the page limit: Is the 10-page limit for each option?
    - Do we need to prepare separate proposal for each option? (Since we are proposing for both options, 10 pages will not allow the space to describe both approaches and plans – would an additional 5 pages be acceptable if providing a single proposal for both options?)
        - Yes
    - Are cover letters and the table of contents included in the page count?
        - Cover letters and table of contents will not count in the 10 page limit.
6. Is it acceptable to provide the proposal in PDF format in addition to (or instead of) the Word format? Our document templates are very customized and we fear that our

formatting may not appear correctly. We notice we lose formatting if viewing our document in Word via a browser or in Teams for instance. Additionally, we will only be able to provide work samples in PDF format as we redact client information and have separate templates for reports that conflict with our proposal template.

- Yes, vendors may submit their proposal in PDF format in addition to Word format.

7. The fourth bullet point in Section IV (Eligibility Criteria) mentions a vendor contract. Can NYeC provide this document to bidders?

   - NYeC will provide this document to the winning bidder.

8. Paragraph 1 in Section VI (Scope of Work) states "Proposals must clearly detail the vendor's approach for December 2022 NYeC HITRUST Assessor & Security Testing submitting NYeC's validated HITRUST assessment by its annual certification expiration date (October 22) and/or completing its Security Risk Assessments within a timeframe that enables NYeC to report out to NYS DOH to meet its contractual deliverables."

   It would seem this request would not be applicable to firms bidding on Option B only. Please confirm or clarify.

   - The second part of the sentence is applicable to firms bidding on Option B only ("…and/or completing its Security Risk Assessments within a timeframe that enables NYeC to report out to NYS DOH to meet its contractual deliverables.").

9. Does NYeC have a preference to hire one firm that can conduct both Options A and B?

   - The RFP is designed to accommodate both options (one firm that can conduct both, or two separate firms).

10. Section VII (Contents of Proposal), Item 3 (Cost) requests a "detailed budget." Please provide more information on the level of detail you are seeking from bidders in the cost section of the proposal.

    - NYeC seeks a detailed budget outline for the complete scope of the project (Option A and/or B) that will permit an analysis of the reasonableness of the cost estimates.

11. Has NYeC conducted this work before? If yes:
    - When were these projects most recently conducted?
      - Annually since 2018
    - What firm(s) conducted the work?
      - This question is not relevant to the RFP and the ability to submit a proposal.