Solicitation Amendment / Modification

1.	Solicitation No.	02102025/ET
2.	Solicitation Name	Annual IT Risk Assessment
3.	Issue Date	February 10, 2025
4.	Closing Date	March 14, 2025
5.	Solicitation Amendment No.	1
6.	Solicitation Amendment Date	February 27, 2025

7. The above numbered solicitation is amended as set forth in Item 9 below.

8. The hour and dates specified for receipt of proposals/quotations: ☒ is not extended; ☐is extended as described in Item 9 below.

9. Description of Amendment/Modification:

The purpose of this solicitation amendment is to inform prospective offerors/bidders that the above numbered solicitation is hereby amended to provide responses to questions as follows.

1. Is the NIST 800-171 rv 2 assessment in lieu of preparing for a CMMC certification?

Our recent contract does not have the new CMMC v2 language requirements, but DFARS 252.204-7012 is required and something that we complied with.

2. Is there more than one environment that would be in scope for this RFP, or is it one single environment that will cover all of IIE's infrastructure and programs?

One system resides in AWS, all other systems are found in one of our Microsoft tenants/ecosystem.

3. Can we know how many endpoints you have in scope?

Most major systems (approximately 4) are SaaS, we have one system we are responsible for in AWS, less than ~900 endpoints in total servers/laptops.

4. The RFP mentions that the audit may be carried out remotely. Does this mean that IIE does not have any physical CUI or printers on its premises?

CUI is digital**.**

5. Besides the general outline of how the proposal must be presented, is there a particular format that we must adhere to? Is there a sample template that you can provide us?

Reference the RFQ posting.

6. For the Infrastructure Security Assessment, will IIE please identify the counts and types following devices to fully understand the scope:

Servers Physical/virtual -100 total, ~10 in scope other systems are SaaS
Workstations – 650 total,
Routers - 12 total, ~4 in scope
Firewalls - 15 total, ~9 in scope
Wireless access points and SSIDs – 91 – 29 total, 54 – 11 in scope
AD Domains- One AD and One Azure will be 2 Azure
Other devices (IP Phones, IOT, Printers, etc.)

7. Is IIE expecting baseline compliance scanning against server and end-point infrastructure devices?

No.

8. For the Infrastructure Security Assessment, will IIE please identify the cloud infrastructures are in use.

Primarily Azure and AWS.

9. For the Penetration Testing Assessments, is the penetration testing limited to web applications or are external and internal penetration testing in scope?

For the Assessment, just web applications, but are also interested in external and internal penetration testing.

10. For the 25 web-facing applications how many static, dynamic, forms and user roles expected to be tested?

No user testing is expected.

11. For the API testing, will IIE please define how many APIs are in scope and whether they are part of the 25 web-facing applications identified for penetration testing?

Websites are separate to the API.

12. Does IIE have a system security plan that outlines implementation of NIST SP 800-171r2 controls?

Yes.

13. While preference will be given to CMMC Third Party Assessment Organizations, will IIE consider Registered Practitioner Organizations with relevant experience?

Yes.

14. Will vendors without a current ISO 27001 certification or SOC 2 type 2 be considered to participate in this procurement activity?

Yes, but must past our security questionnaire risk assessment.

15. Will IIE please provide the offline IT Security Questionnaire? If not, will IIE please provide the link to access the IT Security Questionnaire?

We will provide post-award.

16. Regarding annual renewal, is IIE expecting a cost proposal to include base year and 4 option years?

Yes, first year expect to do everything, but we intend to do additional annual security reviews annually for example some years you may only do technical penetration testing and other full risk assessments.

17. Can you provide more details on the current maturity level of your information security program?

Level 2.

18. Are there any specific compliance deadlines for CMMC 2.0 or NIST 800-171v2 that we should be aware of?

No.

19. Do you have a list of in-scope assets, including applications, networks, cloud environments, and endpoints, that need to be assessed?

Yes.

20. Are there any third-party vendors or external systems that interact with your infrastructure that should be included in the assessment?

Yes, most systems in scope are SaaS products.

21. What level of evidence collection and documentation do you expect for CMMC 2.0 and NIST 800-171v2 compliance validation?

Appropriate documentation.

22. Are you currently using a GRC Platform? If so, which one?

No.

23. How do you currently track Plan of Action & Milestones (POA&M) and SPRS (Supplier Performance Risk System) scores?

Spreadsheet.

24. Are there any specific concerns or known vulnerabilities within your IT infrastructure that should be prioritized?

No.

25. Can you confirm the number of web-facing applications (25) and application interfaces (6) included in penetration testing?

We currently have under 25 websites and 6 APIs.

26. Do you have any testing restrictions (e.g., production systems, off-limits assets) that we should be aware of?

No.

27. Would you like internal penetration testing in addition to external testing?

This may be something that we would like to be done.

28. Are there any industry-specific compliance requirements (e.g., HIPAA, GDPR) that should be considered during the security testing?

CMMC and NIST 800-171.

29. What is your expected timeline for completing the risk assessment and penetration testing?
We believe the assessments should take 1 to 2 months.

30. Who are the key stakeholders we will be working with during the engagement?

Security, IT Operations, and Program team.

31. What level of weekly reporting and progress updates do you expect?

Reference RFQ.

32. How many departments should be targeted for interviews in the program assessment?

For those necessary, we expect up to 3.

33. How many policies are to be evaluated?

Those necessary for CMMC.

34. Have you already gone through a CMMC analysis?

Yes.

35. How many:

a. Routers are in-scope?

- ~4

b. Firewalls are in-scope?

~9.

c. Servers are in-scope?

~10, others are SaaS.

d. Endpoints are in-scope?

650.

36. Application sizes:

a. How many target URLs are there?

Under 25 websites.

b. What are the functions of each of the applications?

Financial System, CRM, Data Warehouse, Application Submission System, Program Websites.

c. What is the size of each of the applications?

Unknown.

d. Would you like any applications tested without credentials?

Yes.

e. Would you like any applications tested with regular credentials?

No.

f. Would you like them tested with admin credentials?

No.

g. Are there any e-commerce capabilities?

No.

37. How many APIs are to be tested?

Up to 6.

38. Do you want your Incident Detection System tested?

It can be

39. For the first year there will be no year over year comparisons unless you have a previous one. Do you have a previous one?

We do.

40. Have you previously established an account with SAM to submit your SPRS score or will we need to work with you to establish the account?

We have submitted our SPRS scores.

41. Is the IT Security Questionnaire to be submitted with our proposal or post-award?

Post Award.

42. Have you conducted a CMMC maturity assessment in the past and if so, what is the current CMMC maturity level of the current information security architecture/program as it relates to NIST 800-171 v2?

Level 2, one system in AWS that would require Nist 800-171 others are SaaS.

43. In what environments would penetration testing be conducted (e.g., production, development, staging, user acceptance testing, etc.)?

Production.

44. Since testing will be performed remotely, will there be specific security requirements or Virtual Private Network (VPN) or Virtual Desktop Interface (VDI) needed for the remote connectivity? Will client-owned equipment(laptop) be provided?

VPN, VDI and equipment maybe be made available.

45. Has any prior technical penetration testing or assessment activities been conducted? If so, please describe.

Yes, internal API scans and external penetration testing.

46. Will there be specific communication tools or platforms used during the assessment such as Microsoft Teams, Slack or Jira?

We use Teams.

47. Our company is not currently a C3PAO, but we are in the process of becoming a C3PAO and we have team members who hold various levels of CMMC certifications. Will this status reduce the value your team will apply to our response and capabilities to assist you in this effort?

No.

48. Does the entity have an up-to-date asset inventory? If so, will this be shared, or accessible once assessment activities begin?

Yes.

49. As per the Statement of Work, you have requested 25 web facing applications. What technology is used to develop and maintain these applications?

Wordpress, Drupal, Joomla

50. Could you please provide more details about the 6 interfaces that need to be pen tested. Are these custom interfaces, out of box or black box interfaces?

Integrations between our systems, CRM to DB, CRM to Financial System, Financial System to Data Warehouse, CRM to Application System and CRM to other applications

51. Could you help provide more details around the APIs?

CRM to Financial System is SOAP API, CRM to Data warehouse is REST, CRM to Application System is REST and CRM to some (3) other applications are REST primarily for data transfers.

52. Are any containers or serverless computing services in scope for assessment? If so, how many, and what types are in the environment?

No.

53. Is credentialed or non-credentialed testing required?

No.

54. Are there any limitations on the timing of performing these penetration tests? For example, only outside of business hours.

No, to be agreed upon.

55. Does the organization have existing pen testing tools that the vendor may utilize or is the vendor expected to bring their own?

Bring your own tools.

56. Are there any specific methodologies or frameworks the organization prefers for penetration testing?

No.

57. What cloud services are currently in use (e.g., AWS, Azure, GCP)?

Primarily Azure and AWS.

58. Is there a specific security or application engineering team that the vendor will be working with?

Yes.

59. Are there any specific policies, procedures, or standards that have been recently updated for your organization?

We update our policy as needed.

60. Please clarify the total number of pages acceptable for the Technical Proposal? The implementation work plan is limited to five pages total, yet sections 1-6 indicate two pages per section, equating to 10 pages total?

Response should not be longer than 5 pages, and any section should not exceed 2 pages.

61. Please clarify the Technical Approach page limit (page 8). Are we supposed to submit two pages or four pages?

"Technical Approach: In a narrative – not to exceed four (2) pages – the Offeror will demonstrate its understanding, ability and overall approach to performing the requirements described in the Scope of Work, Activities & Tasks and Deliverables." - response should not be longer than 5 pages, and any section should not exceed 2 pages**.**

62. Please clarify the Capability Statement page limit (page 8). Is it two or three pages?

"Capability Statement: A narrative – not to exceed two (2) pages... CVs are not included in the 3-page length limit." response should not be longer than 5 pages, and any section should not exceed 2 pages

63. Are there any related initiatives or dependencies that we need to be aware of?

No.

64. Is there an incumbent providing similar services to IIE? If yes, is the incumbent performing to the satisfaction of IIE, and the Chief Executive Officer, Chief Administrative Officer, and/or Chief Technology Officer?

Yes, we are looking for a new party for these assessments.

Is the incumbent eligible to bid on this contract?

We are looking for a new party to conduct these assessments.

65. Will Vendors be permitted to use non-United States Citizen team members to perform and/or support any and all Annual IT Risk Assessment and Technical Testing activities?

No.

66. Will Vendors be permitted to use off-shore teams (Not physically located in the United States) to perform and/or support any and all Annual IT Risk Assessment and Technical Testing Activities?
Yes.

67. Will Vendors be permitted to use offshore teams (Not physically located in the United States) to perform and/or support any and all Annual IT Risk Assessment and Technical Testing Activities through an onshore terminal, server, or data center?

Yes.

68. Will Vendors be permitted to use non-United States Citizen team members (physically located in the United States) to perform and/or support any and all penetration testing activities?

Yes.

69. Will Vendors be permitted to use off-shore teams (Not physically located in the United States) to perform and/or support any and all penetration testing activities?

Yes.

70. Is our understanding correct that this Annual IT Security Risk Assessment is being used to prepare for being assessed by a C3PAO and meet CMMC Level 2 at a later date and time of IIE's own choosing?

Yes.

71. Is our understanding correct that this engagement is NOT to be assessed by a C3PAO to achieve CMMC Level 2 Certification?

Correct.

72. Could you share the number of security policies that have been drafted, written, and/or approved?

We have several security policies that have been produced and believe have all required policies for the assessment.

73. Could you share the number of system security plans that have been drafted, written, and/or approved?

We have one for this assessment.

74. Given the limited, finite, number of CMMC Third Party Assessment Organizations (C3PAOs), and that there are far more CMMC Certified Assessors (CCA), would you be willing to consider giving the same preference to organizations with a team member holding a Cyber AB CCA Certification and that are not C3PAOs for this engagement so that one is not limiting who they can be assessed with when it is time to be assessed? Especially since one is likely looking for the talent with both knowledge and skill versus an organization that houses the talent?

Yes.

75. Could you share what brand routers, firewalls, and wireless access points are being used?

Yes,to disclose later.

Could you also share how many routers, firewalls, and wireless access points are being used?

Yes. Answered in our question.

Could you share if the routers, firewalls and wireless access points are currently being managed in house by IIE or by an external third-party managed IT or managed service provider?

Yes, managed by both.

76. Could you share the number of servers and the number end-point infrastructures IIE is using?

Less than 900.

77. Could you share who IIE's cloud service providers are?

Microsoft Office 365, TeamViewer, OneTrust, Microsoft and AWS, etc.

78. Could you share what prior internal CMMC projects or work have been done or may be in progress?

N/A

79. Has IIE located where Controlled Unclassified Information resides in IIE's information systems?

Yes.

80. For penetration testing assessments, could you list the 25 web facing applications' URLs?

To be disclosed later.

81. For each of the 25 web facing applications, were these application custom developed externally, custom developed in house, commercial off the shelf or commercial off the shelf with some customizations developed inhouse or by a third party? If these applications have been tailored or custom developed, could you share what programming language they were written in?

COTS with some customizations

82. Are these 25 application penetration tests only from only an unauthenticated (no username/passwords provided) web application penetration test?

Yes.

Is IIE looking to test from the perspective of multiple roles to see what vulnerabilities exist from having limited authorized access? If yes, how many roles?

No.

83. Because of how the RFP is formatted, we are assuming that these six application interfaces differ from the Application Programming Interface (API) Testing bullet point. To that end, for penetration testing assessments, could you share what are these six application interfaces are, and what their business functions are?

These are primarily used for data transfers. CRM to DB, CRM to Financial System, CRM to Application System and CRM to some (3) other applications.

84. For penetration testing assessments, where are the 25 web facing applications hosted?
Different locations

Are they hosted on premise?

Some are hosted by us in Azure.

Are they a Software as a Service (SaaS) Solution?

Yes.

Are they hosted on a public cloud managed by IIE?

Yes.

85. As part of the server and endpoint infrastructure hardening review, is there an expectation that an internal and external network penetration test be performed to assess the underlying network infrastructure, servers and end points?

No, but we may want to request such testing.

86. For penetration testing assessments, could you share how many application programming interfaces endpoints are there for each application? The number should include both public and private APIs. Could you share if these are REST or SOAP APIs?

CRM to Financial System is SOAP API, CRM to Data warehouse is REST, CRM to Application System is REST and CRM to some (3) other applications are REST

87. For penetration testing assessments, could you share how many application programming interfaces endpoints are there for each application? The number should include both public and private APIs. Could you share if these are REST or SOAP APIs?

Private APIs , CRM to Financial System is SOAP API, CRM to Data warehouse is REST, CRM to Application System is REST and CRM to some (3) other applications are REST.

88. Our understanding is that this engagement is an IT Risk Assessment and Technical Testing. If the vendor is processing proprietary data or personal data, we believe requesting an ISO27001 and/or a SOC2 is reasonable as that vendor would be embedded as part of IIE's operations. However, in IT Risk Assessment and Technical Testing, the vendor is not embedded as part of IIE's operations and it will likely not be processing proprietary or personal data. To that end, we wondering if IIE would reconsider this requirement. –

We do; you will be asked to answer our security questionnaire for a risk assessment.

END OF AMENDMENT