Request for Proposals

Penetration Test

Delivering solutions that put people first.

12/28/2023

PROPRIETARY AND CONFIDENTIAL

Contents

Introduction

Noridian Healthcare Solutions, LLC (Noridian) invites qualified offerors, with special consideration given to small businesses, to submit a proposal to this Request for Proposals (RFP) to provide a security assessment that will allow it to:

1. Gain a better understanding of potential corporate network vulnerabilities associated with Noridian's externally facing network architecture.
2. Evaluate the internal security posture of Noridian by identifying potential internal vulnerabilities within Noridian's network.
3. Assess compliance with the CMS FISMA Assessment (FA) control objectives described in this document. All of the FA controls are listed in the CMS Information Security (IS) Acceptable Risk Safeguards (ARS), however, Noridian must only test a subset of the controls annually and the controls to be tested during this engagement are detailed in this document. Please see the Reference Websites section for a link to the ARS.

Noridian is seeking to identify and select an independent organization to perform the activities listed above. It is the intention of Noridian to award the winner a contract for one year for the security assessment. The remainder of this document provides additional information that will allow a service provider to understand the scope of the effort and develop a proposal in the format desired by Noridian.

Offerors are advised to pay careful attention to the language used throughout the RFP. Failure to satisfy a term, condition, or requirement of this RFP may result in an unresponsive proposal.

Company Background

Noridian Healthcare Solutions, LLC (Noridian), a wholly owned subsidiary of Noridian Mutual Insurance Company, develops solutions for federal, state, and commercial health care programs through a full suite of innovative offerings, including claims processing, medical review, and contact center and provider administrative services. Noridian has served as a government claims contractor for Medicare since the federal program's inception in 1966. The company is headquartered in Fargo, N.D., and employs approximately 2000 staff throughout the country.

Response Requirements and Timeline

Form of Final Agreement and Offeror's Representations

By submitting a proposal to this RFP, each offeror agrees that, if selected to provide services, it will agree to and comply with all Noridian security requirements and evaluation parameters. All material submitted in response to the RFP by the successful offeror, as well as the RFP itself, may be incorporated as part of the final contract.

If at any time between submission of an offeror's proposal to this RFP and final selection of an offeror, the offeror finds it necessary to modify any aspect of its proposal, the offeror must notify Noridian immediately, in writing to the Contact Person(s) identified below, of the offeror's intent. Failure to do so may result in the rejection of the offeror and selection of an alternate.

By submitting a proposal to this RFP, each offeror represents that:

- Offeror has read and understands the RFP, and the offeror's proposal is made in accordance therewith.
- Offeror's proposal is based upon materials, systems, and equipment required by the RFP with any exceptions clearly noted in offeror's proposal.
- Offeror is not presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from covered transactions by any Federal or State department or agency; and
- Offeror does not have any conflicts of interests that would prohibit it from entering a contract with Noridian for the services or solutions described in this RFP.

Contact Information

Any correspondence regarding this RFP, including questions, responses, etc. must be directed in writing to:

rfp@noridian.com

Subject Line: RFP - 2024 Penetration Testing

Attn: Marissa Paulson and Tara Odden

Noridian personnel other than the Contact(s) listed above are not authorized to discuss this RFP with potential offerors before the Proposal Due Date and Time. Contact with any Noridian personnel not listed above may result in disqualification. Noridian will not be held responsible for oral responses to potential offerors regardless of the source. Noridian will respond to offerors' questions in writing.

Proposal Due Date

Proposals are due on or before **5:00pm CST on March 8, 2024,** by submitting a proposal via email to the Contact(s) identified above.

Any proposal(s) received after the specified Due Date and Time will be considered late and non-responsive, unless otherwise agreed to by Noridian. Noridian is not responsible for lost, misplaced, or misdirected proposals.

Tentative Timetable for Review Process

Event	Date
RFP release	January 17, 2024
Deadline for Offeror questions	February 9, 2024
Noridian responses to offerors' questions	February 23, 2024
Proposals due by 5:00 PM CT	March 8, 2024
Final selection of offeror	March 22, 2024

Other Key Dates

Event	Tentative Date
Initial kickoff meeting with vendor	April 1, 2024
Window for work to be completed during (formal exit conference with preliminary findings at the conclusion of onsite testing)	April 1, 2024-May 10, 2024
Issuance of Draft Report	May 20, 2024
Noridian Reviews Draft Report	May 24, 2024
Issuance of Final Network Security Report	May 31, 2024

Evaluation Criteria and Selection Process

Award of the contract(s) under this RFP will be based on the offeror's proposal that in Noridian's sole discretion will be the most advantageous to it in terms of cost, ability to meet requirements, and other factors as specified elsewhere in this RFP. Noridian reserves the right to:

- Reject all proposals and discontinue this RFP process without obligation or liability to any potential offeror.
- Accept other than the lowest priced proposal.
- Award a contract based on initial offers received without discussions or requests for best and final offers.
- At its discretion, and without explanation to any offeror, at any time choose to discontinue or modify this RFP without obligations to any offeror.

The final awarding of the contract(s) under this RFP is estimated to occur as described above in the RFP Timetable for Review Process.

The following criteria will be utilized when evaluating your response. This is not to be considered an all-inclusive list.

Description
Offeror's Profile ▪ Organization's experience in this space ▪ Customer history and relevance
Ability to meet the requirements
Offeror's acceptance of dates of work
Pricing/Cost

Terms and Conditions

All offers from Noridian are contingent on Noridian and the selected vendors' execution of a Master Services Agreement (Agreement) which will be provided by Noridian. The Agreement will replace any in-force or previously negotiated terms and conditions that may currently be in effect with an offeror(s). Noridian reserves the right to cancel the Agreement negotiation at any time if Noridian deems it to be in Noridian's best interests to do so.

Required government flow-downs and security requirements related to Noridian's government work are non-negotiable.

Technical Requirements

Noridian is requiring the assessment of the following:

- Independent external penetration test of all external firewalls, load-balancing devices, and web servers i.e. testing of public IP addresses.
- Internal and perimeter vulnerability testing to identify weaknesses/vulnerabilities and rate in accordance with National Institute of Standards and Technology (NIST) and Federal Information Processing Standards (FIPS) standards. Testing will be on systems with various operating systems including Windows, Linux, UNIX, and Novell. Testing will also include a random selection of workstations.
- Evaluate the configurations, related controls, and monitoring for Intrusion Detection and Prevention Systems and primary firewalls, routers, switches, and load balancers.
- Vulnerability and security weakness testing on externally facing internet applications and rate in accordance with National Institute of Standards and Technology (NIST), Industry Best Practices and Federal Information Processing Standards (FIPS) standards.
- Test the security of Noridian's external websites to identify weaknesses/vulnerabilities and rate in accordance with National Institute of Standards and Technology (NIST) and Industry Best Practices. Testing will be on all of Noridian's externally facing websites.

- If possible, assess compliance with the CMS control objectives described in this document and within each ARS control. All of the controls are listed in the CMS IS ARS, however, Noridian must only test a subset of the controls annually and the controls to be tested during this engagement are detailed in this document. Please see the Reference Websites section for a link to the ARS.
- Evaluation of security of the M365 environment

The testing will not be announced to IT operations. Noridian is looking for a semi-blind external penetration test and internal vulnerability/penetration test. Therefore, Noridian will provide additional details beyond this document once testing is complete, and evaluation begins.

During testing, control failures may be identified. Noridian may implement a fix to address these failures and will coordinate retesting of control findings as necessary with the vendor. The vendor will perform initial retesting as part of the statement of work. If a second retest is necessary, due to no fault of the vendor, the vendor will be compensated by Noridian for the additional labor incurred. No more than two (2) retests will be performed on any control. For the purposes of this RFP, a 15% control failure rate should be assumed.

All testing must be conducted from within the United States of America. No offshore testing, in whole or in part, is permitted.

Scoping Information

1. **External Penetration Test**

DC External:

Assigned network: 1x /25 subnet

Active IPs: ~25 with inbound access.

* NIST Documents that are of relevance:

SP 800-53 Recommended Security Controls for Federal Information Systems

SP 800-115 Technical Guide to Information Security Testing and Assessments

* FA Controls may overlap with this section, please price the work in this section and indicate the overlap in the FA section

2. **Internal and Perimeter Network Vulnerability Assessment and Penetration Testing**

Reserved network: /16 subnet

Assigned networks (approx.): 100

Testing of approximately 200 workstations, 10% of the total population, throughout the Noridian internal network

3. **Configuration review of 1 clusters of firewalls, 1 cluster of routers, and 1 sets of load balancers.**

* NIST Documents that are of relevance:

SP 800-53 Recommended Security Controls for Federal Information Systems

SP 800-115 Technical Guide to Information Security Testing and Assessments

4. **Intrusion Detection and Prevention Systems Review**

Review existing change controls, configurations, alerting and monitoring capabilities, and business process to receive appropriate information in a timely manner.

Host Intrusion Prevention System (HIPS) configuration, alerting and monitoring review

Network Intrusion Prevention System (NIPS) configuration, alerting and monitoring review

Event correlation, alerting and monitoring review

* NIST Documents that are of relevance:

SP 800-41 Guidelines on Firewalls and Firewall Policy

SP 800-53 Recommended Security Controls for Federal Information Systems

SP 800-92 Guide to Computer Security Log Management

SP 800-94 Guide to Intrusion Detection and Prevention (IDS) Systems

5. **Firewall Reviews**

Examine configurations of (2) Cisco ASA Firewalls and (1) Juniper Firewall from the Noridian Medicare Portal (NMP) environment and review existing change controls.

* NIST Documents that are of relevance:

SP 800-41 Guidelines on Firewalls and Firewall Policy

SP 800-53 Recommended Security Controls for Federal Information Systems

SP 800-94 Guide to Intrusion Detection and Prevention (IDP) Systems

* FA Controls may overlap with this section, please price the work in this section and indicate the overlap in the FA section

6. **Internet Facing Application In-Depth Vulnerability Testing**

In-depth testing of one internet facing applications for vulnerabilities and security risks

Noridian Medicare Portal (NMP) – Noridian's secure provider portal

* NIST Documents that are of relevance:

SP 800-53 Recommended Security Controls for Federal Information Systems

SP 800-115 Technical Guide to Information Security Testing and Assessments

7. **External Website Vulnerability Testing**

Number of website addresses in target:

Externally Accessed Domains: (25)

* NIST Documents that are of relevance:

SP 800-53 Recommended Security Controls for Federal Information Systems

SP 800-115 Technical Guide to Information Security Testing and Assessments

Proposal Submission

The deadline for proposals is on or before **5:00pm CST March 8, 2024.** Submit the proposal and the Offeror's Profile questionnaire via email to the contact below:

rfp@noridian.com

Subject Line: RFP – 2024 Penetration Testing
ATTN: Marissa Paulson and Tara Odden

Detailed Proposal Requirements

Vendor's proposal shall be submitted in several parts as set forth below. The Vendor will confine its submission to those matters sufficient to define its proposal, and to provide an adequate basis for Noridian's evaluation of the Vendor's proposal.

1. Executive Summary
2. Scope, Approach, and Methodology
3.Project Management Approach
4. Detailed and Itemized Pricing

5. Conflict of Interest
6. Appendix: *Sample Deliverable*
7. Appendix: *References*
8. Appendix: *Project Team Staffing*
9. Appendix: *Company Overview*

The detailed requirements for each of the above-mentioned sections are outlined below:

1. EXECUTIVE SUMMARY

This section will present a high-level synopsis of the Vendor's responses to the RFP. The Executive Summary should be a brief overview of the engagement and should identify the main features and benefits of the proposed work. All deliverables must be Section 508 compliant.

2. SCOPE, APPROACH, AND METHODOLOGY

Include detailed testing procedures (including testing tools utilized) and technical expertise by phase. Testing and analysis will be performed in accordance with CMS guidelines and NIST SP800-115 Technical Guide to Information Security Testing and Assessment. Specifically, any terminology utilized within the proposal should be based on the NIST special publication previously mentioned. It is important to note that NIST SP800-115 defines penetration testing to include validation of all vulnerabilities. **This must be part of the selected Vendor's scope, approach, and methodology in order to eliminate the potential for false positives during the reporting process.**

This section will act as the Statement of Work (SOW) to be used as a guideline by the consultants during the security testing. This section should include a description of each major type of work being requested of the vendor. The proposal should reflect each of the sections listed below.

• External Penetration Test
• Internal and Perimeter Vulnerability Assessment and Penetration Testing
• Intrusion Detection and Prevention Systems Review
• Firewall Reviews
• Cloud Security Testing (M365)
• External Facing Application Testing
• External Website Vulnerability Assessment

3. PROJECT MANAGEMENT APPROACH

Include the method and approach used to manage the overall project and client correspondence. Briefly describe how the engagement proceeds from beginning to end. Include a timeline for completing the various components identified earlier in this RFP. Also include examples or your approach for status updates and notifying client of potential security issues uncovered.

4. DETAILED AND ITEMIZED PRICING

Include a fee breakdown by project phase and estimates of travel expenses. Travel expenses should follow the U.S. General Services Administration guidelines and per diem rates for Fargo, ND. Please see the Reference Websites section for a link to the U.S. General Services Administration website.

The following project phases should be used for the fee breakdown: External Penetration Test, Internal and Perimeter Vulnerability Assessment and Penetration Testing, Intrusion Detection and Prevention Systems Review, Firewall Reviews, Physical Security Penetration Testing, External Application Testing, External Website Vulnerability Testing, Cloud security assessment.

5. CONFLICT OF INTEREST

Any company receiving this RFP that has done work with ANY member of the Noridian Network of Companies, either through contracts issued by a member of the Noridian Network of Companies OR through contracts issued by government agencies MUST detail all work performed during calendar years 2020-2023. Any company indicating previous work performed with the Noridian Network of Companies in any form must indicate how it will address either the appearance of or actual conflict of interest issues.

FAILURE TO COMPLETELY DOCUMENT PREVIOUS WORK PERFORMED OR FAILURE TO ADEQUATELY DOCUMENT HOW THE RESPONDING COMPANY WILL ADDRESS CONFLICT OF INTEREST ISSUES CAN RESULT IN IMMEDIATE DISQUALIFICATION OF THE COMPANY'S PROPOSAL.

6. APPENDIX: SAMPLE DELIVERABLES

Include a sample of the reports and working papers you would utilize.

7. APPENDIX: REFERENCES

Three (3) current penetration testing corporate references of similar size to Noridian (At least 1,500 desktop users) including company name, contact name, title, address, telephone number, and client relationship synopsis. Corporate References must be from the industries of Health Care, Insurance or Finance. References may be contacted.

8. APPENDIX: PROJECT TEAM STAFFING

Include biographies and relevant experience of key staff and management personnel. List the personnel who would work on this project along with their qualifications and relevant experience. Describe bonding process and coverage levels of employees. Affirm that no employees, agents, consultants or independent contractors who may be working on the engagement have ever been convicted of a felony, have been (1) excluded from participation in

any federal or state Medicare, Medicaid, or any other third party payer program or appear on the federal government's Excluded Parties List System currently maintained by the General Services Administration (GSA) or the CMS OIG's List of Excluded Individuals/Entities; or (2) designated pursuant to Executive Order 13224 (OFAC), nor is any such action pending. Also, please detail if any staff who would be working on this engagement are agents, consultants or independent contractors.

9. APPENDIX: COMPANY OVERVIEW

- Key contact name(s), title, address (if different from above address), direct telephone and fax numbers.
- Person(s) authorized to contractually bind the organization for any proposal in response to this RFP.
- Brief history, including year established and number of years your company has been offering Information Security Testing.
- Pursuant to the Federal Acquisition Regulation (FAR), provide indication if the company qualifies as a small business, veteran-owned small business, service-disabled veteran-owned small business, HUBZone small business, small disadvantaged business, or women-owned small business.

Deliverables

1. DETAILED TECHNICAL REPORT

A document developed for the use of Noridian's technical staff which discusses: the methodology employed, positive security aspects identified, detailed technical vulnerability findings and an assignment of an impact rating for each vulnerability following FIPS Publication 199 which defines the following three levels of potential impact on organizations or individuals should there be a breach of security:

The potential impact is **LOW** if —

> The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.

The potential impact is **MODERATE** if —

> The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. A

serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.

The potential impact is **HIGH** if —

The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

The document developed should also include supporting detailed exhibits for vulnerabilities when appropriate (including results of testing tools, scripts, etc.) and detailed technical remediation steps.

Specifically, for system vulnerabilities, two detailed technical reports will be submitted to Noridian. One will have all vulnerabilities sorted by vulnerability, and the second will be sorted by DNS name.

Noridian requires the following documentation in addition to any vulnerability reports you may normally provide. These requirements include but are not limited to:

- Vulnerabilities must be reproducible and outline what tool was used to produce each vulnerability.
- Vulnerabilities shall not utilize proprietary tools where the vulnerability cannot be reproduced with another tool.
- Vulnerability report must include CVE, CWE, OWASP, or BID references or other reference source as agreed upon by Noridian Technical Contact.
- Vendor agrees to manually test at least one sample of each similar vulnerability type (e.g. cross-site scripting, SQL injection, etc.) per application or host to ensure false-positives are eliminated prior to report delivery.
- Web Penetration Testing Vulnerability reports must include step-by-step walk-through documentation which can be used to reproduce the vulnerability using agreed-upon open-source tools. Documentation must include all parameters on all vulnerable

application pages, including all inputs resulting in vulnerability detection so that they can be reproduced.

2. EXECUTIVE SUMMARY REPORT

A document developed to summarize the scope, approach, findings and recommendations, in a manner suitable for senior management.

Specifically, two executive summary reports will be submitted to Noridian. The first will address the Security Assessment of the Noridian Network of Companies, while the second will focus solely on the cloud evaluation.

3. PRESENTATIONS

The selected vendor may be required to make several presentations to Noridian staff as to the results of the security assessment. All presentations will be arranged by staff listed within this document and will possibly include executive-level presentations and technical staff-level presentations.

4. STATUS UPDATES

Formal weekly status updates shall be provided to the Noridian primary project contact and any additional designated personnel. Also, more frequent informal communication must occur during the fieldwork stage to ensure Noridian is informed of work progress and any potential security issues uncovered during testing.

Reference Websites

The following websites contain some of the documents referenced within this RFP:

CMS Business Partner Systems Security Manual (BPSSM) version 15

https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Info-Security-Library-Items/CMS1223332.html?DLPage=1&DLEntries=10&DLSort=0&DLSortDir=ascending

CMS Information Security (IS) MAC Acceptable Risk Safeguards (ARS) version

*To be shared as this is not available online.

Common Vulnerabilities and Exposures (CVE)
http://cve.mitre.org/

Common Weakness Enumeration (CWE)

http://cwe.mitre.org/

NIST Special Publication Home Page:
http://csrc.nist.gov/publications/PubsSPs.html

Open Web Application Security Project (OWASP)
http://www.owasp.org/

U.S. General Services Administration – Per Diem Rates:
http://www.gsa.gov/portal/category/100120