

Request for Proposals

2026 FISMA Audit

CONTENTS

Introduction	2
History	2
Company Background	3
Response Requirements and Timeline	4
Form of Final Agreement and Offeror’s Representations	4
Contact Information	4
Proposal Due Date	5
Tentative Timetable for Review Process	5
Evaluation Criteria and Selection Process	5
Terms and Conditions	6
Offeror’s Response	6
Detailed Proposal Requirements	7
Deliverables	10
Technical Requirements	12
Scoping Information	13
Other Key Dates	44
Reference Websites	44
Proposal Submission	45
Pricing	45

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 CMS FISMA Assessment.

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. Noridian conducts this security assessment annually, and it is the intention of Noridian to award the winner a contract for one year for the security assessment, while retaining the option to award the same winner subsequent contracts for years two and three 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.

HISTORY

Noridian Healthcare Solutions has consistently partnered with external vendors to conduct CMS FISMA Security Control Assessments (SCA) as part of its MAC contract obligations. These engagements have supported the renewal of Noridian's Authority to Operate (ATO) and compliance with CMS ARS 5.1 control objectives.

In recent years, Noridian contracted with various firms to perform internal and external penetration testing, control evaluations, and documentation reviews. As part of these engagements vendors have provided tailored assessments aligned with CMS requirements, including FedRAMP High baselines and NIST 800-53 compliance.

Noridian maintains a structured vendor onboarding and oversight process, including background check compliance, data lifecycle controls, and subcontractor flow-down requirements consistent with FISMA and CMS ARS standards.

This history reflects Noridian’s commitment to leveraging qualified vendors for rigorous, compliant, and transparent audit execution in support of CMS’s information security objectives.

COMPANY BACKGROUND

Noridian Healthcare Solutions, LLC (Noridian), a wholly owned subsidiary of HealthyDakota Mutual Holdings, 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. The scope of this RFP includes the below described contracts:

Medicare Parts A and B

Noridian is the Medicare Administrative Contractor (MAC) for Medicare Parts A/B for both Jurisdictions E and F, serving Alaska, Arizona, California, Hawaii, Idaho, Montana, North Dakota, Nevada, Oregon, South Dakota, Utah, Washington, Wyoming, Guam, American Samoa, and the Northern Mariana Islands.

Medicare DME

Noridian is also the Durable Medical Equipment MAC (DMEMAC) for Jurisdictions A and D, which includes 28 states: Alaska, Arizona, California, Connecticut, Delaware, Hawaii, Idaho, Iowa, Kansas, Maine, Maryland, Massachusetts, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New York, North Dakota, Oregon, Pennsylvania, Rhode Island, South Dakota, Utah, Vermont, Washington, Wyoming; the District of Columbia; and three territories: Guam, American Samoa and the Northern Mariana Islands.

SMRC

The purpose of the SMRC is to perform medical reviews and medical review related activities in support of three initiatives within the Center for Program Integrity (CPI), including: 1. The Provider Compliance Group (PCG) ‘Specialty Reviews’, 2. Program Integrity Reviews, and 3. Healthcare Fraud Prevention Partnership (HFPP) Reviews.

North Dakota State Medicaid

Noridian designs effective solutions for state health care programs. Since Medicaid programs vary from state to state, without a common language, Noridian specifically concentrates on reducing the provider burden by making programs easy to understand. Part of our service includes identifying, educating, and coaching provider organizations struggling with claims.

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: CMS FISMA Assessment

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 November 3rd 2025, 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	September 15, 2025
Deadline for Offeror questions	October 10, 2025
Noridian responses to offerors' questions	October 20, 2025
Proposals due by 5:00 PM CT	November 3, 2025
Final selection of offeror	November 17, 2025

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
<ul style="list-style-type: none"> ▪ Organization's experience in this space ▪ Customer history and relevance
Ability to meet the requirements
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.

OFFEROR'S RESPONSE

All offerors must include responses to the following in their proposals:

1. Offeror's website URL.
2. Brief history of offeror's company and its ownership.
3. A description of the company's certification process.

4. The names of all company accreditations and certifications.
5. Whether there are any pending lawsuits involving offeror's company and/or any potential conflicts with Noridian or HealthyDakota Mutual Holdings. Please provide details regarding any pending lawsuit(s) and/or conflict(s).
6. Whether offeror's company had any judgment and/or liens filed in the last five years. Please provide details regarding the judgment and/or lien and what actions have been taken to remedy, if any.
7. Whether offeror's company currently has an existing business relationship with Noridian or HealthyDakota Mutual Holdings.
8. Offeror's business classification, including small business, woman owned business, minority owned business, HUBZone, etc. Please specify relevant small business categories.
9. Other factors that make offeror's company the best choice for Noridian over the term of the business relationship.

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**
- **Physical Security Penetration Testing**
- **External Facing Application Testing**
- **External Website Vulnerability Assessment**
- **FISMA Assessment – Year One**
- **FISMA Assessment – Option Year Two**
- **FISMA Assessment – Option Year Three**

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, FISMA Assessment – Year One, FISMA Assessment – Option Year Two and FISMA Assessment – Option Year 3. An average price per control/enhancement would also be beneficial.

Noridian understands testing may overlap and cost savings will be achieved due to economies of scale. Please reflect these savings in your pricing and indicate the pricing of the two FA add-on sections both collectively and mutually exclusive. For example, the breakdown should include the price to perform all functions except the FISMA Assessment – Option Year 2 section and FISMA Assessment – Option Year 3. The breakdown should then indicate the cost of each of the FISMA Assessment Add-on sections individually as well as indicate the cost savings if both add-on sections were performed.

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 2016-2019. 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 FISMA and 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 whom 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 FISMA evaluation.

3. WORKING PAPERS

Verification of the performance of the applicable assessment procedures for each control is a fundamental aspect of the FISMA Assessment (FA) process. The selected vendor shall ensure that a cross reference to section/page/paragraph in the working papers of the applicable audit/review documentation is clearly described. The applicable work papers shall be included with the FA audit and shall document the testing and evaluation conducted as outlined within each ARS control. CMS requires the submission of all FA working papers.

4. 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.

5. 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.

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.
- Conduct a Physical Security Penetration Test attempting to gain physical entry into the Noridian facilities to provide an insight as to how well the organization is handling physical access controls and whether or not employees are abiding to company security policies. Provide a documented test plan to identify an acceptable level of exploitation and define the Rules of Engagement for the operation.
- 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.
- Assess compliance with the CMS FISMA Assessment (FA) control objectives described in this document and within each ARS control. All of the FA 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.

The testing will 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

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

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

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

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. Physical Security Penetration Testing.

Conduct a Physical Security Penetration Test in an attempt to gain physical entry into the Noridian facilities to provide insight as to how well the organization is handling physical access controls and whether or not employees are abiding to company security policies. A documented test plan should be provided to identify and agree upon an acceptable level of exploitation and also define the Rules of Engagement for the operation.

*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. 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

8. 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

FISMA Assessment – Option Year 1*

The following FA controls and enhancements should be tested. The quantity and level of testing should be sufficient to ensure compliance with the control section of each FA control and enhancement. Detailed working papers must be provided and are submitted to CMS. The detail for each FA control and enhancement is provided in the attachment “FA Controls – Year One”. *Note: The following selection of controls are subject to change at any time.*

Testing methods should include:

- a. Guidance provided in the assessment objective section of each FA control and enhancement**
 - and***
 - b. Guidance provided in the assessment method and objects section of each FA control and enhancement**
 - or***
-

a. Equivalent testing methods can be used.

References listed in each FA control and enhancement can be used to provide clarification to the control; however, the focus of the testing should be to ensure compliance with the control.

AC - ACCESS CONTROL

AC-01	-	Policy and Procedures
AC-02	-	Account Management
AC-02(01)	-	Automated System Account Management
AC-02(02)	-	Automated Temporary and Emergency Account Management
AC-02(03)	-	Disable Accounts
AC-02(04)	-	Automated Audit Actions
AC-02(05)	-	Inactivity Logout
AC-02(07)	-	Privileged User Accounts
AC-02(09)	-	Restrictions on Use of Shared and Groups Accounts
AC-02(11)	-	Usage Conditions
AC-02(12)	-	Account Monitoring for Atypical Usage
AC-02(13)	-	Disable Accounts for High-Risk Individuals
AC-03	-	Access Enforcement
AC-03(09)	-	Controlled Release
AC-03(11)	-	Restrict Access to Specific Information Types
AC-03(14)	-	Individual Access
AC-04	-	Information Flow Enforcement
AC-04(04)	-	Flow Control of Encrypted Information
AC-05	-	Separation of Duties

AC-06	-	Least Privilege
AC-06(01)	-	Authorize Access to Security Functions
AC-06(02)	-	Non-privileged Access for Nonsecurity Functions
AC-06(03)	-	Network Access to Privileged Commands
AC-06(05)	-	Privileged Accounts
AC-06(06)	-	Privileged Access by Non-Organizational Users
AC-06(07)	-	Review of User Privileges
AC-06(09)	-	Log Use of Privileged Functions
AC-06(10)	-	Prohibit Non-privileged Users from Executing Privileged Functions
AC-07	-	Unsuccessful Logon Attempts
AC-07(02)	-	Purge or Wipe Mobile Device
AC-08	-	System Use Notification
AC-09	-	Previous Logon Notification
AC-09(01)	-	Unsuccessful Logons
AC-10	-	Concurrent Session Control
AC-11	-	Device Lock
AC-11(01)	-	Pattern-hiding Displays
AC-12	-	Session Termination
AC-14	-	Permitted Actions Without Identification or Authentication
AC-17	-	Remote Access
AC-17(01)	-	Monitoring and Control
AC-17(02)	-	Protection of Confidentiality and Integrity Using Encryption

AC-17(03)	-	Managed Access Control Points
AC-17(04)	-	Privileged Commands and Access
AC-17(06)	-	Protection of Mechanism Information
AC-17(09)	-	Disconnect or Disable Access
AC-18	-	Wireless Access
AC-18(01)	-	Authentication and Encryption
AC-18(03)	-	Disable Wireless Networking
AC-18(04)	-	Wireless Access Restrict Configurations by Users
AC-18(05)	-	Wireless Access Antennas and Transmission Power Levels
AC-19	-	Access Control for Mobile Devices
AC-19(05)	-	Full Device and Container-based Encryption
AC-20	-	Use of External Systems
AC-20(01)	-	Limits on Authorized Use
AC-20(02)	-	Portable Storage Devices — Restricted Use
AC-20(03)	-	Non-organizationally Owned Systems — Restricted Use
AC-20(05)	-	Portable Storage Devices - Prohibited Use
AC-21	-	Information Sharing
AC-22	-	Publicly Accessible Content

IA - IDENTIFICATION AND AUTHENTICATION

IA-01	-	Policy and Procedures
IA-02	-	Identification and Authentication (Organizational Users)

IA-02(01)	-	Multifactor Access to Privileged Accounts
IA-02(02)	-	Multifactor Access to Non-Privileged Accounts
IA-02(05)	-	Individual Authentication with Group Authentication
IA-02(06)	-	ACCESS TO ACCOUNTS — SEPARATE DEVICE
IA-02(08)	-	Access to Accounts - Replay Resistant
IA-02(12)	-	Acceptance of PIV Credentials
IA-03	-	Device Identification and Authentication
IA-04	-	Identifier Management
IA-04(04)	-	Identify User Status
IA-05	-	Authenticator Management
IA-05(01)	-	Password-Based Authentication
IA-05(02)	-	Public Key-Based Authentication
IA-05(06)	-	Protection of Authenticators
IA-05(15)	-	GSA-APPROVED PRODUCTS AND SERVICES
IA-06	-	Authenticator Feedback
IA-07	-	Cryptographic Module Authentication
IA-08	-	Identification and Authentication (Non-Organizational Users)
IA-08(01)	-	Acceptance of PIV Credentials from Other Agencies
IA-08(02)	-	ACCEPTANCE OF EXTERNAL AUTHENTICATORS
IA-08(04)	-	Use of Defined Profiles
IA-11	-	Re-Authentication
IA-12	-	Identity Proofing

- IA-12(02) - Identity Evidence
- IA-12(03) - Identity Evidence Validation and Verification
- IA-12(04) - In-Person Validation and Verification
- IA-12(05) - Address Confirmation

PS - PERSONNEL SECURITY

- PS-01 - Policy and Procedures
- PS-02 - Position Risk Designation
- PS-03 - Personnel Screening
- PS-03(04) - Citizenship Requirements
- PS-04 - Personnel Termination
- PS-04(01) - Post-Employment Requirements
- PS-04(02) - Automated Actions
- PS-05 - Personnel Transfer
- PS-06 - Access Agreements
- PS-07 - External Personnel Security
- PS-08 - Personnel Sanctions
- PS-09 - Position Descriptions

PM - PROGRAM MANAGEMENT

- PM-01 - Information Security Program Plan
- PM-02 - Information Security Program Leadership Role

PM-03	-	Information Security and Privacy Resources
PM-04	-	Plan of Action and Milestones Process
PM-05	-	System Inventory
PM-05(01)	-	Inventory of Personally Identifiable Information
PM-06	-	Measures of Performance
PM-07	-	Enterprise Architecture
PM-08	-	Critical Infrastructure Plan
PM-09	-	Risk Management Strategy
PM-10	-	Authorization Process
PM-11	-	Mission and Business Process Definition
PM-12	-	Insider Threat Program
PM-13	-	Security and Privacy Workforce
PM-14	-	Testing, Training, and Monitoring
PM-15	-	Security and Privacy Groups and Associations
PM-16	-	Threat Awareness Program
PM-16(01)	-	Automated Means for Sharing Threat Intelligence
PM-17	-	Protecting Controlled Unclassified Information on External Systems
PM-18	-	Privacy Program Plan
PM-19	-	Privacy Program Leadership Role
PM-20	-	Dissemination of Privacy Program Information
PM-20(01)	-	Privacy Policies on Websites, Applications, and Digital Services
PM-21	-	Accounting of Disclosures

PM-22	-	Personally Identifiable Information Quality Management
PM-23	-	Data Governance Body
PM-24	-	Data Integrity Board
PM-25	-	Minimization of PII Used in Testing, Training, and Research
PM-26	-	Complaint Management
PM-27	-	Privacy Reporting
PM-28	-	Risk Framing
PM-29	-	Risk Management Program Leadership Roles
PM-30	-	Supply Chain Risk Management Strategy
PM-30(01)	-	Suppliers of Critical or Mission-Essential Items
PM-31	-	Continuous Monitoring Strategy
PM-32	-	Purposing

SA - SYSTEM AND SERVICES ACQUISITION

SA-01	-	Policy and Procedures
SA-02	-	Allocation of Resources
SA-03	-	System Development Life Cycle
SA-03(01)	-	MANAGE PREPRODUCTION ENVIRONMENT
SA-03(02)	-	Use of Live Operational Data
SA-03(03)	-	TECHNOLOGY REFRESH
SA-04	-	Acquisition Process
SA-04(01)	-	Functional Properties of Controls

SA-04(02)	-	Design and Implementation Information for Security Controls
SA-04(05)	-	System, Component, and Service Configurations
SA-04(09)	-	Functions, Ports, Protocols, and Services in Use
SA-04(10)	-	Use of Approved PIV Products
SA-05	-	System Documentation
SA-08	-	Security and Privacy Engineering Principles
SA-8(33)	-	MINIMIZATION
SA-09	-	External System Services
SA-09(01)	-	RISK ASSESSMENTS AND ORGANIZATIONAL APPROVALS
SA-09(02)	-	Identification of Functions, Ports, Protocols, and Services
SA-09(05)	-	Processing, Storage, and Service Location
SA-10	-	Developer Configuration Management
SA-11	-	Developer Testing and Evaluation
SA-11(01)	-	STATIC CODE ANALYSIS
SA-11(05)	-	Penetration Testing
SA-11(08)	-	Dynamic Code Analysis
SA-15	-	Development Process, Standards, and Tools
SA-15(03)	-	Criticality Analysis
SA-16	-	Developer Provided Training
SA-17	-	Developer Security Architecture and Design
SA-21	-	Developer Screening
SA-22	-	Unsupported System Components

SI - SYSTEM AND INFORMATION INTEGRITY

SI-01	-	Policy and Procedures
SI-02	-	Flaw Remediation
SI-02(02)	-	Automated Flaw Remediation Status
SI-02(06)	-	Removal of Previous Versions of Software and Firmware
SI-03	-	Malicious Code Protection
SI-04	-	System Monitoring
SI-04(01)	-	System-Wide Intrusion Detection System
SI-04(02)	-	Automated Tools and Mechanisms for Real-Time Analysis
SI-04(04)	-	Inbound and Outbound Communications Traffic
SI-04(05)	-	System-Generated Alerts
SI-04(10)	-	Visibility of Encrypted Communications
SI-04(11)	-	Analyze Communications Traffic Anomalies
SI-04(12)	-	Automated Organization-Generated Alerts
SI-04(13)	-	Analyze Traffic and Event Patterns
SI-04(14)	-	Wireless Intrusion Detection
SI-04(16)	-	Correlate Monitoring Information
SI-04(18)	-	Analyze Traffic and Covert Exfiltration
SI-04(20)	-	Privileged Users
SI-04(22)	-	Unauthorized Network Services
SI-04(23)	-	Host-Based Devices
SI-05	-	Security Alerts, Advisories, and Directives

SI-05(01)	-	Automated Alerts and Advisories
SI-06	-	Security and Privacy Function Verification
SI-07	-	Software, Firmware, and Information Integrity
SI-07(01)	-	Integrity Checks
SI-07(02)	-	Automated Notifications of Integrity Violations
SI-07(05)	-	Automated Response to Integrity Violations
SI-07(07)	-	Integration of Detection and Response
SI-07(15)	-	Code Authentication
SI-08	-	Spam Protection
SI-08(02)	-	Automatic Updates
SI-10	-	Information Input Validation
SI-11	-	Error Handling
SI-12	-	Information Management and Retention
SI-12(01)	-	Limit Personally Identifiable Information Elements
SI-12(02) Research	-	Minimize Personally Identifiable Information in Testing, Training, and
SI-12(03)	-	Information Disposal
SI-16	-	Memory Protection
SI-18	-	Personally Identifiable Information Quality Operations
SI-18(04)	-	Individual Requests
SI-19	-	De-Identification

PT - PERSONALLY IDENTIFIABLE INFORMATION PROCESSING AND TRANSPARENCY

PT-01	-	Policy and Procedures
PT-02	-	Authority to Process Personally Identifiable Information
PT-03	-	Personally Identifiable Information Processing Purposes
PT-04	-	Consent
PT-05	-	Privacy Notice
PT-05(02)	-	Privacy Act Statements
PT-06	-	System of Records Notice
PT-06(01)	-	Routine Uses
PT-06(02)	-	Exemption Rules
PT-07	-	Specific Categories of Personally Identifiable Information
PT-07(01)	-	Social Security Numbers
PT-07(02)	-	First Amendment Information
PT-08	-	Computer Matching Requirements

* ARS version 5.1, Appendix A, CMSR High Impact Level Data includes some CMS and HHS specific controls. Noridian will require testing on the finalized controls and enhancements. Further guidance is provided in NIST SP-800-53 rev 5 Appendix C.

FISMA Assessment – Year Two*

The following FA controls and enhancements should be tested. The quantity and level of testing should be sufficient to ensure compliance with the control section of each FA control and enhancement. Detailed working papers must be provided and are submitted to CMS. The detail for each FA control and enhancement is provided in the attachment “FA Controls – Year Two”. *Note: The following selection of controls are subject to change at any time.*

Testing methods should include:

- a. **Guidance provided in the assessment objective section of each FA control and enhancement**
- and*
- b. **Guidance provided in the assessment method and objects section of each FA control and enhancement**
- or*
- a. **Equivalent testing methods can be used.**

References listed in each FA control and enhancement can be used to provide clarification to the control; however, the focus of the testing should be to ensure compliance with the control.

AT - AWARENESS AND TRAINING

AT-01	-	Policy and Procedures
AT-02	-	Literacy Training and Awareness
AT-02(01)	-	Practical Exercises
AT-02(02)	-	Insider Threat
AT-02(03)	-	Social Engineering and Mining
AT-02(04)	-	Suspicious Communications and Anomalous System Behavior
AT-02(05)	-	Advanced Persistent Threat
AT-02(06)	-	Cyber Threat Environment
AT-03	-	Role-Based Training
AT-03(01)	-	Environmental Controls
AT-03(02)	-	Physical Security Controls
AT-03(03)	-	Practical Exercises
AT-03(05)	-	Processing Personally Identifiable Information
AT-04	-	Training Records

AU - AUDIT AND ACCOUNTABILITY

AU-01	-	Policy and Procedures
AU-02	-	Event Logging
AU-03	-	Content of Audit Records
AU-03(01)	-	Additional Audit Information
AU-03(03)	-	Limit Personally Identifiable Information Elements
AU-04	-	Audit Log Storage Capacity
AU-05	-	Response to Audit Logging Processing Failures
AU-05(01)	-	Storage Capacity Warning
AU-05(02)	-	Real-Time Alerts
AU-06	-	Audit Record Review, Analysis, and Reporting
AU-06(01)	-	Automated Process Integration
AU-06(03)	-	Correlate Audit Record Repositories
AU-06(05)	-	Integrated Analysis of Audit Records
AU-06(06)	-	Correlation with Physical Monitoring
AU-07	-	Audit Record Reduction and Report Generation
AU-07(01)	-	Automatic Processing
AU-08	-	Time Stamps
AU-09	-	Protection of Audit Information
AU-09(02)	-	Store on Separate Physical Systems or Components
AU-09(03)	-	Cryptographic Protection
AU-09(04)	-	Access by Subset of Privileged Users

AU-09(05)	-	Dual Authorization
AU-09(06)	-	Read Only Access
AU-10	-	Non-Repudiation
AU-11	-	Audit Record Retention
AU-12	-	Audit Record Generation
AU-12(01)	-	System-Wide and Time-Correlated Audit Trail
AU-12(03)	-	Changes by Authorized Individuals
AU-16	-	Cross-Organizational Audit Logging

CP - CONTINGENCY PLANNING

CP-01	-	Policy and Procedures
CP-02	-	Contingency Plan
CP-02(01)	-	Coordinate with Related Plans
CP-02(02)	-	Capacity Planning
CP-02(03)	-	Resume Missions and Business Functions
CP-02(05)	-	Continue Missions and Business Functions
CP-02(06)	-	Alternate Processing and Storage Sites
CP-02(07)	-	Coordinate with External Service Providers
CP-02(08)	-	Identify Critical Assets
CP-03	-	Contingency Training
CP-03(01)	-	Simulated Events
CP-03(02)	-	Mechanisms Used in Training Environments
CP-04	-	Contingency Plan Testing

CP-04(01)	-	Coordinate with Related Plans
CP-04(02)	-	Alternate Processing Site
CP-04(04)	-	Full Recovery and Reconstitution
CP-06	-	Alternate Storage Site
CP-06(01)	-	Separation from Primary Site
CP-06(02)	-	Recovery Time and Point Objectives
CP-06(03)	-	Accessibility
CP-07	-	Alternate Processing Site
CP-07(01)	-	Separation from Primary Site
CP-07(02)	-	Accessibility
CP-07(03)	-	Priority of Service
CP-07(04)	-	Preparation for Use
CP-08	-	Telecommunications Services
CP-08(01)	-	Priority of Service Provisions
CP-08(02)	-	Single Points of Failure
CP-08(03)	-	Separation of Primary and Alternate Providers
CP-08(04)	-	Provider Contingency Plan
CP-08(05)	-	Alternate Telecommunications Service Testing
CP-09	-	System Backup
CP-09(01)	-	Testing for Reliability and Integrity
CP-09(02)	-	Test Restoration Using Sampling
CP-09(03)	-	Separate Storage for Critical Information

- CP-09(05) - Transfer to Alternate Storage Site
- CP-09(08) - Cryptographic Protection
- CP-10 - System Recovery and Reconstitution
- CP-10(02) - Transaction Recovery
- CP-10(04) - Restore within Time Period

IR - INCIDENT RESPONSE

- IR-01 - Policy and Procedures
- IR-02 - Incident Response Training
 - IR-02(01) - Simulated Events
 - IR-02(02) - Automated Training Environments
 - IR-02(03) - Breach
- IR-03 - Incident Response Testing
 - IR-03(02) - Coordination with Related Plans
- IR-04 - Incident Handling
 - IR-04(01) - Automated Incident Handling Processes
 - IR-04(02) - DYNAMIC RECONFIGURATION
 - IR-04(04) - Information Correlation
 - IR-04(06) - Insider Threats – Specific Capabilities
 - IR-04(08) - Correlation with External Organizations
 - IR-04(10) - SUPPLY CHAIN COORDINATION
 - IR-04(11) - Integrated Incident Response Team
 - IR-04(12) - Malicious Code and Forensic Analysis

IR-04(14)	-	Security Operations Center
IR-05	-	Incident Monitoring
IR-05(01)	-	Automated Tracking, Data Collection, and Analysis
IR-06	-	Incident Reporting
IR-06(01)	-	Automated Reporting
IR-06(03)	-	SUPPLY CHAIN COORDINATION
IR-07	-	Incident Response Assistance
IR-07(01)	-	Automation Support for Availability of Information and Support
IR-08	-	Incident Response Plan
IR-08(01)	-	Breaches

MA - MAINTENANCE

MA-01	-	Policy and Procedures
MA-02	-	Controlled Maintenance
MA-02(02)	-	Automated Maintenance Activities
MA-03	-	Maintenance Tools
MA-03(01)	-	Inspect Tools
MA-03(02)	-	Inspect Media
MA-03(03)	-	Prevent Unauthorized Removal
MA-03(04)	-	Restricted Tool Use
MA-03(05)	-	Execution with Privilege
MA-03(06)	-	Software Updates and Patches
MA-04	-	Nonlocal Maintenance

- MA-04(03) - Comparable Security and Sanitization
- MA-05 - Maintenance Personnel
- MA-05(01) - Individuals Without Appropriate Access
- MA-06 - Timely Maintenance

PE - PHYSICAL AND ENVIRONMENTAL PROTECTION

- PE-01 - Policy and Procedures
- PE-02 - Physical Access Authorizations
- PE-02(01) - Access by Position or Role
- PE-03 - Physical Access Control
- PE-03(01) - System Access
- PE-04 - Access Control for Transmission
- PE-05 - Access Control for Output Devices
- PE-06 - Monitoring Physical Access
- PE-06(01) - Intrusion Alarms and Surveillance Equipment
- PE-06(04) - Monitoring Physical Access to Systems
- PE-08 - Visitor Access Records
- PE-08(01) - Automated Records Maintenance and Review
- PE-09 - Power Equipment and Cabling
- PE-10 - Emergency Shutoff
- PE-11 - Emergency Power
- PE-11(01) - Alternate Power Supply - Minimal Operational Capability
- PE-12 - Emergency Lighting

PE-12(01)	-	Essential Missions and Business Functions
PE-13	-	Fire Protection
PE-13(01)	-	Detection Systems - Automatic Activation and Notification
PE-13(02)	-	Suppression Systems - Automatic Activation and Notification
PE-14	-	Environmental Controls
PE-15	-	Water Damage Protection
PE-15(01)	-	Automation Support
PE-16	-	Delivery and Removal
PE-17	-	Alternate Work Site
PE-18	-	Location of System Components

* ARS version 5.1, Appendix A, CMSR High Impact Level Data includes some CMS and HHS specific controls. Noridian will require testing on the finalized controls and enhancements. Further guidance is provided in NIST SP-800-53 rev 5 Appendix C.

FISMA Assessment – Option Year 3*

The following FA controls and enhancements should be tested. The quantity and level of testing should be sufficient to ensure compliance with the control section of each FA control and enhancement. Detailed working papers must be provided and are submitted to CMS. The detail for each FA control and enhancement is provided in the attachment “FA Controls – Year Three”. *Note: The following selection of controls are subject to change at any time.*

Testing methods should include:

- a. Guidance provided in the assessment objective section of each FA control and enhancement**
and
- b. Guidance provided in the assessment method and objects section of each FA control and enhancement**
or

a. Equivalent testing methods can be used.

References listed in each FA control and enhancement can be used to provide clarification to the control; however, the focus of the testing should be to ensure compliance with the control.

CA - ASSESSMENT, AUTHORIZATION, AND MONITORING

CA-01	-	Policies and Procedures
CA-02	-	Control Assessments
CA-02(01)	-	Independent Assessors
CA-02(02)	-	Specialized Assessments
CA-02(03)	-	LEVERAGING RESULTS FROM EXTERNAL ORGANIZATIONS
CA-03	-	Information Exchange
CA-03(06)	-	Transfer Authorizations
CA-05	-	Plan of Action and Milestones
CA-06	-	Authorization
CA-06(01)	-	Joint Authorization Intra-Organization
CA-07	-	Continuous Monitoring
CA-07(01)	-	Independent Assessment
CA-07(03)	-	Trend Analyses
CA-07(04)	-	Risk Monitoring
CA-08	-	Penetration Testing
CA-08(01)	-	Independent Penetration Testing Agent or Team
CA-08(02)	-	RED TEAM EXERCISES
CA-08(03)	-	Facility Penetration Testing

CA-09 - Internal System Connections

CA-09(01) - Compliance Checks

CM - CONFIGURATION MANAGEMENT

CM-01 - Policy and Procedures

CM-02 - Baseline Configuration

CM-02(02) - Automation Support for Accuracy and Currency

CM-02(03) - Retention of Previous Configurations

CM-02(06) - Development and Test Environments

CM-02(07) - Configure Systems and Components for High-Risk Areas

CM-03 - Configuration Change Control

CM-03(01) - Automated Documentation, Notification, and Prohibition of Changes

CM-03(02) - Testing, Validation, and Documentation of Changes

CM-03(04) - Security and Privacy Representatives

CM-03(06) - Cryptography Management

CM-03(07) - Review System Changes

CM-04 - Impact Analyses

CM-04(01) - Separate Test Environments

CM-04(02) - Verification of Controls

CM-05 - Access Restrictions for Change

CM-05(01) - Automated Access Enforcement and Audit Records

CM-05(05) - Privilege Limitation for Production and Operation

CM-05(06)	-	Limit Library Privileges
CM-06	-	Configuration Settings
CM-06(01)	-	Automated Management, Application, and Verification
CM-06(02)	-	Respond to Unauthorized Changes
CM-07	-	Least Functionality
CM-07(01)	-	Periodic Review
CM-07(02)	-	Prevent Program Execution
CM-07(05)	-	Authorized Software - Allow
CM-07(09)	-	Prohibiting the Use of Unauthorized Software
CM-08	-	System Component Inventory
CM-08(01)	-	Updates During Installation and Removal
CM-08(02)	-	Automated Maintenance
CM-08(03)	-	Automated Unauthorized Component Detection
CM-08(04)	-	Accountability Information
CM-08(06)	-	Assessed Configurations and Approved Deviations
CM-08(07)	-	Centralized Repository
CM-09	-	Configuration Management Plan
CM-09(01)	-	Assignment of Responsibility
CM-10	-	Software Usage Restrictions
CM-11	-	User-Installed Software
CM-11(02)	-	Software Installation with Privileged Status
CM-12	-	Information Location

CM-12(01) - Automated Tools to Support Information Location

CM-14 - Signed Components

MP - MEDIA PROTECTION

MP-01 - Policy and Procedures

MP-02 - Media Access

MP-03 - Media Marking

MP-04 - Media Storage

MP-05 - Media Transport

MP-05(03) - Custodians

MP-06 - Media Sanitization

MP-06(01) - Review, Approve, Track, Document, and Verify

MP-06(02) - Equipment Testing

MP-06(03) - Nondestructive Techniques

MP-06(08) - Remote Purging or Wiping of Information

MP-07 - Media Use

MP-07(02) - Prohibit Use of Sanitization-Resistant Media

PL - PLANNING

PL-01 - Policy and Procedures

PL-02 - System Security and Privacy Plan

PL-04 - Rules of Behavior

PL-04(01) - Social Media and External Site / Application Usage Restrictions

PL-07	-	Concept of Operations
PL-08	-	Security and Privacy Architectures
PL-08(01)	-	Defense-In-Depth
PL-09	-	Central Management
PL-10	-	Baseline Selection
PL-11	-	Baseline Tailoring

RA - RISK ASSESSMENT

RA-01	-	Policy and Procedures
RA-02	-	Security Categorization
RA-03	-	Risk Assessment
RA-03(01)	-	Supply Chain Risk Assessment
RA-05	-	Vulnerability Monitoring and Scanning
RA-05(02)	-	Update Vulnerabilities to be Scanned
RA-05(04)	-	Discoverable Information
RA-05(05)	-	Privileged Access
RA-05(06)	-	AUTOMATED TREND ANALYSES
RA-05(10)	-	CORRELATE SCANNING INFORMATION
RA-05(11)	-	Public Disclosure Program
RA-07	-	Risk Response
RA-08	-	Privacy Impact Assessments
RA-09	-	Criticality Analysis

RA-10 - Threat Hunting

SC - SYSTEM AND COMMUNICATIONS PROTECTION

SC-01 - Policy and Procedures

SC-02 - Separation of System and User Functionality

SC-03 - Security Function Isolation

SC-03(01) - Hardware Separation

SC-03(03) - Minimize Nonsecurity Functionality

SC-04 - Information in Shared System Resources

SC-05 - Denial-of-Service Protection

SC-05(01) - Restrict Ability to Attack Other Systems

SC-05(02) - Capacity, Bandwidth, and Redundancy

SC-05(03) - Detection and Monitoring

SC-07 - Boundary Protection

SC-07(03) - Access Points

SC-07(04) - External Telecommunications Services

SC-07(05) - Deny By Default — Allow By Exception

SC-07(07) - Split Tunneling for Remote Devices

SC-07(08) - Route Traffic to Authenticated Proxy Servers

SC-07(10) - Prevent Exfiltration

SC-07(11) - Restrict Incoming Communications Traffic

SC-07(12) - Host-Based Protection

SC-07(14)	-	Protect Against Unauthorized Physical Connections
SC-07(17)	-	Automated Enforcement of Protocol Formats
SC-07(18)	-	Fail Secure
SC-07(21)	-	Isolation of System Components
SC-07(22)	-	Separate Subnets for Connecting to Different Security Domains
SC-07(24)	-	Personally Identifiable Information
SC-08	-	Transmission Confidentiality and Integrity
SC-08(01)	-	Cryptographic Protection
SC-08(02)	-	Pre- and Post-Transmission Handling
SC-08(03)	-	Cryptographic Protection for Message Externals
SC-10	-	Network Disconnect
SC-12	-	Cryptographic Key Establishment and Management
SC-12(01)	-	Availability
SC-13	-	Cryptographic Protection
SC-15	-	Collaborative Computing Devices and Applications
SC-17	-	Public Key Infrastructure Certificates
SC-18	-	Mobile Code
SC-18(04)	-	Prevent Automatic Execution
SC-20	-	Secure Name/Address Resolution Service (Authoritative Source)
SC-21	-	Secure Name/Address Resolution Service (Recursive or Caching Resolver)
SC-22	-	Architecture and Provisioning for Name/Address Resolution Service
SC-23	-	Session Authenticity

SC-24	-	Fail In Known State
SC-28	-	Protection of Information At Rest
SC-28(01)	-	Cryptographic Protection
SC-39	-	Process Isolation

SR - SUPPLY CHAIN RISK MANAGEMENT

SR-01	-	Policy and Procedures
SR-02	-	Supply Chain Risk Management Plan
SR-02(01)	-	Establish SCRM Team
SR-03	-	Supply Chain Controls and Processes
SR-04(02)	-	Track and Trace
SR-04(03)	-	Validate as Genuine and Not Altered
SR-05	-	Acquisition Strategies, Tools, and Methods
SR-05(02)	-	Assessments Prior to Selection, Acceptance, Modification, or Update
SR-06	-	Supplier Assessments and Reviews
SR-08	-	Notification Agreements
SR-09	-	Tamper Resistance and Detection
SR-09(01)	-	Multiple Stages of System Development Life Cycle
SR-10	-	Inspection of Systems or Components
SR-11	-	Component Authenticity
SR-11(01)	-	Anti-counterfeit Training
SR-11(02)	-	Configuration Control for Component Service and Repair

SR-12 - Component Disposal

* ARS version 5.1, Appendix A, CMSR High Impact Level Data includes some CMS and HHS specific controls. Noridian will require testing on the finalized controls and enhancements. Further guidance is provided in NIST SP-800-53 rev 5 Appendix C.

OTHER KEY DATES

Event	Tentative Date
On-site initial kickoff meeting with vendor	Second week of January 2026
Vendor Provides PBC list to Noridian	Third week of January 2026
Window for work to be completed during (formal exit conference with preliminary findings at the conclusion of onsite testing)	Third week of January 2026 – End of April 2026
Remediation of findings (Noridian) and retesting (Vendor) completed	Mid-April 2026 to Start of May 2026
Issuance of Draft Report	Start of May 2026
Noridian Reviews Draft Report	Mid-May 2026
Issuance of Final Network Security Report	End of May 2026
Issuance of Final FISMA Evaluation Report	End of May 2026

REFERENCE WEBSITES

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

CMS Business Partner Systems Security Manual (BPSSM) version 15.1

<https://www.hhs.gov/guidance/sites/default/files/hhs-guidance-documents/CMS/r13307ss.pdf>

CMS Information Security (IS) MAC Acceptable Risk Safeguards (ARS) version 5.1

*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:

<https://www.gsa.gov/travel/plan-book/per-diem-rates>

PROPOSAL SUBMISSION

The deadline for proposals is on or before November 3rd 2025. Submit the proposal and the Offeror's Profile questionnaire via email to the contact below:

rfp@noridian.com

Subject Line: CMS FISMA Assessment

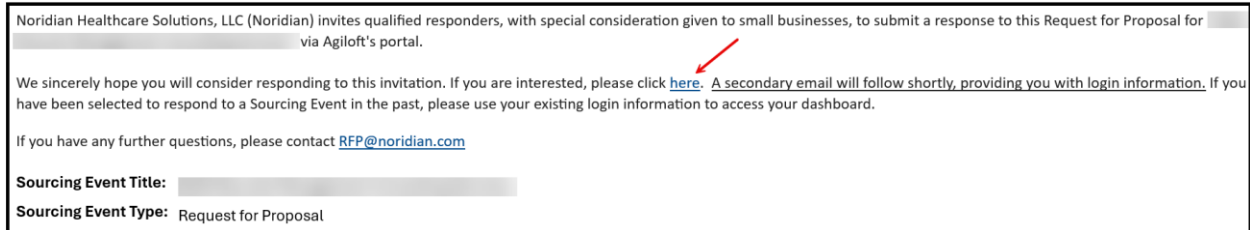
PRICING

The resulting contract is anticipated to have a term of three years. Noridian requests offerors to submit pricing in a table format like the example format below.

AGILOFT USER GUIDE

Accessing and Responding to the Sourcing Event

1. In your invitation email, please click the “here” link to access the Sourcing Event in Agiloft.



2. You will be prompted to enter your username and password, which you would have received in a separate email from Agiloft
 - a. If you have accessed the system previously, you will use your existing username and password.
 - b. If you are copying and pasting the username and password from the email, please ensure there are no spaces
3. You can access the official sourcing event package under the attachments section.
4. Upon review of the sourcing event package, please click either I am Interested or Not Interested.
5. To submit questions, please use the Questions and Answers section.
 - a. Type your question into the Ask a Question box and then click Submit Question.
6. To submit your proposal, please do so in the Attachments Section.
 - a. Either click attach/manage or you may drag and drop your documents
 - b. Please do not upload your proposal in the Customer Portal. Your proposal must be uploaded in the Sourcing Event for visibility to our Procurement Team.
7. For any questions, please contact rfp@noridian.com