OMB Control #: 0938-NEW
Expiration Date: XX/XX/20XX

NON-EXCHANGE ENTITY:	
SYSTEM NAME:	
SYSTEM ACRONYM:	
CURRENT FISCAL YEAR:	

Plan of Action and Milestone (POA&M) Metrics Totals (Security, Other & Privacy Combined)	
POA&M Findings by Weakness Status	
ONGOING	0
DELAYED	0
COMPLETED	0
ACCEPTED RISK	0
Total	0
Open Findings by Risk Level	
CRITICAL	0
HIGH	0
MODERATE	0
LOW	0
Total	0
Total # of Open Findings (Ongoing, Delayed, & Accepted)	0

Number of POA&M Items By Security Control Family	TOTAL Open	Ongoing	Delayed	Completed	Accepted Risk
AC	0	0	0	0	0
AT	0	0	0	0	0
AU	0	0	0	0	0
CA	0	0	0	0	0
CM	0	0	0	0	0
CP	0	0	0	0	0
IA	0	0	0	0	0
IR	0	0	0	0	0
MA	0	0	0	0	0
MP	0	0	0	0	0
PE	0	0	0	0	0
PL	0	0	0	0	0
PS	0	0	0	0	0
RA	0	0	0	0	0
SA	0	0	0	0	0
SC	0	0	0	0	0
SI	0	0	0	0	0
Other	0	0	0	0	0

Number of POA&M Items By Privacy Control Family	Total Open	Ongoing	Delayed	Completed	Accepted Risk
AP	0	0	0	0	0
AR	0	0	0	0	0
DI	0	0	0	0	0
DM	0	0	0	0	0
IP	0	0	0	0	0
SE	0	0	0	0	0
TR	0	0	0	0	0
UL	0	0	0	0	0

Plan of Action and Milestone (POA&M) Metrics Totals (Security Only)	
POA&M Findings by Weakness Status	
ONGOING	0
DELAYED	0
COMPLETED	0
ACCEPTED RISK	0
Total	0
Open Findings by Risk Level	
CRITICAL	0
HIGH	0
MODERATE	0
LOW	0
Total	0
Total # of Open Findings (Ongoing, Delayed, & Accepted)	0

Gap Analysis Tracking	TOTAL Open	Ongoing	Delayed	Completed	Accepted Risk
NEE V. 1.0	0	0	0	0	0
NEE V. 1.2	0	0	0	0	0
NEE V. 2.0	0	0	0	0	0
NEE V. 3.0	0	0	0	0	0
NEE V. 4.0	0	0	0	0	0

Plan of Action and Milestone (POA&M) Metrics Totals (Privacy Only)	
POA&M Findings by Weakness Status	
ONGOING	0
DELAYED	0
COMPLETED	0
ACCEPTED RISK	0
Total	0
Open Findings by Risk Level	
CRITICAL	0
HIGH	0
MODERATE	0
LOW	0
Total	0
Total # of Open Findings (Ongoing, Delayed, & Accepted)	0

PRA DISCLOSURE: According to the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number. The valid OMB control number for this information collection is 0938-NEW, expiration date is XX/XX/20XX. The time required to complete this information collection is estimated to take up to 144,652 hours annually for all direct enrollment entities. If you have comments concerning the accuracy of the time estimate(s) or suggestions for improving this form, please write to: CMS, 7500 Security Boulevard, Attn: PRA Reports Clearance Officer, Mail Stop C4-26-05, Baltimore, Maryland 21244-1850. ****CMS Disclosure**** Please do not send applications, claims, payments, medical records or any documents containing sensitive information to the PRA Reports Clearance Office. Please note that any correspondence not pertaining to the information collection burden approved under the associated OMB control number listed on this form will not be reviewed, forwarded, or retained. If you have questions or concerns regarding where to submit your documents, please contact Brittany Cain at Brittany.Cain@cms.hhs.gov.

Plan of Action and Milestone (POA&M) Metrics Totals (Other Only)	
POA&M Findings by Weakness Status	
ONGOING	0
DELAYED	0
COMPLETED	0
ACCEPTED RISK	0
Total	0
Open Findings by Risk Level	
CRITICAL	0
HIGH	0
MODERATE	0
LOW	0
Total	0
Total # of Open Findings (Ongoing, Delayed, & Accepted)	0

NON-EXCHANGE ENTITY:	
SYSTEM NAME:	
SYSTEM ACRONYM:	
CURRENT FISCAL YEAR:	

System Name	System Acronym	System Criticality as defined by FIPS	Confidentiality	Availability	Integrity	If no weaknesses identified, provide a reason	Risk Subtotal
0	0	Moderate	Moderate	Moderate	Moderate		0

Weakness Identifier	Control Family	Control Details	Weakness Description	Weakness Source	POC	Resources Required	Scheduled Completion Date	Milestones With Completion Dates	Changes to Milestones Date	Completion Date	Weakness Status	Risk Level	NEE Version	Compensating Controls	Comments

NON-EXCHANGE ENTITY:	1
SYSTEM NAME:	2
SYSTEM ACRONYM:	3
CURRENT FISCAL YEAR:	4

System Name	System Acronym	System Criticality as defined by FIPS	Confidentiality	Availability	Integrity	If no weaknesses identified, provide a reason
5	6	7 Moderate	8 Moderate	9 Moderate	10 Moderate	11

Weakness Identifier	Control Family	Control Details	Weakness Description	Weakness Source	POC	Resources Required	Scheduled Completion Date	Milestones With Completion Dates	Changes to Milestones Date	Completion Date	Weakness Status	Risk Level	NEE Version	Compensating Controls	Comments
12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27

1. Non-Exchange Entity: Please enter the name of the Non-Exchange Entity.

2. System Name: Please enter the system name.

3. System Acronym: Please enter the system acronym.

4. Current Fiscal Year: Please enter the current fiscal year.

5. System Name [No Action Required]: This field is auto-filled from the name entered in instruction #2.

6. System Acronym [No Action Required]: This field is auto-filled from the acronym entered in instruction #3.

7. System Criticality: This will be moderate for any system connecting to the Federal Data Services Hub.

8. Confidentiality: This will be moderate for any system connecting to the Federal Data Services Hub.

9. Availability: This will be moderate for any system connecting to the Federal Data Services Hub.

10. Integrity: This will be moderate for any system connecting to the Federal Data Services Hub.

11. If no weaknesses identified, provide a reason [Drop- down list provided]:

Choose from the following six options:
- All weaknesses eliminated
- No review conducted
- No weaknesses found
- System in development
- System reclassified – not a system
- System retired

12. Weakness Identifier: A unique number assigned to each POA&M entry that is used to track the weakness. Typically the weakness identifier is comprised of the following: System name/acronym; Quarter (A, B C, or D) and Fiscal Year the weakness was first recorded; and a sequence number. (example: **SYSTEM_A_2023_3**).

13. Control Family [Drop-down list provided]: Please chose the control family or category that best signifies the origin of the finding.

Choose from the following Options:
- Other
- AC
- AT
- AU
- CA
- CM
- CP
- IA
- IR
- MA
- MP
- PE
- PL
- PS
- RA
- SA
- SC
- SI
- Privacy-AP
- Privacy-AR
- Privacy-DI
- Privacy-DM
- Privacy-IP
- Privacy-SE
- Privacy-TR
- Privacy-UL

14. Control Details: Enter the security control(s) in which the weakness was discovered (examples: **AC-2**, **AU-10**, **IR-2**, and **SA-9**). Multiple controls may be entered if applicable.

15. Weakness Description: Description of the vulnerability or risk identified. This information may be found in the Security Assessment Report (SAR) or other security audit type report.

16. Weakness Source: A source shall be reported for all weaknesses. When recording the weakness source, both the type of review and the date on which the review was conducted or published shall be provided. If the weakness represents a repeat finding, each source in which the weakness was identified shall be documented.

17. Point of Contact (POC): A POC shall be identified and documented for each weakness. The POC shall at a minimum refer to the position/role responsible for resolving the weakness (examples: Information System Security Officer [ISSO], Privacy Coordinator, System Owner), a contact telephone number, and/or an email address.

18. Resources Required: The resources required to successfully complete the weakness shall be estimated and documented. The estimate shall be based on the total resources required to fulfill all the milestones necessary for weakness mitigation. Resources shall be estimated as monetary value and/or staffing requirements. When identifying monetary value, the amount shall be categorized as New Funding, Existing Funding, or Reallocated Funding. Staffing requirements shall be estimated as staff-hours or full time equivalents (FTEs) and categorized as New Staff or Existing Staff.

19. Scheduled Completion Date: A completion date shall be assigned to every weakness, to include the month, day, and year using the format: MMDDYYYY. This date is the estimated date in which all milestones for the weakness will be completed and when the weakness will be closed. The scheduled completion date ***shall not*** change once recorded.

The expected remediation timeline period is based on the risk level.

***Critical*: 15 days**
***High*: 30 days**
***Moderate*: 90 days**
***Low*: 365 days**

y

20. Milestones with Completion Dates: Each weakness shall have at least one milestone with an associated completion date to facilitate corrective action. A milestone will identify specific requirements or key steps to correct an identified finding/action item. Milestone(s) with completion date entries, once recorded, ***shall not*** be removed or changed. Even if you only have ***ONE*** milestone it still needs to contain a completion date.

For ease of reading and managing, it is recommended you number your milestones as shown in the sample below and on the *POA&M Sample* Tab. All milestones should be entered in the single cell provided that corresponds with the identified weakness.

(1) Milestone1 08/10/2024
(2) Milestone2 09/15/2024
(3) Milestone3 10/30/2024

21. Changes to Milestone Completion Dates: Any necessary revisions to the original milestone completion date(s) due to the original date being surpassed because additional time or resources are required, shall be documented. This revised Milestone Completion Date(s) does not replace the original Milestone Completion Date, but is an amendment.

For ease of reading and managing, it is recommended you number your milestone changes as shown in the sample below and on the *POA&M Sample* Tab. It is also recommended you start with the milestone in which the plan has changed. All milestones should be entered in the single cell provided that corresponds with the identified weakness.

(2) Milestone2 10/01/2024
(3) Milestone3 11/15/2024

22. Completion Date: The date that all of the weakness milestones have been completed and the weakness can be closed, to include the month, day, and year using the format: MMDDYYYY. .

23. Weakness Status [Drop-down list provided]: A status shall be assigned to each weakness.

Chose from the following four options:
Ongoing—This status is assigned only when a weakness is in the process of being mitigated and has not yet exceeded the associated Scheduled Completion Date.
Delayed—This status is assigned when a weakness is being mitigated after the associated Scheduled Completion Date has passed. An explanation shall be provided in the Weakness Comments field.
Completed—This status is assigned when all corrective actions have been completed for a weakness such that the weakness is successfully mitigated. Documentation shall be required to demonstrate the weakness has successfully been resolved. The Date of Completion shall be recorded for a completed weakness.
Accepted Risk—This status is assigned when the a weakness has been been accepted as a risk by the NEE entity. A compensating control and comments explaining why the risk has been accepted and mitigating factors that have been implemented to minimize their occurance should be provided. Accepted risks will be reviewed by CMS to determine if it is acceptable for CMS.

24. Risk Level [Drop-down list provided]: Risk level of weakness identified in SAR, Audit, or Review. The assignment of risk levels should follow the methodology outlined in NIST 800-30 Appendices G, H, and I. In assigning risk levels, CMS requires only 4 levels of granularity: Critical, High, Moderate, and Low. (See the *Risk Calculation Instructions* tab for additional information).

The 4 risk levels can be defined as the following:
Critical: A threat event could be expected to have a **multiple severe or catastrophic** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
High: A threat event could be expected to have a ***severe or catastrophic*** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Moderate: A threat event could be expected to have a ***serious*** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Low: A threat event could be expected to have a ***limited*** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.

Choose from the following four options:
Critical
High
Moderate
Low

25. NEE Version: This field is provided to identify the version of the NEE Security and Privacy controls being utilized.

Choose from the following options:
NEE V. 1.0
NEE V. 1.2
NEE V. 2.0
NEE V. 3.0
NEE v. 4.0

26. Compensating Controls: Please list and describe any compensating controls that have been put in place in lieu of the prescribed control(s).

27. Comments: Any additional information or details necessary to clarify weakness information, status and/or traceability shall be documented in the Weakness Comments field.

In determining risk levels, please become familiar with the National Institute of Standards and Technology Special Publication (NIST SP) 800-30 Revision 1.

Below are tables from NIST SP 800-30 Revision 1 for your reference. When assigning risk levels, CMS requires 4 levels of granularity: ***Critical, High***, ***Moderate***, and ***Low***. When utilizing the NIST tables from NIST SP 800-30 Revision 1, Appendices G, H, and I, please consolidate ***Very High*** with ***Critical*** and ***Very Low*** with ***Low***.

From Appendix G

Likelihood of Occurrence

Table G-2: Assessment Scale - Likelihood of Threat Event Initiation (Adversarial)

Qualitative Values	Semi-Quantitative Values		Description
Critical	96-100	10	Adversary is ***almost certain*** to initiate the threat event.
High	80-95	8	Adversary is ***highly likely*** to initiate the threat event.
Moderate	21-79	5	Adversary is ***somewhat likely*** to initiate the treat event.
Low	5-20	2	Adversary is ***unlikely*** to initiate the threat event.
Very Low	0-4	0	Adversary is ***highly unlikely*** to initiate the threat event.

Table G-3: Assessment Scale - Likelihood of Threat Event Occurrence (Non-Adversarial)

Qualitative Values	Semi-Quantitative Values		Description
Critical	96-100	10	Error, accident, or act of nature is ***almost certain*** to occur; or occurs more than 100 times a year.
High	80-95	8	Error, accident, or act of nature is ***highly likely*** to occur; or occurs between 10-100 times a year.
Moderate	21-79	5	Error, accident, or act of nature is ***somewhat likely*** to occur; or occurs between 1-10 times a year.
Low	5-20	2	Error, accident, or act of nature is ***unlikely*** to occur; or occurs less than once a year, but more than once every 10 years.
Very Low	0-4	0	Error, accident, or act of nature is ***highly unlikely*** to occur; or occurs less than once every 10 years.

Table G-4: Assessment Scale - Likelihood of Threat Event Resulting in Adverse Impacts

Qualitative Values	Semi-Quantitative Values		Description
Critical	96-100	10	If the threat event is initiated or occurs, it is ***almost certain*** to have adverse impacts.
High	80-95	8	If the threat event is initiated or occurs, it is ***highly likely*** to have adverse impacts.
Moderate	21-79	5	If the threat event is initiated or occurs, it is ***somewhat likely*** to have adverse impacts.
Low	5-20	2	If the threat event is initiated or occurs, it is ***unlikely*** to have adverse impacts.
Very Low	0-4	0	If the threat event is initiated or occurs, it is ***highly unlikely*** to have adverse impacts.

Table G-5: Assessment Scale - Overall Likelihood

Likelihood of Threat Event Initiation or Occurrence	Likelihood Threat Events Result in Adverse Impacts				
	Very Low	Low	Moderate	High	Critical
Critical	Low	Moderate	High	Critical	Critical
High	Low	Moderate	Moderate	High	Critical
Moderate	Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Moderate	Moderate
Very Low	Very Low	Very Low	Low	Low	Low

From Appendix H

Impact

Table H-2: Examples of Adverse Impacts

Type of Impact	Impact
Harm to Operations	(1) Inability to perform current missions/business functions. -In a sufficiently timely manner. -With sufficient confidence and/or correctness. -Within planned resource constraints (2) Inability, or limited ability, to perform missions/business functions in the future. -Inability to restore missions/business functions. -In a sufficiently timely manner. -With sufficient confidence and/or correctness. -Within planned resource constraints. (3) Harms (e.g., financial costs, sanctions) due to noncompliance. -With applicable laws or regulations. -With contractual requirements or other requirements in other binding agreements (e.g., liability). (4) Direct financial costs. (5) Relational harms. -Damage to trust relationships. -Damage to image or reputation (and hence future or potential trust relationships).

Type of Impact	Impact
Harm to Assets	(1) Damage to or loss of physical facilities. (2) Damage to or loss of information systems or networks. (3) Damage to or loss of information technology or equipment. (4) Damage to or loss of component parts or supplies. (5) Damage to or of loss of information assets. (6) Loss of intellectual property.
Harm to Individuals	(1) Injury or loss of life. (2) Physical or psychological mistreatment. (3) Identity theft. (4) Loss of Personally Identifiable Information. (5) Damage to image or reputation.
Harm to Other Organizations	(1) Harms (e.g., financial costs, sanctions) due to noncompliance. -With applicable laws or regulations. -With contractual requirements or other requirements in other binding agreements. (2) Direct financial costs. (3) Relational harms -Damage to trust relationships. -Damage to reputation (and hence future or potential trust relationships).
Harm to Nation	(1) Damage to or incapacitation of a critical infrastructure sector. (2) Loss of government continuity of operations. (3) Relational harms. -Damage to trust relationships with other governments or with nongovernmental entities. -Damage to national reputation (and hence future or potential trust relationships). (4) Damage to current or future ability to achieve national objectives. -Harm to national security.

Table H-3: Assessment Scale - Impact of Threat Events

Qualitative Values	Semi-Quantitative Values		Description
Critical	96-100	10	The threat event could be expected to have multiple severe or catastrophic adverse effects on organizational operations, organizational assets, individuals, other organizations, or the Nation.
High	80-95	8	The threat event could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation. A severe or catastrophic adverse effect means that, for example, the threat event 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.
Moderate	21-79	5	The threat event could be expected to have a serious adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation. A serious adverse effect means that, for example, the threat event 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.
Low	5-20	2	The threat event could be expected to have a limited adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation. A limited adverse effect means that, for example, the threat event 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.
Very Low	0-4	0	The threat event could be expected to have a negligible adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation.

From Appendix I

Risk Determination

Table I-2: Assessment Scale - Level of Risk (Combination of Likelihood and Impact)

Likelihood (Threat Event Occurs and Results in Adverse Impact)	Level of Impact				
	Very Low	Low	Moderate	High	Critical
Critical	Very Low	Low	Moderate	High	Critical
High	Very Low	Low	Moderate	High	Critical
Moderate	Very Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Low	Moderate
Very Low	Very Low	Very Low	Very Low	Low	Low

Table I-3: Assessment Scale - Level of Risk

Qualitative Values	Semi-Quantitative Values		Description
Critical	96-100	10	**Critical risk** means that a threat event could be expected to have multiple severe or catastrophic adverse effects on organizational operations, organizational assets, individuals, other organizations, or the Nation.
High	80-95	8	**High risk** means that a threat event could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Moderate	21-79	5	**Moderate risk** means that a threat event could be expected to have a serious adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Low	5-20	2	**Low risk** means that a threat event could be expected to have a limited adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Very Low	0-4	0	**Very low risk** means that a threat event could be expected to have a negligible adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.

CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES
OFFICE OF INFORMATION SERVICES

NON-EXCHANGE ENTITY:	**NEE1 SAMPLE**
SYSTEM NAME:	**NEE1 System 1 SAMPLE**
SYSTEM ACRONYM:	**N1S1**
CURRENT FISCAL YEAR:	**2024**

System Name	System Acronym	System Criticality as defined by FIPS	Confidentiality	Availability	Integrity	If no weaknesses identified, provide a reason
NEE1 System 1 SAMPLE	N1S1	**Moderate**	**Moderate**	**Moderate**	**Moderate**	

Weakness Identifier	Control Family	Control Details	Weakness Description	Weakness Source	POC	Resources Required	Scheduled Completion Date	Milestones With Completion Dates	Changes to Milestones Date	Completion Date	Weakness Status	Risk Level	NEE Version	Compensating Controls	Comments
TESTSYS_A_2023_2	AC	AC-2	Account Management process is not documented.	Initial Security Assessment Review 02/12/23	John Doe, CISO	8 hours Existing Staff	03/15/2023	(1) Create an account management process 02/28/2023 (2) Document process 03/01/2023 (3) Review process with staff 03/10/2023 (4) Implement Process 03/12/2023 (5) Review effective of new process 03/14/2023 (6) Update POA&M 03/15/2023	(1) Create an account management process 02/15/2023 (2) Document process 02/20/2023 (3) Review process with staff 02/25/2023 (4) Implement Process 02/26/2023 (5) Review effective of new process 02/28/2023 (6) Update POA&M 03/01/2023	03/01/2023	Completed	Moderate		N/A	
TESTSYS_A_2023_1	PE	PE-10	There is no EPO in server room 1.	Initial Security Assessment Review 02/12/23	John Doe, CISO	20 hours Existing Staff $65,000 Professional Services and Equipment	08/01/2023	(1) Solicit vendors to provide EPO solution and estimate of cost 02/25/2023 (2) Choose vendor to perform work 04/15/2023 (3) Initiate the install of the emergency power shutoff solution 07/01/2023 (4) Test the implemented EPO solution 07/15/2023 (5) Finalize solution and update POA&M 08/01/2023	(3) Initiate the install of the emergency power shutoff solution 05/01/2024 (4) Test the implemented EPO solution 05/15/2024 (5) Finalize solution and update POA&M 06/01/2024		Delayed	Moderate		N/A	Awaiting funding to implement EPO solution
TESTSYS_A_2023_1	IA	IA-5	Update the control implementation statement to document the processes used to implement control requirements a-f, h, and i.	SSP Review 06/10/2023	John Doe, CISO	10 hours Existing Staff	07/30/2023	(1) Update the implementation standards a-f, h, and i for IA-5 in the SSP 06/20/2023 (2) Review changes to the SSP with the security staff 07/01/2023 (3) Finalize the implementation standards based on staff comments and recommendations 07/30/2023		07/30/2023	Completed	Low		N/A	
TESTSYS_A_2024_3	PE	PE6.2	Lack of processes for: (a) reviewing physical access logs at least once every two months, and (b) coordinating results of reviews and investigations with the organization's incident response capability.	Annual Attestation 03/01/2024	John Doe, CISO	20 hours Existing Staff	05/20/2024	(1) Create a process reviewing physical access logs at least once every two months and coordinating results of reviews and investigations with the organization's incident response capability 03/08/2024 (2) Document process 04/01/2024 (3) Review process with staff 04/15/2024 (4) Implement Process 05/01/2024 (5) Review effective of new process 05/15/2024 (6) Update POA&M 05/20/2024			Ongoing	Low		N/A	
TESTSYS_A_2024_4	SI	SI-2	Windows server BD1-3 has not been patched in 3 months	Annual Attestation 03/01/2024	John Doe, CISO	40 hours Existing Staff	03/15/2024	(1) Develop a plan and schedule to patch the servers monthly. Update the SSP to reflect the plan to patch the servers 03/15/2024 (2) Test the outstanding patches in the test environment (3) Implement patches on the production server	(2) Continuing testing in the test environment (3) Implement patches on the production server		Delayed	High		N/A	Need additional testing due to possible adverse affects of applying the patch. MS24-013 (KB2929961)
TESTSYS_A_2024_5	RA	RA-5	The organization does not employ vulnerability scanning tools	Annual Attestation 03/01/2024	John Doe, CISO	80 hours Existing Staff $3000 Tools and Training	04/01/2024	(1) Shop vulnerability scanning tools 03/05/2024 (2) Select vulnerability scanning tool 03/10/2024 (3) Obtain training on the product 03/15/2024 (4) Test product in the test environment 03/20/2024 (5) Implement solution in production and monitor 04/01/2024			Ongoing	High		N/A	

Weakness Status	Risk Level	No weaknesses identified	Fiscal Year	Control	Non-Exchange Entity Security and Privacy Version
Ongoing	Critical	All weaknesses eliminated	2018	**Other**	**NEE V. 1.0**
Completed	High	No review conducted	2019	**AC**	**NEE V. 1.2**
Delayed	Moderate	No weaknesses found	2020	**AT**	**NEE V. 2.0**
Accepted Risk	Low	System in development	2021	**AU**	**NEE V. 3.0**
		System reclassified – not a system	2022	**CA**	**NEE V. 4.0**
		System retired	2023	**CM**	
			2024	**CP**	
			2025	**IA**	
			2026	**IR**	
			2027	**MA**	
			2028	**MP**	
			2029	**PE**	
			2030	**PL**	
				PS	
				RA	
				SA	
				SC	
				SI	
				Privacy - AP	
				Privacy - AR	
				Privacy - DI	
				Privacy - DM	
				Privacy - IP	
				Privacy - SE	
				Privacy - TR	
				Privacy - UL	

Record of Changes					
Number	Date	Reference	A = Add M = Modify D = Delete	Description of Change	Change Request #
1.00	22-Jan-2018		M	Conversion of MARS-E 2.0 POA&M template v4.2 to Non Exchange Entity POA&M template v1.0; Updated Year range to 2018-2023; Updated Version column F to NEE; updated control families to match NEE controls set; Removed AE on multiple tabs and replaced with NEE; updated POA&M metrics page for new NEE versioning; updated changelog and reset; updated datasheet for versioning; updated sample.	N/A
1.20	1-Feb-2018		M	description of Change	N/A
1.21	20-Jun-2018		M	Corrected hidden row 17 issue with filtering	N/A
1.22	7-Nov-2018		A, M	(1) Errata fixes to POA&M template, POA&M Instructions and Risk Calculation instructions to correct spacing, row heights, formatting and adjustments to wording for clarity.; (2) Extending out Fiscal year to 2030, updated Data sheet and POA&M Template sheet; (3) Update to Metrics and POA&M template sheet for FISCAL Year drop down placement (4) Added 28 on POA&M Instructions sheet. "Completed POA&M items may be archived 1 year after completion"; (5) Update to Privacy Metrics COUNTIF formula on POA&M Metrics sheet; (6) Update Metrics sheet to capture data already entered on POA&M Template sheet to reduce replicative entries	N/A
1.30	20-Mar-2019		A, M	1) Extended metric formula range to 5000 rows. 2) Extended filter and drop down ranges to include new rows. 3) Locked Column Name/Filter row. 4) Added Risk Subtotal on the template page. 5) Rows change color based on risk level selected. 6) Updated drop down list for NEE Version column and expanded metric page tracking for additional versions. 7) Spell check updates.	N/A
1.40	3-Dec-2020		A	1) Updated Data Sheet and POA&M tab to include "Critical" to Drop down list for risk levels 2) Update to Risk Calculation instructions tab to align with HHS guidance, adding in "Critical" severity to the previously listed “Very High” from NIST guidance. 3) Updated Metrics tab to include tracking of Critical level risks. 4) Updated POA&M instructions tab for critical findings and NEE versioning selection. 5) Added NEE V. 3.0 for drop down in column N and updated POA&M instructions tabs to include NEE V. 3.0. 6) Updated Metrics tab to include tracking of NEE V. 3.0 statuses. 7) Added remediation timeline based on risk level to the POA&M instructions tab.	N/A
1.50	11-Feb-2022		A	1) Updated conditional formatting for risk level findings. High findings have been changed from red to orange. Critical is now red. 2) Added NEE V. 3.1 for drop down in column N and updated POA&M instructions tabs to include NEE V. 3.1. 3) Updated Metrics tab to include tracking of NEE V. 3.1 statuses. 4) Corrected total findings metric's formulas to include critical findings. 5) Updated cell formatting in the Template, POA&M and Risk Calculation tabs. 6) Updated date formats in the Sample tab. 7) Added new dropdown item "Accepted Risks" for Weakness Status column. 8) Updated metrics tab to include forumla tracking for Accepted Risks. 9) Updated instructions tab to include description for Accepted Risks.	N/A
1.51	18-Feb-2022		M	1) Updated all references to note NEE version changes made by MITRE upon finalization of NEE V. 4.0 (previously said to be V. 3.1). 2) Updated errors in recent Change Log entries	N/A
1.52	10-Oct-2023		M	1) Removed watermark on POA&M Sample tab to conform with 508 compliance, and added "SAMPLE" to NON-EXCHANGE ENTITY name and SYSTEM NAME.	N/A