DEPARTMENT OF HEALTH & HUMAN SERVICES
Centers for Medicare & Medicaid Services
7500 Security Boulevard, Mail Stop N3-13-27
Baltimore, Maryland 21244-1850

CENTERS FOR MEDICARE & MEDICAID SERVICES (CMS)

Office of Information Technology (OIT)
Information Security and Privacy Group (ISPG)
7500 Security Blvd
Baltimore, MD 21244-1850

CMS INTERCONNECTION SECURITY AGREEMENT (ISA)

Between

CENTERS FOR MEDICARE & MEDICAID SERVICES (CMS)

And

<Insert Non-CMS Organization Name>

FINAL
Version <Insert #>
<INSERT ISA Date>
ISA Template January 9, 2019 – Version 1.2

TABLE OF CONTENTS

This CMS and **<Insert Non-CMS Organization Name>** ISA Review Log is maintained to record the annual reviews. The CMS and **<Insert Non-CMS Organization Name>** ISA Review Log is provided below.

REVIEW LOG

Date of Review	Initials of Reviewer	Name of Reviewer	Organization of Reviewer	ISA Version
<INSERT DATE OF THE REVIEW>	<INSERT INITIALS OF THE REVIEWER>	<INSERT STAFF NAME OF THE REVIEWER>	<INSERT STAFF REVIEWER'S ORGANIZATION>	<INSERT ISA VERSION REVIEWED>

1. PURPOSE

The purpose of this Interconnection Security Agreement (ISA) is to establish procedures for mutual cooperation and coordination between the Centers for Medicare & Medicaid Services (CMS) and **<Insert Non-CMS Organization Name>** hereafter referenced as the "Non-CMS Organization", regarding the development, management, operation, and security of a connection between CMS' **<Insert CMS' Network Name & Acronym>** , hereafter known as the CMS Network, and the Non-CMS Organization's network. This ISA is intended to minimize security risks and ensure the confidentiality, integrity, and availability (CIA) of CMS information[1] as well as the information that is owned by the external organization that has a network interconnection[2] with CMS. This ISA ensures the adequate security[3] of CMS information being accessed and provides that all network access satisfies the mission requirements of both CMS and Non-CMS Organization hereafter known as "both parties".

Federal policy requires agencies to develop ISAs for federal information systems and networks that share or exchange information with external information systems and networks. This ISA is based on the National Institute of Standards and Technology (NIST) *Security Guide for Interconnecting Information Technology Systems* (Special Publication (SP) 800-47 http://csrc.nist.gov/publications/PubsSPs.html). NIST SP 800-47 states: "A system that is approved by an ISA for interconnection with one organization's system shall meet the protection requirements equal to, or greater than, those implemented by the other organization's system." The guidelines establish information security (IS) measures that shall be taken to protect the connected systems and shared data. CMS IT managers and IS personnel shall comply with NIST SP 800-47, or any successor document in managing the process of interconnecting information systems and networks.

The ISA contains all information both parties need to understand their responsibilities to each other in protecting the privacy and security of the systems they will connect and the information they will use that connection to transmit. In addition to assigning specific responsibilities to each party, it outlines security safeguards, including administrative, operational, and technical requirements. Administrative requirements include the business and legal requirements for each party, setting out contractual obligations and listing appropriate recourses. It also authorizes mutual permission to connect both parties and establishes a commitment to protect data that is exchanged between the networks or processed and stored on systems that reside on the networks. Through this ISA, both parties shall minimize the susceptibility of their connected systems and networks to IS risks and aid in mitigation and recovery from IS incidents.

---

[1] ***"Information"*** is defined as "any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics, that is owned by, produced by or for, or is under the control of the United States Government." (Executive Order 12958)

[2] ***"Network interconnection"*** is defined as "the direct connection of two or more IT networks for the purpose of sharing data and other information resources." (This is based on the definition of system interconnection in NIST SP 800-47, Security Guide for Interconnecting Information Technology Systems)

[3] ***"Adequate security"*** is defined as "a level of security that is commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information." (Office of Management and Budget (OMB) Circular A-130)

2. CMS BACKGROUND

2.1 CMS

As an agency of the Department of Health and Human Services (DHHS), CMS administers the Medicare, Medicaid, and State Children's Health Insurance Program (SCHIP) programs. Its mission is to ensure effective, up-to-date health care coverage and to promote quality care for beneficiaries.

2.2 CMS INFORMATION SECURITY PROGRAM

The CMS IS Program helps CMS accomplish its mission by ensuring the CIA of CMS information resources. The CMS IS Program has developed policies, standards, procedures, and guidelines that ensure the adequate protection of agency information and comply with Federal laws and regulations. CMS monitors the security of its network twenty-four (24) hours a day, seven (7) days a week, i.e., 24/7, through a variety of administrative, operational, and technical processes. Training initiatives are continuously updated to ensure that managers, users, and technical personnel are aware that they are responsible for the adequate security of their information systems.

2.3 CMS ROLES AND RESPONSIBILITIES

2.3.1 CMS Chief Information Officer (CIO)

The CMS CIO is responsible for the overall implementation and administration of the CMS Information Security Program.

2.3.2 CMS CHIEF INFORMATION SECURITY OFFICER (CISO)

The CMS CISO supports the CIO in the implementation of the CMS IS Program. The CMS CISO directs, coordinates, and evaluates the IS policy of CMS.

2.3.3 CMS INFORMATION SYSTEM SECURITY OFFICER (ISSO)

The CMS ISSO is the liaison for IS within their assigned portfolio of systems. ISSOs implement standard IS policies and collaborate across CMS concerning the CIA of information resources. Although the ISSOs report directly to their own management, as part of their IS responsibilities, the ISSOs have responsibilities to the CMS CISO and thus, to the CMS CIO. In their IS role, ISSOs take direction from the CMS CIO or the CMS CISO when action is required to protect CMS assets from potential vulnerabilities and threats. The CMS CISO and ISSOs will work with Non-CMS Organization to enhance IS measures.

2.3.4 CMS BUSINESS OWNERS (BO)

The CMS Business Owner (BO) is responsible for the management and oversight of the**<Insert CMS information system name & acronym>** hereafter known as the CMS information system that requires the interconnection with the Non-CMS Organization. The BO serves as the primary

point of contact (POC) for the Non-CMS Organization on matters related to **<Insert CMS information system name & acronym>** .

3. NON-CMS ORGANIZATION BACKGROUND

3.1 NON-CMS ORGANIZATION

<Insert background information about Organization B, including a brief description of the organization and its mission>

3.2 IT SECURITY PROGRAM

<Insert a brief description of Organization IS program>

3.3 ROLES AND RESPONSIBILITIES

<Insert a brief description of each role and associated responsibilities of the Non-CMS Organization that are equivalent to the CMS roles and responsible for implementing IT and IS policies, procedures, and tools that support CIA.>

3.3.1 (ROLE)

<Insert roles and responsibilities>

3.3.2 (ROLE)

<Insert roles and responsibilities>

3.3.3 (ROLE)

<Insert roles and responsibilities>

3.3.4 (ROLE)

<Insert roles and responsibilities>

3.3.5 (ROLE)

<Insert roles and responsibilities>

4. SCOPE

The scope of this ISA is based on the following, but not limited to the:

- Interconnection between CMS information system and the Non-CMS Organization.
- Existing and future users including employees from both parties, contractors and subcontractors at any tier; and other federally and non-federally-funded users managing, engineering, accessing, or utilizing the Non-CMS Organization Network.
- Related network components belonging to both parties, such as hosts, routers, and switches; IT devices that assist in managing security such as firewalls, intrusion detection

systems (IDS), and vulnerability scanning tools; desktop workstations; servers; and major applications (MA) that are associated with the network connection between both parties[4].

5. AUTHORITY

By interconnecting with the CMS network and CMS information system, Non-CMS Organization agrees to be bound by this ISA and the use of CMS Network and CMS information system in compliance with this ISA.

The authority for this ISA is based on the following, but not limited to the:

- Federal Information Security Management Act of 2002 (FISMA);
- OMB Circular A-130, Appendix III, *Security of Federal Automated Information Systems;*
- 18 United States Code U.S.C. 641 Criminal Code: Public Money, Property or Records;
- 18 U.S.C. 1905 Criminal Code: Disclosure of Confidential Information;
- Privacy Act of 1974, 5 U.S.C. § 552a; and
- Health Insurance Portability and Accountability Act (HIPAA) of 1996 P.L. 104-191 (only if there is an exchange of PHI)

This ISA is also in compliance with DHHS policies listed at http://www.hhs.gov/read/irmpolicy/, and CMS policies listed at the CMS IS webpage http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/. These sites may be updated periodically. Where new policies and guidance affect the content of this ISA, the ISA will continue to be in effect, and will updated at its next periodic review.

6. STATEMENT OF REQUIREMENTS

The expected benefit of the interconnection is **<Insert Business Expectation>**

6.1 GENERAL INFORMATION/DATA DESCRIPTION

<Insert a description of the information and data that will be made available, exchanged, or passed one-way only by the interconnection of the two systems / networks>

[4] A ***"major application"*** is an application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. (OMB A-130)

6.2 SERVICES OFFERED

CMS shall:

- Provide 24/7 operation of the CMS IT Service Desk (1-800-562-1963, 410-786-2580 or mailto:cms_it_service.desk@cms.hhs.gov) for the Non-CMS Organization Point of Contact (POC) to communicate any security issues; and
- Provide installation, configuration, and maintenance of CMS edge router(s) with interfaces to multiple CMS core and edge routers.

The Non-CMS Organization shall:

<Insert Non-CMS Organization IT Help Desk information regarding operating times, process, and contact information>

7. SYSTEM DESCRIPTIONS

7.1 CMS SYSTEM

Name: CMS
Function: <Insert CMS' System Function>
Location: <Insert CMS physical site location>

Description of data, including Sensitivity or Classification level: **<Insert description>**

Describe and document the information handled by the system and the overall system security level as LOW, MODERATE or HIGH. Refer to the *CMS Information Security Levels* document on

	Information Category	Level
Security Level	**<Select and enter the Information Category from the System Security Level referenced above. Insert all entites that are applicable.>**	**<Insert HIGH, MODERATE or LOW.>**

Overall Security Level Designation: **<Insert highest level from the table above>**

7.2 NON-CMS ORGANIZATION SYSTEM

Name: <Insert Organization B's System>
Function: **<Insert Organization B's System Function>**

Location: <Insert Organization B's Physical Site Location>

Description of data, including Sensitivity or Classification level: **<Insert description>**

Describe and document the information handled by the system and the overall system security level as LOW, MODERATE or HIGH. Refer to the NIST FIPS 199[5]. For additional guidance refer to *CMS Risk Management Handbook Chapter 12 Security and Privacy Planning, Sections 3.1.5-3.1.7.*[6]

	Information Category	Level
Security Level	**<Select and enter the Information Category from the System Security Level referenced above. Insert all entites that are applicable.>**	**<Insert HIGH, MODERATE or LOW.>**

Overall Security Level Designation: **<Insert highest level from the table above>**

7.3 TOPOLOGICAL DIAGRAM

Appendix A of this ISA must include a topological drawing that illustrates the interconnectivity between both systems, including all components (e.g., firewalls, routers, switches, hubs, servers, encryption devices, computer workstations, and storage location for receiving system). Both parties shall notify each other of any requirements such as additional router connections or increases in volume associated with this ISA.

8. SECURITY RESPONSIBILITIES

Both parties shall maintain a level of security that is commensurate with the risk and magnitude of the harm that could result from the loss, misuse, disclosure, or modification of the information contained on the system with the highest sensitivity levels.

[5] http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf
[6] https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/RMH-Chapter-12-Security-and-Privacy-Planning.pdf

8.1 COMMUNICATION/INFORMATION SECURITY POINTS OF CONTACT

Both parties shall:

- Designate a technical lead for their respective network and provide POC information to facilitate direct contacts between technical leads to support the management and operation of the interconnection;
- Maintain open lines of communication between POCs at both the managerial and technical levels to ensure the successful management and operation of the interconnection; and
- Inform their counterpart promptly of any change in technical POCs and interconnections.

CMS shall:

- Inform their counterpart promptly of any change in technical POC and interconnection;
- Identify a CMS ISSO to serve as a liaison between both parties and assist the Non-CMS Organization in ensuring that its IS controls meet or exceed CMS requirements.

Non-CMS Organization shall designate an IS POC the equivalent of the CMS ISSO, who shall act on behalf of the Non-CMS Organization and communicate all IS issues involving the Non-CMS Organization to CMS via the CMS ISSO.

8.2 RESPONSIBLE PARTIES

Appendix B is a list of the responsible parties and contacts for each system. It is the responsibility of each respective approving authority to ensure the timely updating of Appendix B and for the notification of such changes to the alternate party within 30 days of any personnel change. Updating Appendix B does not require the re-signing of this ISA by either party.

9. PERSONNEL/USER SECURITY

9.1 USER COMMUNITY

Both parties shall:

- Ensure that all employees, contractors, and other authorized users with access to the CMS Network and the Non-CMS Organization and the data sent and received from either organization are not security risks and meet the requirements of the Office of Management and Budget (OMB) at http://www.whitehouse.gov/omb/ and the HHS Office of Security and Drug Testing, Personnel Security/Suitability Handbook, dated February 1, 2005.

- Enforce the following IS best practices:
  - Least Privilege: Only authorizing access to the minimal amount of resources required for a function;

- Separation of Duties: A basic control that prevents or detects errors and irregularities by assigning responsibility for initiating transactions, recording transactions and custody of assets to separate individuals; and
- Role-Based Security: Access controls to perform certain operations ('permissions') are assigned to specific roles.

9.2 COMMITMENT TO PROTECT SENSITIVE INFORMATION

Both parties shall not release, publish, or disclose information to unauthorized personnel, and shall protect such information in accordance with provisions of the laws cited in Section 5 and any other pertinent laws and regulations governing the adequate safeguard of the agency.

The Non-CMS Organization shall:

- Ensure that each of the Non-CMS Organization contractor employee signs form CMS R-0235, CMS Data Use Agreement at http://www.cms.gov/Medicare/CMS-Forms/CMS-Forms/downloads/cms-r-0235.pdf.
- Ensure that outsourced operations where non-CMS personnel may have access to information, CMS systems, and network components shall also comply with the security required by Federal Acquisition Regulation (FAR) clause 52.239-1, Privacy or Security Safeguards and CMS IS policies, standards, and procedures.

9.3 TRAINING AND AWARENESS

Both parties shall have all users, including employees, contractors, and other authorized users complete the CMS IS awareness training upon enactment of this ISA and then annually thereafter at: https://www.cms.gov/cbt/.

9.4 PERSONNEL CHANGES/DE-REGISTRATION

Both parties shall:

- Provide notification to their respective BOs of the separation or long-term absence of their network owner or technical lead.
- Provide notification to their respective BO of any changes in the ISSO or POC information.
- Provide notification to the CMS Access Administrator (CAA) of changes to user profiles, including users who resign or change job responsibilities. For a list of current CAA see: https://vpnext.cms.hhs.gov/EUADOCS.

10. POLICIES

Both parties shall adhere to all DHHS and CMS IS policies, procedures, and guidelines in the *CMS Information Security and Privacy Library* at https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html

10.1 RULES OF BEHAVIOR

Both parties shall ensure that all users with access to the CMS Network, the CMS information system, the Non-CMS Organization network and any data received from the other organization shall adhere to all current *HHS Rules of Behavior (RoB) (For Use of Technology Resources and Information)*, which is available at http://www.hhs.gov/ocio/policy/.

10.2 SECURITY DOCUMENTATION

Both parties shall ensure that security is planned for, documented, and integrated into the System Life-Cycle from the IT system's initiation to the system's disposal. For guidance, see *CMS eXpedited Life Cycle* at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/XLC/index.html and the *CMS Risk management Handbook* at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html.

CMS shall review the *CMS System Security Plan (SSP)* for CMS information system and the CMS network annually and update when a major modification as required by the CMS SSP Procedures.

The Non-CMS Organization shall:

- Maintain an SSP on the Non-CMS Organization's network and update whenever there is a major modification. The SSP shall be compliant with the CMS Risk Management Handbook procedures at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html and the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-18 *Guide for Developing Security Plans for IT Systems* at http://csrc.nist.gov/publications/PubsSPs.html.
- Make accessible to CMS all IS program documents from the Non-CMS Organization.

11. NETWORK SECURITY

11.1 NETWORK MANAGEMENT

Both parties shall:

- Ensure that this interconnection is completely isolated from the Internet.
- Ensure that this interconnection is completely isolated from all other customer / business processes.

11.2 MATERIAL NETWORK CHANGES

Both parties shall:

- Submit to the CMS CIO any proposed changes to either network or the interconnecting medium accompanied by a valid business justification;

- Renegotiate this ISA before any changes are implemented;
- Report planned technical changes to the network architecture that affect the interconnection through the CMS BO to the Office of Information Technology (OIT), Infrastructure User Services Group (IUSG);
- Conduct a risk assessment based on the new network architecture and modify and re-sign this ISA within one (1) month prior to implementation;
- Conduct a Security Impact Analysis (SIA) based on the new network architecture and modify and re-sign this ISA within one (1) month prior to implementation; and
- Notify the respective BOs and OIT, IUSG (through the CMS BO) when access is no longer required.

11.3 NEW INTERCONNECTIONS

Both parties shall prohibit new interconnections unless expressly agreed upon in a modification to this ISA and signed by both parties.

11.4 NETWORK INVENTORY

Non-CMS Organization shall maintain and make available to CMS upon request a list of all Non-CMS Organization subnets connected to CMS' network and periodically update the information including information on each owner, physical location, IP address, host's name, hardware, operating system version, and applications.

11.5 FIREWALL MANAGEMENT

- Configure the CMS network perimeter firewall in accordance with OIT, IUSG.
- Block all network traffic incoming from the Internet to CMS unless it is explicitly permitted.
- Install a firewall between the perimeter (demarcation point) of the Non-CMS Organization's network and CMS' network if deemed necessary by OIT, IUSG.

The Non-CMS Organization shall:

- Maintain responsibility for configuring all Non-CMS Organization network perimeter firewalls with a policy at least as stringent as OIT, IUSG.
- Provide to OIT, IUSG through the CMS BO a list of Non-CMS Organization authorized web (HTTP), FTP and SMTP servers (identified individually as HTTP, FTP, and/or SMTP) on the Non-CMS Organization's network.

12. INCIDENT PREVENTION, DETECTION, AND RESPONSE

12.1 INCIDENT HANDLING

Both parties shall:

- Handle and report incidents in accordance with the *CMS RMH Chapter 8 Incident Handling* at the CMS IS webpage https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/RMH-Chapter-08-Incident-Response.pdf; and
- Notify their designated technical counterparts immediately by telephone or e-mail when a security incident is detected, so that the other party may take steps to determine whether its network has been compromised and to take appropriate security precautions.

12.2 VULNERABILITY SCANNING

Both parties shall:

- Disseminate intrusion detection alerts to respective BO counterparts for all subnets within the scope of this ISA;
- Report to the both the CMS BO and the Non-CMS Organization's BO any security incident that either organizations subnets within the scope of this ISA; and
- Block inbound and outbound access for any CMS or Non-CMS Organization information systems on the subnets within the scope of this ISA that are the source of unauthorized access attempts, or the subject of any security events, until the risk is remediated.

12.3 DISASTERS AND OTHER CONTINGENCIES

Both parties shall notify immediately their designated counterparts as defined in the information system contingency plan in the event of a disaster or other contingency that disrupts the normal operation of one or both of the connected networks.

13. MODIFICATIONS

If any personnel changes occur involving the POCs listed in this ISA, the terms of this ISA shall remain in full force and effect, unless formally modified by both parties. Any modifications that change the security posture to this ISA shall be in writing and agreed upon and approved in writing by either parties or their designees.

14. COMPLIANCE

Non-compliance with the terms of this ISA by either party may lead to termination of the interconnection. CMS may block network access for the Non-CMS Organization if the Non-CMS Organization does not implement reasonable precautions to prevent the risk of security incidents spreading to CMS' network. CMS is authorized to audit the security of Non-CMS Organization's Network periodically by requesting that Non-CMS Organization provide documentation of compliance with the security requirements in this ISA (see Section 20,

RECORDS). The Non-CMS Organization shall provide CMS access to its IT resources impacted by this ISA for the purposes of audits.

15. COST CONSIDERATIONS

Both parties agree to be responsible for their own systems and costs of the interconnecting mechanism and/or media. No financial commitments to reimburse the other party shall be made without the written concurrence of both parties. Modifications to either system that are necessary to support the interconnection are the responsibility of the respective system/network owners' organization. This ISA does not authorize, require, nor preclude any transfer of funds without the agreement of both parties.

16. TIMELINE

This ISA shall become effective upon the signature of the parties involved and remain in effect until terminated by either party. This ISA is subject to annual review and must be reauthorized when significant changes (that can affect the security state of the information system) are implemented that impact that validity of the agreement as an effective enforcement of security requirements. . If one or both of the parties wish to terminate this agreement, they may do so upon thirty (30) days written notice or in an event of a security incident or suspected incident CMS has the right to immediately terminate the connection.

17. ORDER OF PRECEDENCE

In the event of an inconsistency between the terms and conditions of this ISA and the terms and conditions of any other agreement, memorandum of understanding, or acquisition between CMS and Non-CMS Organization, the terms and conditions of this ISA shall have precedence.

18. CONFIDENTIALITY

Subject to applicable statutes and regulations, including the Freedom of Information Act, the parties agree that the terms and conditions (any proprietary information) of this ISA shall not be disclosed to any third party outside of the Government without the prior written consent of the other party.

19. SURVIVAL

The parties' rights and obligations shall survive expiration or termination of this ISA.

20. RECORDS

The Non-CMS Organization shall maintain all records that it may create in the normal course of its business in connection with activity under this ISA for the term of this ISA and for at least three (3) years after the date this ISA terminates or expires. Such records shall be made available to CMS to ensure compliance with the terms and conditions of this ISA. The records shall be made available during regular business hours at the Non-CMS Organization offices, and CMS' review shall not interfere unreasonably with the Non-CMS Organization business activities.

21. ASSIGNMENT

If any term or condition of this ISA becomes inoperative or unenforceable for any reason, such circumstances shall not have the effect of rendering the term or condition in question inoperative or unenforceable in any other case or circumstances, or of rendering any other term or condition contained in this ISA to be invalid, inoperative, or unenforceable to any extent whatsoever. The invalidity of a term or condition of this ISA shall not affect the remaining terms and conditions of this ISA.

22. SEVERABILITY

If any term or condition of this ISA becomes inoperative or unenforceable for any reason, such circumstances shall not have the effect of rendering the term or condition in question inoperative or unenforceable in any other case or circumstances, or of rendering any other term or condition contained in this ISA to be invalid, inoperative, or unenforceable to any extent whatsoever. The invalidity of a term or condition of this ISA shall not affect the remaining terms and conditions of this ISA.

23. WARRANTY

CMS does not warrant that Non-CMS Organization interconnection to the CMS' network under this ISA will meet Non-CMS Organization requirements, expectations, or even the stated expected benefit of Non-CMS Organization interconnection to the CMS (see Provision 6, Statement of Requirements). Non-CMS Organization bears the entire risk regarding the quality and performance of its interconnection with the CMS, and Non-CMS Organization exclusive remedy is to terminate this ISA in accordance with the terms and conditions herein.

CMS EXPRESSLY DISCLAIMS ALL WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE WITH REGARD TO NON-CMS ORGANIZATION'S INTERCONNECTION TO THE CMS.

24. LIMITATION OF LIABILITY

UNDER NO CIRCUMSTANCES AND UNDER NO LEGAL THEORY, WHETHER TORT (INCLUDING NEGLIGENCE), CONTRACT, OR OTHERWISE, SHALL CMS BE LIABLE TO NON-CMS ORGANIZATION OR ANY OTHER PERSON FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY CHARACTER INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF GOODWILL, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, OR ANY AND ALL OTHER COMMERCIAL DAMAGES OR LOSSES, EVEN IF SUCH PARTY SHALL HAVE BEEN INFORMED OF THE POSSIBILITY OF SUCH DAMAGES.

25. FORCE MAJEURE

Non-CMS Organization failure to comply with any term or condition of this ISA as a result of conditions beyond its fault, negligence, or reasonable control (such as, but not limited to, war,

strikes, floods, governmental restrictions, riots, fire, other natural disasters or similar causes beyond Non-CMS Organization control) shall not be deemed a breach of this ISA.

26. SIGNATURES

Both parties agree to work together to ensure the joint security of the connected networks and the data they store, process, and transmit, as specified in this ISA. Each party certifies that its respective network is designed, managed, and operated in compliance with all relevant federal laws, regulations, and policies.

We agree to the terms and conditions of this ISA.

Director, OIT/IUSG

(Name)

(Signature) (Date)

Project Manager (equivalent)

(Name)

(Signature) (Date)

CMS Chief Information Security Officer

(Name)

(Signature) (Date)

Chief Information Security Officer (equivalent)

(Name)

(Signature) (Date)

CMS ISSO

(Name)

(Signature) (Date)

ISSO (equivalent)

(Name)

(Signature) (Date)

CMS Business Owner

(Name)

(Signature) (Date)

Business Owner (equivalent)

(Name)

(Signature) (Date)

CMS Project Officer

(Name)

(Title)

(Signature) (Date)