



ROBERT L. QUINN
COMMISSIONER OF
SAFETY

State of New Hampshire

DEPARTMENT OF SAFETY
JAMES H. HAYES BLDG. 33 HAZEN DR.
CONCORD, N.H. 03305
(603) 271-2791

October 22, 2020

His Excellency, Governor Christopher T. Sununu
and the Honorable Council
State House
Concord, New Hampshire 03301

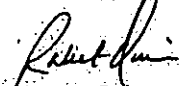
Requested Action:

Authorize the Department of Safety, Division of State Police (NHSP), to enter into a no-cost Memorandum of Understanding (MOU) with the US Department of Transportation (US DOT) Federal Motor Carrier Safety Administration (FMCSA) to establish expectations between FMCSA and the NHSP. Effective upon Governor and Council approval through July 27, 2023.

Explanation:

This MOU is intended to document the methodology and required privacy and security safeguards to support data sharing between the FMCSA Safety and Fitness Electronic Records (SAFER) System and the Performance and Registration Information Systems Management (PRISM) System, which includes interfaces with NHSP commercial motor vehicle inspection software programs including Inspect and CVIEW. These programs are used by NHSP Troopers when conducting commercial motor vehicle enforcement activities in New Hampshire.

Respectfully submitted,


Robert L. Quinn
Commissioner of Safety

**U.S. DEPARTMENT OF TRANSPORTATION
FEDERAL MOTOR CARRIER SAFETY ADMINISTRATION
Office of Information Technology**



MEMORANDUM OF UNDERSTANDING

Between

**The U.S. Department of Transportation (US DOT) Federal Motor Carrier Safety
Administration (FMCSA)
<SAFER System and PRISM System>**

And

**New Hampshire Department of Safety, Division of State Police
Non-FMCSA System hosted and operated by Iteris, Inc.
Version 3.0**

**Effective: 07/01/2020 to 06/30/2023
(Not to Exceed Three Years)**

FOR OFFICIAL USE ONLY
MOU between FMCSA and State Partner

1. Effective Date:

This Memorandum of Understanding (MOU) and the associated Interconnection Security Agreement (ISA) (Appendix I), which is incorporated by reference, supersede and replace any prior MOUs and/or ISA agreements. This MOU shall remain in effect for three (3) years from the date of the last signature on this agreement. At that time, it will be updated, reviewed and reauthorized as necessary. This MOU is subject to annual review by the US Department of Transportation Federal Motor Carrier Safety Administration (the "FMCSA" or "Agency") and must be reauthorized by the Agency if the posture of the understanding is modified or a significant change occurs. One or both parties may terminate this agreement by providing thirty (30) days written notice. In the event of a security incident or suspected incident, either party has the right to immediately terminate the MOU and/or ISA.

2. Purpose:

This MOU sets forth the expectations of the parties and agreement between the signatories, the FMCSA and the State Partner (hereafter "non-FMCSA Organization," "non-FMCSA State Partner," "State Partner," or State). Its intent is to document methodology and required privacy and security safeguards to support the data sharing between the FMCSA SAFER System and PRISM System, which includes the electronic file transfer and web services (hereinafter referred to as the "FMCSA Boundary"), and State Partner support of the State Partner's CVIEW-Plus, Inspect Major Applications, or other inspection software.

Successful implementation of the Performance and Registration Information Systems Management (PRISM) and Safety and Fitness Electronic Records (SAFER) programs requires extensive upload and download of information from State contracted vendors or various State Departments of Transportation, Departments of Public Safety, State Police, and other State agencies responsible for inspecting, monitoring and managing Commercial Vehicle Operations (CVO) within the State. Access to the information may require interface with legacy systems or equipment to acquire the information, conversion to the format used by the FMCSA network services, and require system modifications to meet FMCSA security requirements. The FMCSA has established a methodology, detailed in the FMCSA Motor Carrier Assistance Program Policy (MC-P), that enables a State Partner to qualify for and obtain a non-exclusive interface with the FMCSA Boundary to provide State Partners with access to FMCSA data in order to support the State Partner's PRISM and SAFER programs. This MOU and the corresponding Interconnection Security Agreement (ISA)(Appendix I) establish the methodology for a State Partner to share data and qualify for and obtain an interface with the FMCSA Boundary. The States and FMCSA benefit from successful implementation of the PRISM and SAFER programs.

Specific interconnections between the FMCSA information system and the State Partner's system, if any, will be detailed in the ISA.

FOR OFFICIAL USE ONLY
MOU between FMCSA and State Partner

3. **Responsibilities of the Parties:**

The parties to this MOU and the associated ISA shall:

- Comply with the terms of the MOU and ISA, as applicable.
- Designate a business and technical lead for their respective boundary and provide point of contact (POC) information to facilitate direct contacts between technical leads to support the management and operation of data sharing methods, which may include an established 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.
- Inform their counterpart promptly of any change in POCs.
- Expressly agree upon any changes to the terms of the MOU and execute a signed bilateral modification to effectuate these changes.

FMCSA shall:

- Identify the FMCSA Information System Security Manager (ISSM) to serve as a liaison between both parties.
- As appropriate, communicate with the State Partner regarding FMCSA requirements.

State Partner shall:

- Designate an Information Security (IS) point of contact (POC) the equivalent of the FMCSA ISSO, who shall act on behalf of the State Partner.
- Communicate all IS issues involving the State Partner via the FMCSA ISSM.
- Ensure Privacy and IS controls meet or exceed FMCSA requirements.
- Ensure that all employees, contractors, State contracted vendors, and other authorized users with access to the FMCSA data, Boundary, the State Partner network, and the information sent by and received from either organization are not security risks and that these individuals read, understand and sign the FMCSA Rules of Behavior.
- Provide copies of the signed FMCSA Rules of Behavior (ROB) to FMCSA for all users, upon request.
- Retain copies of all signed FMCSA ROB for three (3) years after the date the MOU and/or ISA terminates or expires.
- Enforce the following Federal Privacy and Security best practices:
 - a. *Least Privilege*-Only authorizing the minimal amount of resources required to perform a function
 - b. *Separation of Duties*-Assigning responsibility to separate individuals for transaction initiation, transaction records, and asset custody in order to prevent and detect errors and irregularities
 - c. *Role-Based Security*-Assigning certain operations ("permissions") to specific user roles
- Not release, publish, or disclose information to unauthorized personnel; Not use the data (i) for a purpose that violates any Federal law; (ii) for mass solicitation mailings, emails, or phone calls of personal or business nature; (iii) for commercial purposes, financial gain, or to support "for profit"

FOR OFFICIAL USE ONLY
MOU between FMCSA and State Partner

non-Government activities; or (iv) to engage in any activities that discredit DOT or FMCSA.

- Protect information in accordance with the laws, regulations and policies cited in the MOU and ISA and with any other applicable laws, regulations, and policies governing adequate safeguards.
- Notify the FMCSA ISSM whenever the State Partner terminates its vendor contract.
- Ensure that State contracted vendors or operations where non-FMCSA personnel may have access to FMCSA information, systems, and network components also comply with the security requirements set forth in FAR Clause 52.239-1, *Privacy or Security Safeguards*.
- Only permit the State or its authorized users to use the State Partner system to access FMCSA systems and data.
- Coordinate with State contracted vendor any costs and expenses associated with restoring access to FMCSA systems and data.

NOTE: Additional responsibilities are identified in the ISA.

4. **Implementing Memorandum of Understanding:**

The MOU and the ISA, which is incorporated by reference, shall serve as the legal basis for authorizing a connection between FMCSA's systems and the State Partner network. The ISA shall document the specifications, protocols, and other requirements for access to the FMCSA Boundary and systems by authorized employees and State provided systems. The ISA may be changed or amended without the MOU being reviewed.

5. **Termination**

- a. Either party may terminate this MOU immediately upon written notice for any reason or no reason at all.
- b. **FMCSA**
FMCSA may block or deny access for the State Partner system network if the State Partner system network does not implement reasonable precautions to prevent the risk of security incidents spreading to the FMCSA network or fails to comply with the MOU or ISA. FMCSA is authorized to audit the security of the State Partner network periodically by requesting that the State Partner provide documentation of compliance with the security requirements in the MOU or ISA. The Non-FMCSA Organization shall provide FMCSA access to its IT resources impacted by the MOU or ISA for the purposes of audits unless restricted by ISO/IEC 27001 or SOC 2 requirements.
- c. **State Partner**
State Partner may terminate this MOU by providing written notice to FMCSA that it has disabled the interconnection and requesting that all user IDs issued to State Partner personnel by FMCSA for the purposes of this MOU be disabled.

FOR OFFICIAL USE ONLY
MOU between FMCSA and State Partner

6. System Changes

a. FMCSA

FMCSA may make system changes that adversely impact State Partner access to FMCSA systems and data. FMCSA will make a good faith effort to provide the State Partner with 30-day notice should FMCSA make any changes to the FMCSA Boundary or systems that adversely impact State Partner access to FMCSA systems and data. In the event that FMCSA makes changes that impact State Partner access to FMCSA systems and data, FMCSA will not bear the burden or provide resources of any kind to enable the State Partner to resume access of FMCSA systems and data.

b. The State Partner is solely responsible for any costs and expenses associated with restoring access to FMCSA systems and data.

7. Costs

The parties shall agree to be responsible for their own systems and the costs of the interconnecting mechanisms 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 owner of the respective system/network organization.

8. Protecting and Sharing Information

a. In connection with this MOU, FMCSA grants State Partner access to MCMIS, which is an FMCSA system of record, and to the SAFER and PRISM programs, which process Privacy Act protected systems of record information that contain personally identifiable information (PII).

b. Access to such systems of record information without prior written consent from the individual whose PII is being disclosed is subject to the applicable routine use exceptions identified in the FMCSA Updated MCMIS SORN, such as the routine use exception for disclosure to state, federal, and local government agencies for the purposes of driver, motor carrier, broker, and freight forwarder investigations, and enforcing commercial operating statutes and regulations and the routine use exception for disclosure to state lead agency grantees and other law enforcement grantees under the Motor Carrier Safety Assistance Program (MCSAP) grant program. <https://www.govinfo.gov/content/pkg/FR-2013-09-25/pdf/2013-23131.pdf> FMCSA.

c. State Partner will protect access to all SAFER and PRISM information as follows:

I. All data, information, records, or other material ("materials") obtained from the FMCSA shall be treated as "For Official Use Only" unless another marking is affixed to the documents or materials. Such materials shall not be released or publicly disclosed in any manner, including in response to litigation demands or public requests for records, without the written consent of the FMCSA.

II. State Partner agrees that only designated and authorized State Partner personnel or State contracted vendors will access data within SAFER and PRISM and that they will only do so using State Partner authorized devices.

FOR OFFICIAL USE ONLY

MOU between FMCSA and State Partner

- III. The State Partner agrees to abide by the terms and conditions of the MCMIS System of Record Notices (SORN) located at <https://www.govinfo.gov/content/pkg/FR-2013-09-25/pdf/2013-23131.pdf>; FMCSA 001 - Motor Carrier Management Information System (MCMIS) - 78 FR 59082, September 25, 2013, the MCMIS PIA (located at: <https://www.transportation.gov/individuals/privacy/motor-carrier-management-information-system-mcmis-march-20-2017>); and the SAFER Privacy Impact Assessment (PIA)(located at: <https://www.transportation.gov/sites/dot.gov/files/docs/resources/individuals/privacy/322921/privacy-fmcsa-safer-pia-011618.pdf>)
This MOU will be updated by FMCSA to reflect any updates to the relevant SORNs and PIAs, as they occur.
- IV. The State Partner will maintain a level of security that is commensurate with the risk and magnitude of harm that could result from the loss, misuse, disclosure, or modification of the information with the highest sensitivity levels contained in the FMCSA system.
- V. State Partner personnel, State contracted vendors and all other authorized users must read and sign the FMCSA Rules of Behavior before being provided access to the FMCSA systems.
- VI. The State Partner shall ensure that effective security safeguards are deployed to protect against the unauthorized disclosure of PII, including sensitive PII, in accordance with Office of Management and Budget (OMB) Circular A-130, Appendix III, *Security of Federal Automated Information Systems*, and any other applicable laws, regulations, and policies governing the privacy and security of Agency data.
- VII. The State Partner will ensure that monitors, printers, hard copy printouts, or any other means of displaying FMCSA data, are in a position so they are not viewable by unauthorized personnel. The State Partner shall ensure that all information received from FMCSA systems is destroyed and reduced to an irreproducible or unidentifiable format once there is no longer a legitimate use for the information or the retention period has ended.
- VIII. The State Partner agrees, if an unauthorized release or disclosure of sensitive or confidential information occurs, to notify FMCSA Information System Security Manager (ISSM) within one hour of discovery or detection at (202) 366-9980 or FMCSASecurity@dot.gov and to work together to determine what actions should be taken to mitigate any resulting damages that have occurred or might occur.
- IX. **The State Partner agrees to assume responsibility for any unauthorized release of confidential or sensitive information that is the result of intentional or negligent conduct of its employees, agents, or contracted vendors. Unauthorized release of confidential or sensitive information may result in the denial of future access to the confidential or sensitive information or to FMCSA systems.**
- X. The State Partner will ensure that all State Partner employees accessing the FMCSA systems complete annual computer security awareness training, which includes training on internet security issues. Annual training must include procedures for handling sensitive Personally Identifiable Information (PII). Upon request, the State Partner will provide documentation to confirm

FOR OFFICIAL USE ONLY

MOU between FMCSA and State Partner

to FMCSA that all State Partner staff have completed annual security training.

- XI.** All provisions in this MOU regarding use, release, and disclosure of information will continue in effect after this MOU is terminated until all covered data or information has been cleared for public release, destroyed, returned to the agency that originally provided such information, or transferred to an agency responsible for appropriate control of the information.
- XII.** The State Partner understands that disputes arising from the MOU or ISA do not give rise to a cause of action against FMCSA. XII. The State Partner agrees that if FMCSA and the State Partner are unable to resolve a dispute, the State's sole remedy is termination of the MOU and/or ISA.
- d. **Optional Vendor Contract Clauses**-FMCSA recommends that the State Partner insert the optional contract clauses provided in this section, or substantively similar clauses, into any associated contracts or agreements with State contracted vendors:
- I. Iteris Inc. agrees that only designated and authorized Iteris Inc. personnel will access data within SAFER and PRISM and that they will only do so using State Partner authorized devices.
- II. Iteris Inc. agrees to abide by the terms and conditions of the MCMIS System of Record Notice (SORN) located at 78 FR 59082, <https://www.govinfo.gov/content/pkg/FR-2013-09-25/pdf/2013-23131.pdf>; the MCMIS PIA (located at: <https://www.transportation.gov/individuals/privacy/motor-carrier-management-information-system-mcmis-march-20-2017>) and the SAFER Privacy Impact Assessment (PIA)(located at: <https://www.transportation.gov/sites/dot.gov/files/docs/resources/individuals/privacy/322921/privacy-fmcsa-safer-pia-011618.pdf>).
- III. FAR Clause 52.239-1
Privacy or Security Safeguards (AUG 1996)
- (a) The Contractor shall not publish or disclose in any manner, without the Contracting Officer's written consent, the details of any safeguards either designed or developed by the Contractor under this contract or otherwise provided by the Government.
- (b) To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of Government data, the Contractor shall afford the Government access to the Contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases.
- (c) If new or unanticipated threats or hazards are discovered by either the Government or the Contractor, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party.
- IV. Iteris Inc. will maintain a level of security that is commensurate with the risk and magnitude of harm that could result from the loss, misuse, disclosure, or modification of the information with the highest

FOR OFFICIAL USE ONLY
MOU between FMCSA and State Partner

sensitivity levels contained in the FMCSA system.

- V. Iteris Inc. agrees to communicate all IS issues involving the State Partner via the FMCSA ISSM.
- VI. Iteris Inc. will ensure Privacy and IS controls meet or exceed FMCSA requirements.
- VII. Iteris Inc. will ensure that all employees, contractors, contracted vendors, and other authorized users with access to the FMCSA data, Boundary, the State Partner network, and/or the information sent by and received from either organization are not security risks and that these individuals read, understand and sign the FMCSA Rules of Behavior before being provided access to the FMCSA systems.
- VIII. Iteris Inc. shall retain copies of all signed FMCSA ROB for three (3) years after the date the MOU and/or ISA terminates or expires.
- IX. Iteris Inc. shall ensure that effective security safeguards are deployed to protect against the unauthorized disclosure of PII, including sensitive PII, in accordance with OMB Circular A-130, Appendix III, *Security of Federal Automated Information Systems*, and any other applicable laws, regulations, and policies governing the privacy and security safeguard of the agency data.
- X. Iteris Inc. agrees that it will not release, publish, or disclose information to unauthorized personnel. The State contracted vendor agrees that it will not use the information (i) for a purpose that violates any Federal law; (ii) for mass solicitation mailings, emails, or phone calls of personal or business nature; (iii) for commercial purposes, financial gain, or to support "for profit" non-Government activities; or (iv) to engage in any activities that discredit DOT or FMCSA.
- XI. Iteris Inc. agrees to ensure that monitors, printers, hard copy printouts, or any other means of displaying FMCSA data, are in a position so they are not viewable by unauthorized personnel. Iteris Inc. shall ensure that all information received from FMCSA systems is destroyed and reduced to an irreproducible or unidentifiable format once its legitimate use or the retention period has ended.
- XII. Iteris Inc. agrees, if an unauthorized release or disclosure of sensitive or confidential Information occurs, to notify New Hampshire State Department of Safety, Division of State Police Information System Security Manager (ISSM) within one hour of discovery or detection at NHSP Communications at 603 223-3825 to work together to determine what actions should be taken to mitigate any resulting damages that have occurred or might occur.
- XIII. Iteris Inc. shall ensure that effective security safeguards are deployed to protect against the unauthorized disclosure of PII, including sensitive PII, in accordance with Appendix III of Office of Management and Budget (OMB) Circular A-130, *Security of Federal*

FOR OFFICIAL USE ONLY
MOU between FMCSA and State Partner

Automated Information Systems and any other applicable laws, regulations, and policies governing the privacy and security safeguard of the agency data. The data processed during the transmission could potentially contain PII, including, but not limited to, the following: Taxpayer ID or SSN, Driver Name, Driver License Number, Driver License State, Driver DOB, CoDriver Name, CoDriver License Number, CoDriver License State, CoDriver DOB.

- XIV. Iteris Inc. shall ensure that any Cloud Hosting Service used by the Non-FMCSA Organization is certified in accordance with ISO/IEC 27001 and attests to trust services principles in accordance with SSAE 16 SOC 2, minimizing security risks of employees, contractors, and others with access to the Cloud Hosting Services connecting to the FMCSA Boundary.
- XV. Iteris Inc. shall enforce the following Federal Privacy and Security best practices:
- a. Least Privilege-Only authorizing the minimal amount of resources required to perform a function
 - b. Separation of Duties-Assigning responsibility to separate individuals for transaction initiation, transaction records, and asset custody in order to prevent and detect errors and irregularities
 - c. Role-Based Security-Assigning certain operations ("permissions") to specific user roles
- XVI. **Iteris Inc. agrees to assume responsibility for any unauthorized release of confidential or sensitive information that is the result of the intentional or negligent conduct of its employees, agents, or contracted vendors. Unauthorized release of confidential or sensitive information may result in the denial of future access to the confidential or sensitive information.**
- XVII. Iteris Inc. will ensure that all its employees, agents, and contracted vendors accessing FMCSA systems complete annual computer security awareness training, which includes training on internet security issues. Annual training must include procedures for handling sensitive Personally Identifiable Information (PII). Upon request, Iteris Inc. will provide documentation to confirm to New Hampshire that all Iteris Inc. staff have completed annual security training.
- XVIII. Iteris Inc. shall require all users (employees, contractors, subcontractors, and other authorized users) to complete the DOT Security Awareness Training (SAT) upon the enactment of this ISA and then annually thereafter.
- XIX. Iteris Inc. shall comply with all applicable Federal IT Security standards, and all applicable laws, regulations, and policies governing adequate IT Security safeguards, including those identified below:
- a. *Federal Information Security Management Act of 2002, 44 U.S.C. § 3553 (2019), amended by the Federal Information Security Modernization Act of 2014, 44 U.S.C. §§ 3551-3558 (2019) (FISMA)*
 - b. *The Privacy Act of 1974, 5 U.S.C. § 552a (2019)*
 - c. *Health Insurance Portability and Accountability Act of*

FOR OFFICIAL USE ONLY

MOU between FMCSA and State Partner

- 1996, Pub. L. No. 104-191 (2019) (HIPAA or HIPPA)
- d. 18 U.S.C. § 641 (2019) (public money, property or records);
 - e. 18 U.S.C. § 1905 (2019) (disclosure of confidential information generally);
 - f. Office of Management and Budget (OMB), Executive Office of the President, Circular A-130, Appendix III, *Security of Federal Automated Information Resources* (2016)
 - g. Office of Management and Budget (OMB), Executive Office of the President, OMB M-06-16, *Protection of Sensitive Agency Information* (2006)
 - h. National Institute of Standards and Technology (NIST), U.S. Department of Commerce, FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems* (2006)
 - i. National Institute of Standards and Technology (NIST), U.S. Department of Commerce, NIST SP 800-37 Rev. 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy* (2018)
 - j. National Institute of Standards and Technology (NIST), U.S. Department of Commerce, NIST SP 800-47, *Security Guide for Interconnecting Information Technology Systems* (2002)
 - k. National Institute of Standards and Technology (NIST), U.S. Department of Commerce, NIST SP 800-53 Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (2015)
 - l. National Institute of Standards and Technology (NIST), U.S. Department of Commerce, NIST SP 800- 61 Rev. 2, *Computer Security Incident and Handling Guide* (2012)
 - m. National Institute of Standards and Technology (NIST), U.S. Department of Commerce, NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)* (2010)
 - n. National Institute of Standards and Technology (NIST), U.S. Department of Commerce, NIST SP 800-160 Vol. 1, *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems* (2018)
 - o. FAR 52.239-1 (2019) (privacy or security safeguards)
 - p. U.S. Department of Transportation, DOT Order 1351.37, *Departmental Cybersecurity Policy* (2011)
 - q. U.S. Department of Transportation, DOT Information Technology and Information Assurance Policy No. 034, *Reporting Cyber Security Incidents and Sensitive Personally Identifiable Information (SPII) Exposure*

FOR OFFICIAL USE ONLY
MOU between FMCSA and State Partner
(2007)

- r. U.S. Department of Transportation, DOT Order 1351.18, *Departmental Privacy Risk Management Policy* (2014)
- XX. Iteris Inc. shall minimize security risks and ensure the confidentiality, integrity, and availability (CIA) of any FMCSA information¹, any New Hampshire information, and any information that is owned by Iteris Inc. that has a system interconnection² with FMCSA or the State Partner. This ensures the adequate security³ of FMCSA information being accessed and provides that all network access satisfies mission requirements.
- XXI. Iteris Inc. shall ensure that security is planned for, documented, and integrated into the system development life cycle from system initiation to disposal. For guidance, see National Institute of Standards and Technology (NIST), U.S. Department of Commerce, NIST SP 800-160 Vol. 1, *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems* (2018).
- XXII. Iteris Inc. shall make all IS program documents accessible to New Hampshire.
- XXIII. *Incident Handling*-Iteris Inc. agrees to manage and report incidents in accordance with:
- i. NIST SP 800-61 Rev.2, *Computer Security Incident Handling Guide* dated August 2012 (<https://csrc.nist.gov/publications/detail/sp/800-61/rev-2>)
 - ii. DOT Information Technology and Information Assurance Policy Number 034, *Reporting Cyber Security Incidents and Sensitive Personally Identifiable Information (SPII) Exposures* dated December 31, 2007
 - iii. FMCSA Incident Response Guidelines Memorandum dated 28 March 2017
 - iv. FMCSA Breach Notification Policy
- XXIV. *Vulnerability Scanning*- Iteris Inc. shall disseminate intrusion detection alerts to respective POC counterparts for all subnets within the scope of the state's ISA with FMCSA;
- XXV. Iteris Inc. shall report security incidents that occur on all subnets within the scope of the state's ISA with FMCSA to Staff Sergeant William Burke, POC for New Hampshire;

¹ **"Information"** is "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." Exec. Order No. 13549, 75 Fed. Reg. 51,609, Sec. 5(d) (Aug. 18, 2010).

² **"System interconnection"** is defined as "the direct connection of two or more IT systems for the purpose of sharing data and other information resources." National Institute of Standards and Technology (NIST), U.S. Department of Commerce, NIST SP 800-47, *Security Guide for Interconnecting Information Technology Systems* (2002), pg. ES-1.

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), Executive Office of the President, Circular A-130, Appendix III, *Security of Federal Automated Information Resources* (2016), pg. 26.

FOR OFFICIAL USE ONLY
MOU between FMCSA and State Partner

- XXVI. Iteris Inc. agrees to monitor and remediate security vulnerabilities for any state information systems on the subnets within the scope of the State's ISA with FMCSA; and
- XXVII. Iteris Inc. agrees to block inbound and outbound access for any state information systems on the subnets within the scope of the state's ISA with FMCSA that are the source of unauthorized access attempts or the subject of any security events until the risk is remediated.
- XXVIII. Iteris Inc. agrees to ensure that the Physical Security of its equipment and facilities within the scope of the state's ISA with FMCSA, at a minimum, will be governed by NIST SP 800-53 Rev 4 physical and environmental controls.
- XXIX. Iteris Inc. will ensure any Cloud Hosting Service used by the vendor is certified in accordance with ISO/IEC 27001 and attests to trust services principles in accordance with SSAE 16 SOC 2 with regard to physical security and security documentation.
- XXX. Iteris Inc. shall periodically review the Cloud Hosting Service ISO/IEC 27001 certificate and SOC 2 type 2 documentation to confirm compliance.
- XXXI. Iteris Inc. understands that disputes arising from this contract to serve as the state's inspection software vendor do not give rise to a cause of action against FMCSA. Iteris Inc. agrees that its sole remedy for disputes related to this contract or the services arising under this contract is against the state, not FMCSA.
- XXXII. Iteris Inc. shall ensure that this interconnection is completely isolated from the Internet except through the persistent VPN tunnel.
- XXXIII. Iteris Inc. shall ensure that this interconnection is completely isolated from all other customer business processes.
- XXXIV. Iteris Inc. shall configuring all network perimeter firewalls with a policy at least as stringent as DOT IT Security Baseline Configurations/CIS Benchmarks.

9. **Dispute Resolution:**
Disagreements between the Parties arising under or relating to this MOU will be resolved by consultation between the Parties. Should disagreement arise as to the interpretation of the provisions of this MOU that cannot be resolved between the Parties, the area(s) of disagreement will be reduced to writing by each Party and presented to the authorized officials at both Parties for resolution. If settlement cannot be reached at this level, and the Parties have failed to resolve the dispute through good faith discussions it may be grounds for termination under Section 5 above.

10. **Amendments to the MOU:**
If any personnel changes occur involving the POCs listed in this MOU, the terms of

FOR OFFICIAL USE ONLY
MOU between FMCSA and State Partner

this MOU shall remain in full force and effect unless formally modified by both parties. Any modifications that change the security posture to this MOU shall be in writing and be agreed upon and approved in writing by both parties.

11. Information Security Agreement ("ISA")

Both Parties agree to execute and incorporate into this MOU the attached ISA (Appendix 1).

12. Severability

The invalidity of a term, condition, or clause of this MOU shall not affect the remaining terms and conditions of this MOU.

13. 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. In the event that FMCSA makes changes that impact the State Partner's access to FMCSA systems and data, FMCSA will not bear the burden or provide resources of any kind to enable the State Partner to resume access of FMCSA systems and data.

14. Confidentiality

Subject to applicable statutes and regulations, including the Freedom of Information Act, the parties agree that any proprietary information contained in the MOU or ISA shall not be disclosed to any third party outside of the Government without the prior written consent of the other party.

Subject to applicable statutes and regulations, including the Freedom of Information Act, the parties agree that the terms and conditions of this ISA shall not be disclosed to anyone other than the parties to this agreement without the prior written consent of the FMCSA. Confidential or proprietary information contained in this MOU shall not be disclosed without the prior written consent of all parties.

15. Records

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

16. Warranty

FMCSA does not warrant the State Partner's interconnection to the FMCSA network under the ISA will meet State Partner requirements or expectations. The State Partner bears the entire risk regarding the quality and performance of its interconnection with the FMCSA, and the State Partner's exclusive remedy is to terminate this ISA in accordance with the terms and conditions herein.

FMCSA EXPRESSLY DISCLAIMS ALL WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED

FOR OFFICIAL USE ONLY
MOU between FMCSA and State Partner

WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE WITH REGARD TO THE NON-FMCSA ORGANIZATION'S CURRENT AND/OR FUTURE INTERCONNECTION TO THE FMCSA.

17. **Points of Contact:**

State Partner Points of Contact

Staff Sergeant William Burke
Assistant Troop Commander Troop G
New Hampshire State Police
33 Hazen Drive
Concord, NH 03305
william.burke@dos.nh.gov
Office: 603 223-8965

FMCSA Points of Contact

Bobby Woodard
Director, Cybersecurity and Privacy
Federal Motor Carrier Safety Administration
1200 New Jersey Ave., SE W68-313
Washington, DC 20590
Ph: (202) 366-2860
bobby.woodard@dot.gov

Nicole Moore
Information System Security Manager (ISSM)
Federal Motor Carrier Safety Administration
1200 New Jersey Avenue SE, W66-417
Washington, DC 20590
Ph: (202) 366-9980
nicole.moore@dot.gov

Pam Gosier-Cox
Privacy Officer
Federal Motor Carrier Safety Administration
1200 New Jersey Avenue SE, W66-417
Washington, DC 20590
Ph: (202) 366-3655
pam.gosier-cox@dot.gov

18. **Definition of Terms and Abbreviations**

- a. VPN - Virtual Private Network
- b. IPSEC - Internet Protocol Security (Internet RFC 2401, Security Architecture for the Internet Protocol).
- c. ISAKMP - Internet Security Association and Key Management Protocol (RFC 2408).
- d. ESP - IP Encapsulating Security Payload (RFC 2406).
- e. PFS - Perfect Forward Secrecy (found within RFC2412, The OAKLEY Key Determination Protocol).
- f. AES -Advanced Encryption Standard (see Federal Information

FOR OFFICIAL USE ONLY
MOU between FMCSA and State Partner

Processing Standards Publication 197).

- g. PSK - Pre-shared Key.
- h. DH - Diffie-Hellman (RFC 2631, Diffie-Hellman Key Agreement Method).
- i. TCP - Transmission Control Protocol (RFC 793).
- j. UDP - User Datagram Protocol (RFC 768).
- k. IP - Internet Protocol.
- l. Tunnel Proxy ACL: Also called 'interesting traffic' or 'crypto access- list'.
- m. DOT: U.S. Department of Transportation
- n. FMCSA: Federal Motor Carrier Safety Administration
- o. CVIEW-Plus: State Partner' implementation of a Commercial Vehicle Information Exchange Window
- p. Inspect: State Partner' implementation of a tool used by State motor vehicle inspectors and other users to collect inspection data and exchange it with the FMCSA network.
- q. Cloud Hosting Service - For the purposes of this MOU, a Cloud Hosting Service is a third-party service such as Microsoft's Azure or Amazon's AWS, that provides network computing resources such as servers, storage, operating systems, physical security, backup, service continuity, etc. at one or more central facilities that are used by party to host applications and data over secure internet communications.
- r. State contracted vendor - A vendor with a current contract awarded by the State Partner identified below in Section 15 to provide inspection software, tools, and other related services.

19. Administration

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

20. State Partner Signatures and Certifications

I understand that by signing below I certify on behalf of New Hampshire, that the State has entered into the contract identified below to provide the state with inspection software:

Contract Name: Commercial Motor Vehicle Enforcement Inspection Software

Contract Number: GC#95

Period of Performance: Start date: May 3, 2017 End date: June 30, 2021

***Please attach a copy of the contract.**

I understand that by signing below, I make the following certifications:

- I certify that I have read and understood the terms of the MOU and of the ISA provided in Appendix 1, which is incorporated by reference.
- I certify that any access granted under this MOU and the attached ISA will be used in strict accordance with the terms and conditions identified in the MOU and ISA.
- I certify that the information I have provided is accurate, to the best of my knowledge and belief.
- **I understand that any false certifications or statements may result in prosecution under 18 U.S.C. § 1001 (false statements to the government).**

FOR OFFICIAL USE ONLY
MOU between FMCSA and State Partner

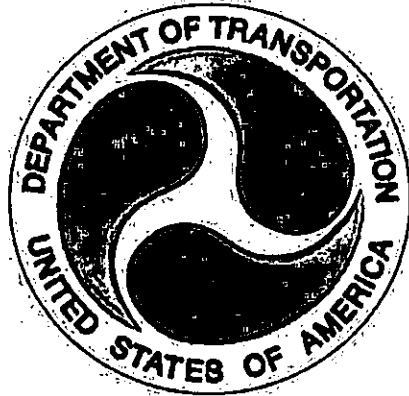
State	Name	Title/Position	Signature	Date
NH	Andrew J. Player	Lieutenant, Troop G	<i>[Handwritten Signature]</i>	6/10/20
NH	Matthew S. Shapiro	Executive Major, Director's Office	<i>[Handwritten Signature]</i>	06-10-20
NH	Steven R. Lavoie	Director of Administration	<i>[Handwritten Signature]</i>	6/10/20

21. FMCSA Signatures

Title	Name	Signature	Date
Cybersecurity and Privacy Director	Bobby Woodard	Bobby L.	Digitally signed by Bobby L. Woodard
Information Security System Manager (ISSM)	Bobby Woodard	Woodard	Date: 2020.07.27 13:07:46 -04'00'

For Official Use Only

**U.S. DEPARTMENT OF TRANSPORTATION
FEDERAL MOTOR CARRIER SAFETY ADMINISTRATION
Office of the Chief Information Officer**



**INTERCONNECTION SECURITY
AGREEMENT (ISA)**

Between

**The U.S. Department of Transportation (US DOT) Federal Motor
Carrier Safety Administration (FMCSA)**

<SAFER, SAFETYNET, ITD, & PRISM Systems>

And

New Hampshire State Police

Non-FMCSA System hosted and operated by Iteris, Inc.

Date 01/2020

Prepared by: FMCSA Office of the Chief Information Officer

Disclosure and Handling Notice

THE ATTACHED MATERIALS CONTAIN DEPARTMENT OF TRANSPORTATION INFORMATION THAT IS "FOR OFFICIAL USE ONLY", OR OTHER TYPES OF SENSITIVE BUT UNCLASSIFIED INFORMATION REQUIRING PROTECTION AGAINST UNAUTHORIZED DISCLOSURE. THE ATTACHED MATERIALS MUST BE HANDLED AND SAFEGUARDED IN ACCORDANCE WITH DOT MANAGEMENT DIRECTIVES GOVERNING PROTECTION AND DISSEMINATION OF SUCH INFORMATION.

AT A MINIMUM, THE ATTACHED MATERIALS WILL BE DISSEMINATED ONLY ON A "NEED-TO-KNOW" BASIS AND WHEN UNATTENDED, MUST BE STORED IN A LOCKED CONTAINER OR AREA OFFERING SUFFICIENT PROTECTION AGAINST THEFT, COMPROMISE, INADVERTENT ACCESS, AND UNAUTHORIZED DISCLOSURE.

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DOT policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of the both FMCSA and Non-FMCSA Organization Disclosure Offices.

ISA Between FMCSA and New Hampshire State Police

Document Revision History

The Interconnection Security Agreement (ISA) between FMCSA and the New Hampshire Division of State Police must be reviewed at least annually. All reviews of this ISA must be documented below.

Date	Version	Description
12/20/19	1.0	Initial Request

Table of Contents

Introduction.....1
 Purpose 1
 DOT FMCSA Security Network Connectivity Policy 2
 Authority 2
 References 3
 Scope 3

Section 1: Interconnection Statement of Requirements3

Section 2: FMCSA Systems Security Requirements.....3
 2.1 ISA Requirements Within and Across Organizational Boundaries 3
 2.2 Physical Security and Environmental Controls 4
 2.3 Incident / Breach Reporting 4
 2.4 Security Audit Trail Responsibility..... 4
 2.5 Training and Awareness 4
 2.6 Security Documentation 5
 2.7 Change Control 5
 2.8 Specific Equipment/Service Restrictions 5

Section 3: Systems Security Considerations6
 3.1 General Information/Data Description..... 6
 3.2 Data Sensitivity 6
 3.3 Non FMCSA Formal Security Policy or Official Mandate..... 6
 3.4 Services Offered 6
 3.5 Period of Operation 7
 3.6 User Community 7
 3.7 Ports, Protocols and Services 7
 3.8 Information Exchange Security..... 7
 3.9 System Monitoring..... 8
 3.10 Remote Access 8

Section 4: Topological Diagram.....9

Section 5: ISA Signatory Authority.....10

Appendix A15
 Point of Contact (POC) Tables..... 15

Appendix B17
 Trusted Behavior 17

Appendix C18
 Rules of Behavior..... 18

ISA Between FMCSA and New Hampshire State Police

Effective Date

This ISA is valid for one (1) year from the date of the last signature below. At that time, it will be updated and reauthorized, as necessary.

Introduction

An Interconnection Security Agreement (ISA) describes a connection in sufficient detail to serve as a sound basis for approving a system-to-system connection. The protection for the connected systems is meant to equal or exceed their individual protection. *The signing of an ISA by the Authorizing Officials of the interconnecting systems is a prerequisite to operating the associated connection. As required by National Institute of Standards and Technology (NIST) Guide for Applying the Risk Management Framework to Federal Information Systems Special Publication (SP) 800-37, the role of authorizing official has inherent U.S. Government authority and is assigned to government personnel only.*

Purpose

The purpose of this Interconnection Security Agreement (ISA) is to establish procedures for cooperation and coordination between the Federal Motor Carrier Safety Administration (FMCSA) and Non-FMCSA / External State or Federal agencies (hereafter "Non-FMCSA Organization"), regarding the operations and security of the system to system connections. This ISA is intended to minimize security risks and ensure the confidentiality, integrity, and availability (CIA) of FMCSA information. This ISA ensures the adequate security of FMCSA information being accessed and provides that all network access satisfies the mission requirements of both FMCSA and the Non-FMCSA Organization (hereafter "both parties").

Federal policy requires agencies to develop ISAs for federal information systems that share or exchange information with external information systems and networks. This ISA is based on the NIST Security Guide for Interconnecting Information Technology Systems Special Publication (SP) 800-47 (<http://csrc.nist.gov/publications/nistpubs/800-47/sp800-47.pdf>) and shall comply with the security required by Federal Acquisition Regulation (FAR) clause 52.239-1, Privacy or Security Safeguards. 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 networks and shared data. FMCSA IT managers and IS personnel shall comply with the NIST guidelines in managing the process of interconnecting information systems and networks.

This ISA documents the responsibilities for both parties, outlines security safeguards, and provides the technical and operational security requirements. This ISA also specifies business and legal requirements for the information systems exchange. This ISA authorizes mutual permission for the information systems exchange and establishes a commitment to protect data that is exchanged between both parties. Through this ISA, both parties shall minimize the susceptibility of their systems and networks to IS risks and aid in mitigation and recovery from IS incidents.

All technical details of the interconnection between both parties are in Section 3 through 6 of this ISA.

DOT FMCSA Security Network Connectivity Policy

DOT Order 1351.37, *Departmental Cybersecurity Policy* (2011), and the Cybersecurity Compendium establish DOT security policy for interconnections.

Authority

Interconnectivity between IT systems is governed by Office of Management and Budget (OMB) Circular A-130, the signed MOU/A between the two organizations that are establishing the interconnection, and the authorities and standards identified below:

- *The Federal Information Security Management Act of 2002*, 44 U.S.C. § 3553 (2019), amended by the *Federal Information Security Modernization Act of 2014*, 44 U.S.C. §§ 3551-3558 (2019) (*FISMA*)
- *The Privacy Act of 1974*, 5 U.S.C. § 552a (2019)
- Published MCMIS System of Records Notice (SORN)
- Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191 (2019) (HIPAA or HIPPA)
- 18 U.S.C. § 641 (2019) (public money, property or records)
- 18 U.S.C. § 1905 (2019) (disclosure of confidential information generally)
- Office of Management and Budget (OMB), Executive Office of the President, Circular A-130, Appendix III, *Security of Federal Automated Information Resources* (2016)
- Office of Management and Budget (OMB), Executive Office of the President, OMB M-06-16, *Protection of Sensitive Agency Information* (2006)
- National Institute of Standards and Technology (NIST), U.S. Department of Commerce, NIST SP 800-37 Rev. 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy* (2018)
- National Institute of Standards and Technology (NIST), U.S. Department of Commerce, NIST SP 800-160 Vol. 1, *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems* (2018)
- FAR 52.239-1 (2019) (privacy or security safeguards)
- U.S. Department of Transportation, DOT Order 1351.37, *Departmental Cybersecurity Policy* (2011)
- U.S. Department of Transportation, DOT Order 1351.37, Appendix D, *OST Cybersecurity Policy* (2017)
- U.S. Department of Transportation, DOT Information Technology and Information Assurance Policy No. 034, *Reporting Cyber Security Incidents and Sensitive Personally Identifiable Information (SPII) Exposure* (2007)
- U.S. Department of Transportation, DOT Order 1351.18, *Departmental Privacy Risk Management Policy* (2014)

References

- FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems* (2006)
- National Institute of Standards and Technology (NIST), U.S. Department of Commerce, NIST SP 800-47, *Security Guide for Interconnecting Information Technology Systems* (2002)
- NIST, U.S. Department of Commerce, NIST SP 800-53 Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (2013)
- National Institute of Standards and Technology (NIST), U.S. Department of Commerce, NIST SP 800- 61 Rev. 2, *Computer Security Incident and Handling Guide* (2012)
- NIST, U.S. Department of Commerce, NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)* (2010)
- NIST, U.S. Department of Commerce, NIST ITL Bulletin, *Secure Interconnections for Information Technology Systems*, February 2003

Scope

This ISA addresses the interconnection of the **DOT FMCSA, SAFER, SAFETYNET, ITD, & PRISM Systems** and the New Hampshire State Police's system, which is hosted and administered by Iteris, Inc. Additionally, the ISA covers application and/or control data traversing the networks.

Section 1: Interconnection Statement of Requirements

System interconnections may be characterized as either direct or networked. Direct connections are single purpose point-to-point connections that support only the two connected systems. Directly connected systems do not rely on another network for their connectivity or security and are physically and electronically isolated from other networks and systems. Networked systems connect via an intervening network that exists as a general support system, not a single-purpose connection. Systems that are connected via an encrypted tunnel, whether via network or any other network, are considered networked systems.

For networked U.S. Government systems, the ISA must include the owner and Authorizing Official (AO) of the network as well as the owners of the applicable systems.

Section 2: FMCSA Systems Security Requirements

2.1 ISA Requirements Within and Across Organizational Boundaries

IT equipment within the organizational boundary of all parties within this ISA is owned, operated and maintained by contracted services or government employees. IT equipment and Systems are designed, developed and authorized in accordance with DOT FMCSA IT security policy and standards that are in accordance with FISMA and applicable NIST guidelines.

ISA Between FMCSA and New Hampshire State Police

Participants of this ISA will protect the data in order to maintain confidentiality, integrity, and availability of the data and information systems. The data and information systems will be protected in accordance with applicable NIST SP 800-53 security controls based on the FIPS 199 Security Categorization of each system to ensure that the connection is protected to the requirements of the higher categorized system.

2.2 Physical Security and Environmental Controls

Physical Security, at a minimum, will be governed by each organizations Physical Security policy and associated controls which must meet applicable NIST SP 800-53 security controls.

2.3 Incident / Breach Reporting

The organization discovering a security incident will report it in accordance with the organization's incident reporting procedures and ensure that the other connecting organization is notified. Notification will be made using the ISA Incident Call Roster Point of Contact Table in Appendix B.

The non-FMCSA Organization will notify DOT FMCSA System(s) personnel of any security incident that may have an operational or security impact on the interconnected Non FMCSA System(s). Likewise, the Non FMCSA personnel shall be notified of any security incident that may have an operational or security impact on Non FMCSA System(s) interconnected to the DOT FMCSA System.

2.4 Security Audit Trail Responsibility

Both parties are responsible for auditing system security events and user activities involving the interconnection. Activities that will be recorded include:

- Event type
- Date and time of event
- User identification
- Workstation/server identification
- Success or failure of access attempts
- Security actions taken by system administrators or ISSOs.

Audit logs will be retained in accordance with federal and local guidelines.

2.5 Training and Awareness

Both parties will ensure that all individuals using the systems have attended initial basic and annual refresher Computer Security Awareness and Training. Additionally, both parties will ensure that persons with significant security responsibilities for the systems receive annual role based training covering their specific areas of responsibility. This training should ensure that staff members know how to report suspicious or prohibited activities.

2.6 Security Documentation

For each system, Security Authorization documentation (e.g., System Security Plan, Contingency Plan, Security Assessment Report, Plan of Action & Milestones, Interconnection Security Agreements, etc.) and all other security related documents will be made available to each party for review and acceptance. Security Authorization documentation will be updated to reflect the establishment of this interconnection and whenever a significant system change occurs or at least annually. The parties are responsible for ensuring that this ISA remains up to date. At a minimum, the following information, will be reviewed for accuracy:

- Names of interconnected systems
- Organizations owning the other systems
- Type of interconnection
- Name and title of authorizing management officials (e.g. Chief Information Officer or Designated Authorizing Authority)
- Interaction among the systems
- Hardware inventory
- Software inventory
- Rules of Behavior

All future changes relating to the security architecture of either system will be updated within the corresponding security documents. The assigned Information System Security Officer(s) for each system will provide the security documentation to the both FMCSA and the New Hampshire State Police upon request.

2.7 Change Control

Significant changes to the system architecture, documentation, or configurations will be reviewed, approved and documented in accordance with each organization's configuration/change control process. Each organization will notify the other if a system change significantly changes the approved security posture of the system or introduces new significant residual risk to either system. Whenever significant changes are made at one or both organizations, e.g., through additional staff, service, etc., this should be recorded as an addendum to the original ISA.

2.8 Specific Equipment/Service Restrictions

The use of specific prohibited or restricted services, protocols, and ports listed in the DOT Cybersecurity Compendium require an approved waiver or exception agreement between the system AOs. Any additional interconnections to either system shall be documented in the appropriate security documentation and each party shall be notified of the new interconnections.

Section 3: Systems Security Considerations

Use this section to document the security features that are in place to protect the confidentiality, integrity, and availability of the data and the systems being interconnected. The technical representative from each organization should discuss the contents on this section to come to a mutual agreement as to which items will be included. Both organizations should answer each item, even if only one party is affected by the item in question.

System Security Considerations

The requirements for interconnection between the two systems is for the express purpose of exchanging data between the FMCSA SAFER System, FMCSA SAFETYNET System, & FMCSA ITD/PRISM System all owned and operated by FMCSA, and the New Hampshire State Police's system hosted and administered by the state's contracted vendor, Iteris Inc. The New Hampshire State Police's system operated by Iteris requires a connection to send and receive SAFER data to support commercial vehicle credentialing and safety systems used by the New Hampshire State Police.

3.1 General Information/Data Description

The purpose of the interconnection between the FMCSA SAFER, FMCSA SAFETYNET, & FMCSA ITD/PRISM Systems and the New Hampshire State Police's system hosted and operated by the state's contracted vendor, Iteris Inc. is to interconnect FMCSA components and provide a single trusted infrastructure. Transmitted data includes FMCSA data and New Hampshire State Police's specific data as required in each configuration or customer deployment.

3.2 Data Sensitivity

The highest level of data that traverses the FMCSA SAFER System, FMCSA SAFETYNET System, & FMCSA ITD/PRISM System is Sensitive but Unclassified (SBU). This may include, but is not limited to, Sensitive Personally Identifiable Information, For Official Use Only, financial, and/or Law Enforcement Sensitive data.

The highest level of data that traverses the New Hampshire State Police's system is Sensitive but Unclassified (SBU). This may include, but is not limited to, Sensitive Personally Identifiable Information, For Official Use Only, financial, and/or Law Enforcement Sensitive data. No criminal information, medical, or related data is transmitted through the Iteris hosted New Hampshire State Police system or Iteris networks.

3.3 Non FMCSA Formal Security Policy or Official Mandate

Not applicable

3.4 Services Offered

The interconnection between the FMCSA SAFER System and Iteris System are supported by File Transfer Protocol (FTP).

The interconnection between the FMCSA SAFETYNET System and Iteris System are supported by web services.

The interconnection between the FMCSA ITD/PRISM System and Iteris System are supported by File Transfer Protocol (FTP) & web services.

ISA Between FMCSA and New Hampshire State Police

Note: The FTP is scheduled to be upgraded to Secure File Transfer Protocol (SFTP) in FY2020. All technology changes will be addressed on the annual review of this ISA.

3.5 Period of Operation

Both systems are operational 24 hours a day, 7 days a week.

3.6 User Community

The user community is comprised of FMCSA, Iteris staff, and state authorized users. All users of both systems will have appropriately adjudicated suitability background investigations.

3.7 Ports, Protocols and Services

The following ports, protocols, and services are allowed between FMCSA and Non-FMCSA Organization Security Domains by default:

List of Required Ports

TCP: Port 20 and 21, 443, and 49152-65535

List of Required Protocols, and services

FTP over TCP Port 20 and 21, configure firewall as FTP passive mode

Port/Protocol/Service	DOT FMCSA	Iteris
FTP	[REDACTED]	[REDACTED]
PRISM Webservices	[REDACTED]	[REDACTED]
SAFER Webservices	[REDACTED]	[REDACTED]

3.8 Information Exchange Security

Information exchange will be encrypted using FIPS 140-2 AES-256 as the minimum standard encryption algorithm. Via web services Iteris forces SSL/TLS connections for HTTP traffic using TLS 1.2. Dynamic Multipoint Virtual Private Network (DMVPN) provides a mechanism for the dynamic negotiation of IPsec encrypted tunnels between any two endpoints, alleviating the need for complex router configurations.

Both organizations will ensure that virus and spyware detection and eradication capabilities are used where appropriate (e.g., workstations, laptops, servers, etc.) and that adequate system access controls are in place and maintained on all components connected to the systems.

3.9 System Monitoring

Iteris systems performance and operations are monitored and managed using the following products and tools:

Azure Monitor

Iteris systems is deploying and/or using the following products and capabilities to monitor security vulnerabilities and compliance:

Azure Monitor

3.10 Remote Access

Iteris currently uses a VPN provided by FMCSA for data transfer to FMCSA systems.

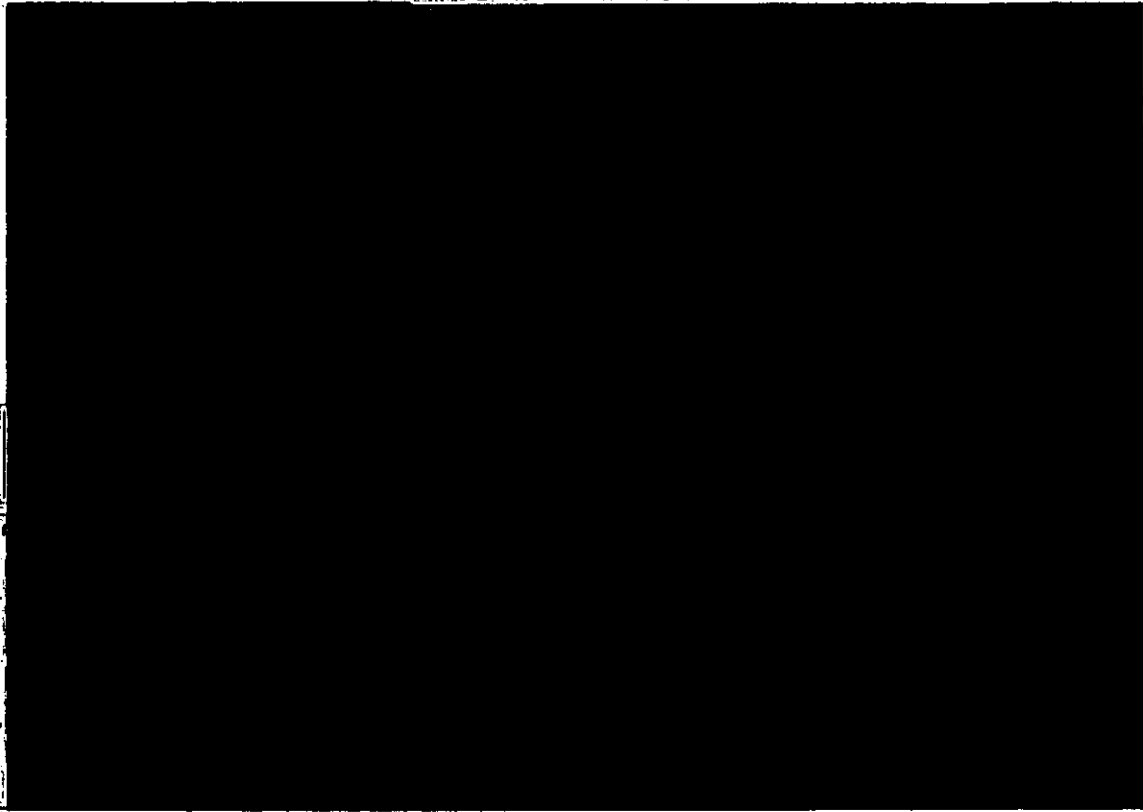
Iteris systems uses the Azure virtual VPN for remote access to Iteris internal systems.

Section 4: Topological Diagram

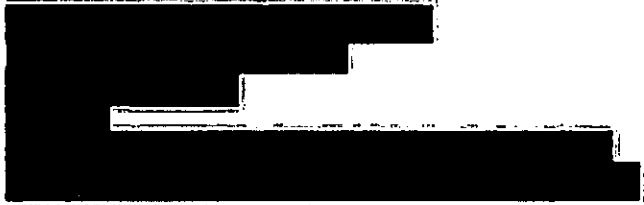
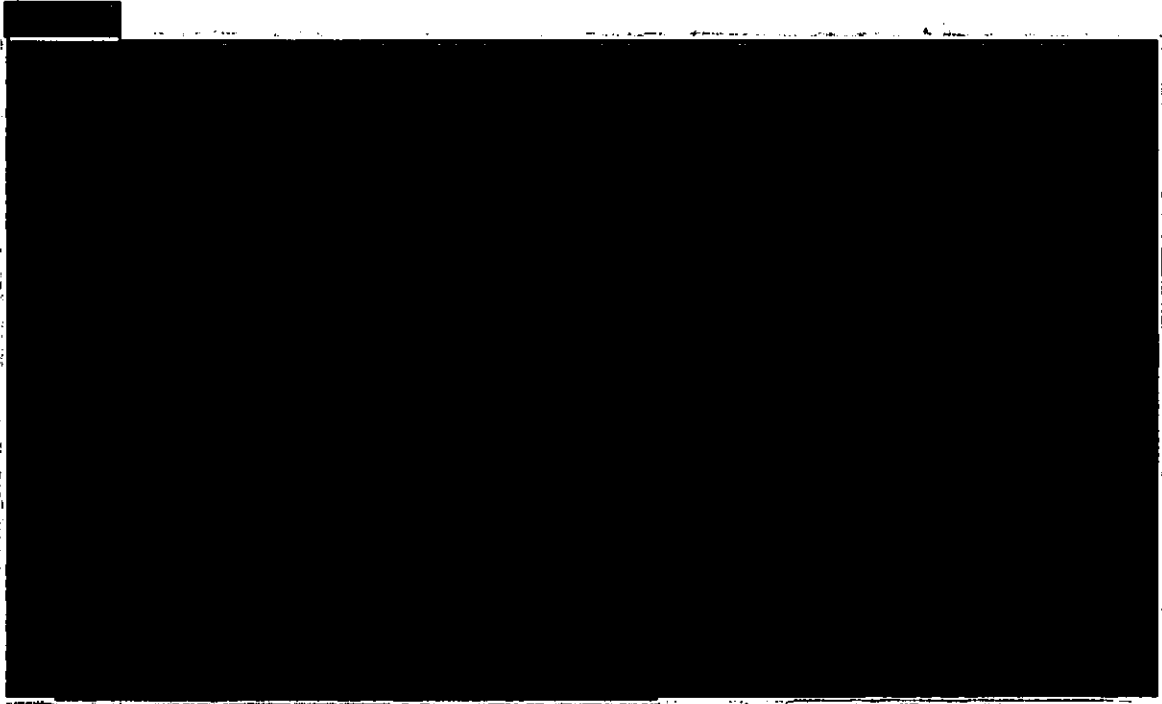
The Iteris network intakes several different data sources from state systems (T0019-T0024 transactions specifically for SAFER data) and combines them into a central database that is used to query information and display to Iteris system users. Iteris servers also push data to the SAFER systems to meet the states' requirement of sharing data with FMCSA. Additionally, Iteris accesses the VPN connection to request data from FMCSA systems including T0025-T0035 data sets and PRISM web services. This data is also compiled into the central database for access. The VPN connection is a persistent connection with time-outs to improve performance and error handling. Figure A-1 shows the Iteris/CMCSA Connection Flow, Figure A-2 shows Data Communications Figure A-3 shows the FMCSA Boundary.

Figure A-1

Figure A-2



ISA Between FMCSA and New Hampshire State Police





ISA Between FMCSA and New Hampshire State Police

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Section 5: ISA Signatory Authority

This ISA is valid for one (1) year after the last date on either signature below. At that time it will be updated, reviewed, and reauthorized. Either party may terminate this agreement upon 30 days advanced notice in writing or in the event of a security incident that necessitates an immediate response.

ISA Between FMCSA and New Hampshire State Police

New Hampshire State Police

Authorizing Official or (equivalent)

XO MATTHEW SHAPIRO

Printed Name:

Matthew S. Shapiro 06-10-20

Signature/Date

Business Owner (equivalent)

LI Andrew Payer

Printed Name:

[Signature] 06/01/2020

Signature/Date

Security Official


Ronald W Reed

Printed Name:

Ronald W Reed, 06/05/2020

Signature/Date

ISA Between FMCSA and Massachusetts, RMV

FMCSA	
AO or AODR	
Printed Name: Charles Taumoepeau	
Signature/Date	CHARLES ONEHUNGA TAUMOEPEAU Digitally signed by CHARLES ONEHUNGA TAUMOEPEAU Date: 2020.02.05 09:35:05 -05'00'
Business Owner-PRISM	
Printed Name: Camille White	
Signature/Date	camille white Digitally signed by camille white Date: 2020.02.04 08:44:55 -05'00'
Business Owner - SAFER	
Printed Name: Thomas Kelly	
Signature/Date	THOMAS EDWARD KELLY Digitally signed by THOMAS EDWARD KELLY Date: 2020.02.04 07:51:23 -05'00'
Business Owner - SAFETYNET	
Printed Name: Jamie Vasser	
Signature/Date	 Digitally signed by Department of Transportation Date: 2020.02.06 09:07:05 -05'00'
ISSM	
Printed Name: Bobby L. Woodard	
Signature/Date	Bobby L. Woodard Digitally signed by Bobby L. Woodard Date: 2020.07.27 13:12:17 -04'00'

ISA Between FMCSA and New Hampshire State Police

Appendix A

Point of Contact (POC) Tables

For all issues associated with this agreement, the established points of contact are as follows:

ISA Point of Contact (POC)

FMCSA	New Hampshire State Police
AO: Charles Taumoepeau	Authorizing Official:
System Owners: Thomas Kelly, Titi Ariyo, Jamie Vasser	System Owner:
System ISSO(s) Jonathan Florance	System ISSO(s):
ISSM: Bobby Woodard	ISSM:
Privacy Officer: Pam Gosier-Cox	Privacy Officer:
Program Managers Tom Kelley, Titi Ariyo, Jamie Vasser	Program Manager

Incident Call Roster

FMCSA			
Name	Role	Email	Phone
Bobby L Woodard	Dir, Cyber & Privacy	bobby.woodard@dot.gov	202-366-2860
Pam Gosier-Cox	Chief Privacy Officer	pam.gosier.cox@dot.gov	202-366-3655
Wan Kuang	Incident Manager	wan.kuang@dot.gov	617-312-3978

Iteris			
Name	Role	Email	Phone
Whitney Raya	Program Manager	wln@iteris.com	208-419-0590
Aaron Jenkins	Development Manager	asj@iteris.com	208-419-0324
Brad Steiner	Systems Architect	brs@iteris.com	208-528-8538
Kohlae Angell	Product Manager	kxa@iteris.com	208-419-0370

ISA Between FMCSA and New Hampshire State Police

New Hampshire State Police			
Name	Role	Email	Phone

Appendix B

Trusted Behavior

The *DOT FMCSA SAFER, SAFETYNET, & ITD/PRISM System* users and the New Hampshire State Police, users, to include system administrators, are expected to protect data in accordance with the policies, standards, and regulations specified for each system. This includes *DOT FMCSA* and the New Hampshire State Police's policy and the documented rules of behavior for each system. The following documents specify specific rules of behavior for each system:

Appendix C

Rules of Behavior

General Rules of Behavior for Users of FMCSA Systems and IT Resources that Access, Store, Receive, or Transmit FMCSA Information. The FMCSA ROB must be printed, read, signed, and submitted by all DOT federal employees, contractors, and other personnel who are provided access to DOT/FMCSA information systems and FMCSA data. The FMCSA ROB is to be submitted to the appropriate FMCSA system owner and FMCSA Cyber Security & Privacy Office.



U. S. Department of Transportation
Federal Motor Carrier Safety Administration

Rules of Behavior

Federal Motor Carrier Safety Administration (FMCSA)

I understand that I am personally responsible for use and misuse of system accounts and passwords. The government reserves the right to monitor the activity of any machine connected to its infrastructure and log details of all inquiries and transactions. FMCSA IT systems are the property of the Federal government. FMCSA owns the data stored on FMCSA databases, including all data recorded for monitoring, email messages and information, even those deemed personal. I understand that by accessing a U.S. government information system and data that I must comply with the following requirements:

1. The FMCSA IT systems are intended for official government use only. FMCSA IT systems may not be used for personal or commercial purposes or for any other unauthorized use.
2. Sensitive information may not be transmitted at a level higher than the level for which the system is approved.
3. Information obtained via the FMCSA IT systems may not be divulged outside of government channels without the express permission of the data owner.
4. Any activity that would discredit FMCSA, including seeking, transmitting, collecting, or storing defamatory, discriminatory, sexually explicit, obscene, harassing, or intimidating messages or material is not permitted.
5. Any activity that violates Federal laws for information privacy (e.g., hacking, spamming, etc.) is not permitted.
6. FMCSA IT system-to-system accounts are provided solely for the use of the agency for which they were created. System-to-System passwords or any other authentication mechanism should never be shared or stored any place accessible to non-authorized persons.
7. Passwords must be reasonable (i.e. not "password" or "administrator") and changed every 90 days. Passwords used by administrators and end-users to access those systems that in turn access FMCSA IT systems, must comply with the current U.S. DOT policy for passwords.
8. Virus prevention tools must be in place on any and all machines from which FMCSA IT systems are accessed. Each user must be able to determine that such a tool is active. The user must also follow their organization guidelines for keeping the software and virus definition tables current.
9. Any password compromise or unauthorized usage of the user accounts must be reported immediately to the Information Systems Security Manager (ISSM) at FMCSASecurity@dot.gov. In addition, the incident should be reported to the local Non FMCSA IT security personnel or person in charge of the IT systems operations.

10. Users must only use Sensitive Personally Identifiable Information (SPII) on encrypted laptops, mobile devices, and storage media. SPII data is any piece of information that can potentially be used to uniquely identify, contact, or locate a single person (home address, date of birth, social security number, driver's license number, etc.).

11. Users must protect all FMCSA confidential/sensitive and privacy information from disclosure.

12. Hard copies of confidential/sensitive and privacy information must be shredded and destroyed.

I understand that Federal law provides for punishment under Title 18, U.S. Code, including a fine and up to 10 years in jail for the first offense for anyone who:

1. Knowingly accesses an information system without authorization, or exceeds authorized access, and obtains information that requires protection against unauthorized disclosure.

2. Intentionally, without authorization, accesses a government information system and impacts the government's operation, including availability of that system.

3. Intentionally accesses a government information system without authorization and alters, damages or destroys information therein.

4. Prevents authorized use of the system or accesses a government information system without authorization, or exceeds authorized access, and obtains anything of value.

My signature below indicates that I have read, understand, and will comply with these requirements as a condition of maintaining active accounts with access to FMCSA IT systems. I also understand that failure to comply with these requirements may result in disciplinary action.

Name of User (Printed)	Talan Kirk
User Signature // Date	 7/24/2020
User email address	tkirk@iteris.com