

BLM Well Information System (WIS) ELECTRONIC COMMERCE AGREEMENT (ECA)

This Electronic Commerce Agreement (ECA) is made as of (enter current date here), by and between the Department of the Interior, Bureau of Land Management (BLM), located at 1849 C St NW, Washington, DC 20240 and (enter your company name here) with offices located at

_____. (Physical Street or Mailing Address)

BLM and (enter your company name here), agree to electronically send and receive report data transactions (Transactions), in agreed formats in substitution for conventional paper-based documents, and to assure that such Transactions are legally valid and enforceable, agree to the following terms and conditions:

WIS is an information system owned and operated by the US Federal Government, and permits members of the public to be granted individual user accounts to the system. In order to comply with US Federal Government e-Authentication requirements, organizations are responsible for maintaining specific records for all WIS application users associated with your organization.

As an organization approved to use WIS, your organization agrees to assign one or more individuals in your organization as an official WIS Account Representative (WISAR). The WISAR acts as the central point of contact and is ultimately responsible for all WIS user accounts associated with their organization.

The WISAR agrees to perform identity-proofing of all individuals granted WIS user accounts and agrees to retain appropriate records that verify identity-proofing has been performed on all individuals granted WIS user accounts. Identity-proofing simply consists of verifying an individual is who they claim to be. Identity proofing requirements can be satisfied by observing and recording pertinent information of qualifying records. These qualifying records are often collected during normal hiring processes.

Identity-proofing and the qualifying records that support identity-proofing can vary based on whether identity-proofing is performed in person or remotely.

In-person identity-proofing: In-person identity-proofing involves face-to-face communication with the individual to be granted a WIS user account (the applicant) and is the preferred method for performing identity-proofing. In-person identity-proofing is performed by having the applicant present to the WISAR government-issued picture identification that contains the applicant's picture, and either the address of record or nationality of the applicant (e.g. driver's license or passport).

The WISAR inspects the photo identification, compares the picture to the applicant, and records the identification number, the address or record and the date of birth of the applicant. If the identification appears valid and the photo matches the applicant then the WISAR can authorize or issue credentials and send notice to the address of record.

Remote identity-proofing: Remote identity-proofing is performed when face-to-face communication with the individual to be granted a WIS user account (the applicant) cannot be performed. Remote identity-proofing still requires the applicant provide identification that verifies their identity. The applicant is required to communicate to the WISAR, a government-issued identification number (e.g. driver's license number or passport number) and a financial account number (e.g., checking account, savings account, loan or credit card number) with confirmation records of either number. For example, applicants may communicate the driver's license number and a savings account number to the WISAR via telephone, and confirm the numbers by sending a copy of the actual driver's license or the actual financial statement to the WISAR via fax or mail.

The WISAR inspects both the identification number and the account number supplied by the applicant. The WISAR then verifies information provided by the applicant including the identification number or the account number through record checks either with the applicable agency or institution or through credit bureaus or similar databases, and confirms that: the

applicant's name, date of birth, address of record, or other personal information in records are on balance consistent with the application and sufficient to identify a unique individual.

If the information provided by the applicant checks out, then the WISAR can authorize or issue credentials and send notice to the address of record confirmed in the records check or, issues credentials in a manner that confirms the ability of the applicant to receive telephone communications or e-mail communications at a telephone number or e-mail address associated with the applicant in records. The WISAR retains all records received by the applicant.

1. Documents. During the term of this ECA, each party may electronically transmit to or receive from the other party any of the following as specified:
 - a. Documents. Document data transaction sets (Documents) are as listed in the Appendix and include all Documents which the parties, by conventional written agreement signed by both parties, have added to the Appendix collectively. The format and transmittal of all Documents will comply with the standards identified for the electronic transmission methodology selected, and the published industry and Government guidelines as set forth in the Appendix.
2. Electronic Transfer Methods. The electronic transfer methods which may be used during the term of this ECA to transmit to, or receive from the other party, may be any of the following:
 - a. Electronic Data Interchange. Electronic Data Interchange (EDI) is the direct computer to computer interchange of data using standards as set forth by the American National Standards Institute (ANSI) Accredited Standards Committee (ASC) X12. The exchange may use the services of a third party service provider with which either party may contract.
 - b. World Wide Web. The World Wide Web (WWW) is the computer to computer exchange of Hypertext Markup Language (HTML) documents using standards as set forth by the World Wide Web Consortium (W3C). The completion of forms on web pages at Universal Resource Locations (URL) as specified in the appendix may be utilized under this agreement.
 - c. Electronic Mail. Electronic Mail (E-Mail) is the electronic exchange of human-to-human communications, notes, informational reports, and files of data using a commercial electronic mail service. Data files must be formatted using ASCII or CSV formats and BLM record layouts as set forth in the Appendix.
 - d. Computer Readable Media. Computer readable media such as magnetic tape, cassettes, floppy disks, or diskettes **will not** be exchanged under this ETPA.
 - e. Electronic Bulletin Boards. The use and exchange of information or data using electronic bulletin boards **will not** be exchanged under this ECA.
3. Third Party Service Providers/Commercial Electronic Mail Services. Documents will be transmitted electronically to each party as specified in the Appendix either directly, using a commercial electronic mail service, or through a third party service provider (Provider) with which either party may contract. Either party may modify its election to use, not to use, or to change a Provider upon 30 days written notice. Each party will be responsible for the costs of any Provider or commercial electronic mail service with which it contracts, unless otherwise set forth in the Appendix.
4. Equipment. Each party, at its own expense, will provide and maintain all of the equipment, software, communications linkages, Provider or commercial electronic mail services, and testing necessary to effectively and reliably transmit and receive Documents.
5. Security Procedures. Each party will properly use those security procedures, including those specified in the Appendix, if any, which are reasonably sufficient for effecting the authorized transmission of Documents and for protecting its business records and data from improper access.

6. Signatures. Each party will adopt as its signature(s) an electronic identification(s) consisting of symbol(s) or code(s) which are to be affixed or contained in each Document transmitted by such party (Signature) as set forth in the Appendix. Each party agrees that any Signature of such party affixed to or contained in any transmitted Document will be sufficient to verify that such party originated such Document and that the contents of the Document are accurate and complete. Neither party will disclose to any unauthorized person the Signature of the other party. Each party will notify the other of its Signature and is authorized to change its Signature at any time and from time to time by such notice as set forth in the Appendix. Any Document without a signature, as described in this paragraph, is invalid.
7. Notices. Notices required or permitted under this ECA will be provided in accordance with the provisions set forth in the Appendix.
8. Receipt. Documents will not be deemed to be received, and no Document will give rise to any obligation, until the same is accessible to the receiving party at such party's Receipt Computer, or, is accessible at such party's Provider, as designated in the Appendix. The receipt date and time for Documents transmitted directly is the date and time that the transaction set is accessible to the receiving party at such party's computer system. The receipt date and time for Documents transmitted using Provider services is the date and time of receipt of the Document by the recipient's Provider. Receipt date and time for E-Mail will be the date and time that BLM receives the Document on its electronic mail server.
9. Transmission. The sender is responsible for ensuring on-time receipt of electronic transmissions to ensure that date and time requirements are met for those Documents which are required by BLM to be filed by a particular date and time.
10. Verification. Upon receipt of any Document, the receiving party will immediately transmit a functional acknowledgment, or return receipt, in return, unless otherwise specified in the Appendix. A functional acknowledgment, or return receipt, will constitute conclusive evidence that a Document was received.
11. Unintelligible Transmissions. If any transmitted Document(s) is received in unintelligible or garbled form, the receiving party will immediately notify the originating party (if identifiable from the received Document) by telephone or by electronic transmission of an error condition.
12. Incorporation of Terms. This ECA is subject to all duly promulgated United States Regulations, including those at 43 CFR Parts 3162, 3163 (July 1, 1999) and any other written agreement which references it or which is referenced in the Appendix. The terms of this ECA will prevail in the event of any conflict with any duly promulgated regulations of the United States promulgated after the effective date of this agreement, or any other written agreement to which this agreement is subject.
13. Enforceability. Each Document transmitted pursuant to this Agreement will be considered, in connection with any Transaction, any other written agreement or this ECA, to be a "writing" or "in writing"; and any such Document containing or to which there is affixed a Signature (Signed Documents) will be deemed for all purposes to have been "signed" and to constitute an "original" when printed from electronic files or records established and maintained in the normal course of business. The parties agree not to contest the validity or enforceability of Signed Documents Under the provisions of any applicable law relating to whether certain agreements are in writing and signed by the bound party. Signed Documents, if introduced as evidence on paper in any judicial, arbitration, mediation or administrative proceedings, will be admissible as between the parties to the same extent and under the same conditions as other business records originated and maintained in documentary form. Neither party will contest the admissibility of copies of Signed Documents under either the business records exception to the hearsay rule nor the best evidence rule on the basis that the Signed Documents were not originated or maintained in documentary form.
14. Recordation. Each party will record and retain copies of all Documents and Transactions to the same extent required for paper documents. Such copy will be made by making and retaining a hard copy, microform or computer Readable record in accordance with reasonably reliable data processing practices. Data stored on a microform or

computer readable record must be retrievable and presentable in a visual or printed form.

15. Termination. This ECA will remain in effect until terminated by either party with not less than 30 days prior written notice, which notice will specify the effective date of termination; provided, however, that any termination will not affect the obligations or rights of the parties arising under any Documents or otherwise under this ECA prior to the effective date of termination. In the event of termination, the regulations referenced in the Appendix will govern.
16. Severability. Any provision of this ECA which is determined to be invalid or unenforceable will be ineffective only to the extent of such determination without affecting the validity or enforceability of any remaining provisions.
17. Entire Agreement. This ECA and the Appendix constitute the complete agreement of the parties relating to the matters specified in this ECA and supersede all prior representations or agreements, whether oral or written, with respect to such matters. No oral modification or waiver of any of the provisions of this ECA will be binding on either party.
18. **GOVERNING LAW. THIS ECA WILL BE GOVERNED BY AND INTERPRETED IN ACCORDANCE WITH THE LAWS OF THE UNITED STATES OF AMERICA.**
19. Effective Date. The effective date for the electronic interchange of Documents is _____.
Transmissions prior to this date need not be accepted by the receiving party.
20. Assignment. This ECA is binding upon and inures to the benefit of the parties hereto and their respective successors and assigns. However, neither party may assign any of its rights or delegate any of its obligations under this ECA without the prior written consent of the other party, which consent will not be unreasonably withheld or delayed. Each party has caused this ECA to be properly executed on its behalf as of the date first above written.

Bureau of Land Management

(Enter Your Company Name Here)

By: _____

By: _____

ELECTRONIC COMMERCE AGREEMENT

1. STANDARDS:

- a. American National Standards Institute (ANSI) Accredited Standards Committee (ASC) X12. (EDI)
- b. American National Standards Institute (ANSI) Accredited Standards Committee II. (E-Mail)

2. SERVICE PROVIDERS:

a. THIRD PARTY SERVICE PROVIDERS:

	<u>PROVIDER NAME</u>	<u>ADDRESS</u>	<u>PHONE NUMBER</u>
Bureau of Land Management	AT&T Easylink	12796 Hollenberg Dr.	1-800-624-5672
	<u>PROVIDER NAME</u>	<u>ADDRESS</u>	<u>PHONE NUMBER</u>
*** _____	_____	_____	_____

*** If your Company uses a third party ISP list their name and phone number here. If your company provides its own ISP Service, leave blank.

3. NOTICES:

- a. Notices required or permitted to be sent pursuant to paragraphs 3, 6, 11, and 15 of this ECA will be directed to the attention of the following:

(1) To BLM :

Electronic Data Specialist
 Office of Assistant Director, IRM
 P.O. Box 25047, WO-500D
 Denver, CO 80225-0047

(2) To: _____(Your Company Name and Contact) _____

- b. Notices will be in writing and will be deemed given if delivered personally or if sent by either party to the other by registered or certified mail, postage prepaid, addressed to the other party at the address of that party stated as above. If notice is given by mail, delivery will be deemed effective 7 days after deposit with postal authorities, unless earlier receipt can be verified.
- c. Notice of changes, which would impact the capability of the recipient to receive a Document or EFT, must be given

30 days in advance of any actual change on the part of the sender.

5. SIGNATURES:

- a. Each party will assign its own Signature for authorization of Documents. The signature will be 12 characters and will be selected following standard computer security password selection techniques.
- b. Notification of new, or changes in the signature, will be submitted in non-electronic writing and no other form.
- c. The Bureau of Land Management's signature which will be used to authorize and execute all electronic transmissions with (your company) is: Paul L. Brown - AFMSS/WIS Program Manager.
- d. The (your company) signature which will be used to authorize and execute all electronic transactions with the Bureau of Land Management is: (name of contact).

6. TERMS AND CONDITIONS:

This agreement is subject to the terms and conditions of all existing agreements or Government regulations which may include, but is not limited to:

- a. 25 CFR (April 1, 1999), 43 CFR (October 1, 1998)
- b. Government Paperwork Elimination Act
- c. Computer Security Act of 1987
- d. Minerals Leasing Acts for Federal and Indian Leases

8. CONTACT POINTS:

- a. Technical issue resolution will be directed to the attention of the following:

	<u>NAME</u>	<u>PHONE NUMBER</u>
(1)	BLM Electronic Data Specialist	303-236-4680
(2)	Your Company Name and Title _____	

- b. Business issue resolution will be directed to the attention of the following:

- (1) BLM: Refer to the appropriate handbook, (Appendix A, Section 7) for identification of the specific Contact point.
- (2) Your Company: _____

Note: If your company has more than one user account at different physical locations (different City and State), list all users by name and phone number.

9. **WORLDK WIDE WEB (WWW):**

Documents may be submitted to the BLM via the World Wide Web using the HTTP protocol and the web page forms at the following URL: http://www.blm.gov/wo/st/en/prog/energy/oil_and_gas/WIS.html

10. **ELECTRONIC MAIL:**

- a. The BLM uses various commercial electronic mail services and all E-Mail transmissions to BLM must be compatible with one of those services. Information on currently available services can be obtained from the BLM contact point identified in paragraph 8 above.
- b. The commercial electronic mail service must have the capability for file attachment and for return receipt.
- c. The password (Signature) will be a part of the encrypted E-Mail data file.

12. **SECURITY SOFTWARE PRODUCTS:**

The use of proprietary software products which use data encryption and public/private keyword technology to ensure security and data integrity must be coordinated, tested, and approved by BLM prior to the actual transmission of any Documents.

WIS Account Representative (WISAR) and Identity-Proofing

WIS is an information system owned and operated by the US Federal Government, and permits members of the public to be granted individual user accounts to the system. In order to comply with US Federal Government e-Authentication requirements, organizations are responsible for maintaining specific records for all WIS application users associated with your organization.

As an organization approved to use WIS, your organization agrees to assign one or more individuals in your organization as an official WIS Account Representative (WISAR). The WISAR acts as the central point of contact and is ultimately responsible for all WIS user accounts associated with their organization.

The WISAR agrees to perform identity-proofing of all individuals granted WIS user accounts and agrees to retain appropriate records that verify identity-proofing has been performed on all individuals granted WIS user accounts. Identity-proofing simply consists of verifying an individual is who they claim to be. Identity proofing requirements can be satisfied by observing and recording pertinent information of qualifying records. These qualifying records are often collected during normal hiring processes.

Identity-proofing and the qualifying records that support identity-proofing can vary based on whether identity-proofing is performed in person or remotely.

In-person identity-proofing: In-person identity-proofing involves face-to-face communication with the individual to be granted a WIS user account (the applicant) and is the preferred method for performing identity-proofing. In-person identity-proofing is performed by having the applicant present to the WISAR government-issued picture identification that contains the applicant's picture, and either the address of record or nationality of the applicant (e.g. driver's license or passport).

The WISAR inspects the photo identification, compares the picture to the applicant, and records the identification number, the address or record and the date of birth of the applicant. If the identification appears valid and the photo matches the applicant then the WISAR can authorize or issue credentials and send notice to the address of record.

Remote identity-proofing: Remote identity-proofing is performed when face-to-face communication with the individual to be granted a WIS user account (the applicant) cannot be performed. Remote identity-proofing still requires the applicant provide identification that verifies their identity. The applicant is required to communicate to the WISAR, a government-issued identification number (e.g. driver's license number or passport number) and a financial account number (e.g., checking account, savings account, loan or credit card number) with confirmation records of either number. For example, applicants may communicate the driver's license number and a savings account number to the WISAR via telephone, and confirm the numbers by sending a copy of the actual driver's license or the actual financial statement to the WISAR via fax or mail.

The WISAR inspects both the identification number and the account number supplied by the applicant. The WISAR then verifies information provided by the applicant including the identification number or the account number through record checks either with the applicable agency or institution or through credit bureaus or similar databases, and confirms that: the applicants name, date of birth, address of record, or other personal information in records are on balance consistent with the application and sufficient to identify a unique individual.

If the information provided by the applicant checks out, then the WISAR can authorize or issue credentials and send notice to the address of record confirmed in the records check or, issues credentials in a manner that confirms the ability of the applicant to receive telephone communications or e-mail communications at a telephone number or e-mail address associated with the applicant in records. The WISAR retains all records received by the applicant.

Resources and Summary

- Blank and Completed Submission Forms
- Sample E-Mail notifications
- Trading Partner Agreement
- Helpful Hints
- WEB-based Resources
- Contact Information