



**Department of
Management**

State of Iowa IT Master Agreement

Contract Declaration and Execution

Agreement #2025-BUS-7274

1. Agreement – General Information and Term			
Agreement Number:	2025-BUS-7274 (Esri #00332632.0)		
Title of Agreement (“Agreement”)	Geographic Information System		
State Piggybacking	Delaware		
Underlying Agreement Number	DTI190015-GIS		
Cooperative Contract Website	https://mmp.delaware.gov/Contracts/		
Start Date (“Effective Date”)	As of last signature		
End Date	May 20, 2026		
Renewal Term	Annual		
Number of Renewals	4		
Use by Other Governmental Entities: This Agreement may be used by other Governmental Entities, including but not limited to other state governments and political subdivisions thereof.			
2. Vendor Information			
Vendor:	Environmental Systems Research Institute, Inc. (Esri)		
Sales Contact:	Name: Joe Eckmann	Email address: jeckmamm@esri.com	Phone: 909-793-2853
Contract Manager:	Name: Contracts & Legal	Email address: legalnotices@esri.com	Phone: 909-793-2853
Addresses:	Main Address: 380 New York Street Redlands, CA 92373-8100	Billing Address: See attached Exhibit 1, Update of Remittance Information	Notice Address: 380 New York Street Redlands, CA 92373-8100
SAM Unique Entity Identifier: WUK9A5UR33S7	Iowa Secretary of State Business Number: 317747	Organized/Incorporated under the laws of: State of California	Vendor Security Framework - Attachment B: NIST 800-53, ISO 270001
3. Agency Information			
Issuer:	State of Iowa, by and through the Iowa Department of Management (“DOM”) or (“Department” per Underlying Agreement)		
Contract Manager:	Laura Shannon	laura.shannon@dom.iowa.gov 515-672-4569	



**Department of
Management**

State of Iowa IT Master Agreement

Contract Declaration and Execution

Agreement #2025-BUS-7274

Addresses:	<u>Contact and Billing Address:</u> IA Dept of Management Attn: Business Services 200 E. Grand Ave, Ste.100 Des Moines, IA 50309 E: ITContracts@dom.iowa.gov	<u>Main Address and Formal Notices Address:</u> Iowa Department of Management Attn: Office of General Counsel 1007 E Grand Ave, G13 Des Moines, IA 50319 email: domlegalnotices@iowa.gov
-------------------	--	--

4. Master Agreement Summary

GIS products, SaaS-based GIS products, associated Data products, and associated services.

5. Documents Incorporated/Order of Precedence

This Agreement and all attachments and external documents identified below are incorporated by this reference and together comprise the terms and conditions governing the relationship between the Parties, to be interpreted in the following order of precedence:

- 5.1. Ancillary agreements unique to an Authorized Entity making purchases hereunder that specifically address state, local, or federal regulatory or compliance concerns and which may be incorporated via an Ordering Document; when mutually agreed upon and signed by both parties.
- 5.2. The following incorporated terms, to the extent expressly designated as applicable in an Ordering Document:
 - 5.2.1. Reserved.
 - 5.2.2. Reserved.
 - 5.2.3. The Federal Certifications, attached as Attachment F.
 - 5.2.4. Iowa Code chapter 8F.
- 5.3. These General Terms and Conditions, including Attachment E Data Processing Addendum, and Attachment G Security Addendum;
- 5.4. The Underlying Agreement identified above;
- 5.5. The terms of any Ordering Documents executed hereunder when mutually agreed upon and signed by both parties.



State of Iowa IT Master Agreement
Contract Declaration and Execution
Agreement #2025-BUS-7274

6. Signatures	
IN WITNESS WHEREOF, in consideration of the mutual covenants set forth above and for other good and valuable consideration, the receipt, adequacy, and legal sufficiency of which are hereby acknowledged, the Parties have caused their respective duly authorized representatives to execute this Agreement, which is effective as of the Effective Date.	
Vendor	State of Iowa (“Department”)
Environmental Systems Research Institute, Inc.	Department of Management
Authorized signature: <i>Annette Kazandjian</i>	Authorized signature: <i>Kraig Paulsen</i>
Date: 12/16/2025 1:01 PM CST	Date: 12/19/2025 11:03 AM CST
Printed Name: Annette Kazandjian	Printed Name: Kraig Paulsen
Title: Managing Business Attorney	Title: Director, Department of Management

Attachment A

General Terms and Conditions

The parties may be referred to herein individually as a **“Party”** or collectively as the **“Parties.”**
The Parties agree to the following:

1. Overview.

- 1.1. Term. The initial term of this Agreement is as stated on the Contract Declaration and Execution Section (CD&E), unless terminated earlier in accordance with the terms of this Agreement. After the expiration of the initial term, DOM may, in its sole discretion, unilaterally renew this Agreement for the number of annual renewals stated on the CD&E. The initial term and any available renewals shall be referred to as the **“Term.”** The Term of this Agreement shall not exceed that of the Underlying Agreement.
- 1.2. Relationship between this Agreement and Individual Ordering Documents. Each Ordering Document as defined in the Underlying Agreement executed hereunder shall be deemed, upon its execution, to incorporate the terms and conditions of this Agreement and shall constitute a separate, distinct, and independent Agreement between Vendor and the applicable Authorized Entity. To the extent an Authorized Entity other than DOM makes a purchase hereunder pursuant to an Ordering Document executed by it, such Authorized Entity shall be solely responsible for any payments due, duties, and obligations otherwise owed Vendor under the separate Ordering Document. In addition, notwithstanding any other provision of this Agreement to the contrary, DOM bears no obligation or liability for any other Authorized Entity’s losses, liabilities, or obligations, including Vendor’s failure to perform, arising out of or relating in any way to this Agreement. Likewise, the State of Iowa generally bears no obligation or liability for any political subdivision or other non-State Entity’s losses, liabilities, or obligations, including the Vendor’s failure to perform, arising out of or relating in any way to this Agreement.
- 1.3. Incorporation of the Underlying Agreement. Governmental entities making purchases hereunder shall be afforded all of the rights, privileges, warranties, and indemnifications afforded the Underlying Agreement, and such rights, privileges, warranties, and indemnifications shall accrue and apply with equal effect to governmental entities making purchases hereunder. Except as otherwise provided herein or in an Ordering Document, Vendor shall perform all duties, responsibilities and obligations required under the Underlying Agreement in the time and manner specified thereunder. In the event of any conflict or inconsistency between the terms and conditions of this Agreement and the Underlying Agreement, such conflict or inconsistency shall be resolved as stated on the CD&E. Where Attachment A General Terms and Conditions are silent, the Underlying Agreement necessarily prevails.

2. Definitions. In addition to any other terms that may be defined elsewhere in this Agreement, the following terms shall have the following meanings:

- 2.1. **“Confidential Information”** means, subject to any applicable federal, state, or local laws and regulations, including Iowa Code Chapter 22, any confidential or proprietary information or trade secrets disclosed by either Party (**“Disclosing Party”**) to the other Party (**“Receiving Party”**) that, at the time of disclosure, is designated as confidential (or like designation), is disclosed in circumstances of confidence, or would be understood by the Parties, exercising reasonable business judgment, to be confidential. Confidential Information does not include any information that: (i) was previously and rightfully in



Department of
Management

Geographic Information System
2025-BUS-7274

the possession of the Receiving Party from a source other than the Disclosing Party; (ii) was known to the Receiving Party prior to the disclosure of the information by the Disclosing Party; (iii) was disclosed to the Receiving Party without restriction by an independent third party having a legal right to disclose the information; (iv) is in the public domain; (v) is independently developed by the Receiving Party without any reliance on Confidential Information disclosed by the Disclosing Party; (vi) is disclosed or is required or authorized to be disclosed in compliance with applicable law; or (vii) is disclosed by the Receiving Party with the written consent of the Disclosing Party.

- 2.2. **“DOM” or “Department”** means the State of Iowa Department of Management or as “Department” per Underlying Agreement and, unless the context clearly indicates otherwise, any independent contractors, consultants, or other third parties (including other governmental entities) who are retained, hired, or utilized by DOM in furtherance of this Agreement.
- 2.3. **“Vendor”** means the entity identified on the CD&E including any employees, or any other Vendor staff or personnel acting on behalf of or at the direction of Vendor, which personnel may alternatively be referred to as **“Vendor Personnel.”**

3. Modified Underlying Agreement Terms.

- 3.1. Where the Underlying Agreement refers to “Department,” “Department” shall mean the Department of Management (“DOM”).
- 3.2. Where the Underlying Agreement refers to contract number DTI190015-GIS in Section 7.2 Purchase Order Requirements item d, that contract number is replaced with 2025-BUS-7274.
- 3.3. Where the Underlying Agreement refers to the State of Delaware, Delaware is replaced with Iowa.
- 3.4. Section 8.1(d) is amended as follows:

The Department will pay each invoice within sixty (60) days after the date of receipt of a correct invoice. ESRI is invited to offer value added discounts at which time a Purchasing Entity is permitted to accept a payment term shorter than 60 days pursuant to Iowa Code 8A.514.

- 3.5. Article 10(a) Confidentiality is amended to delete under 29 Del. C. ' 10001, et seq.,” and replace with Iowa Code Chapter 22. Notwithstanding the provision of 10(a) the State will not disclose Confidential Information under this agreement.
- 3.6. Amend Article 13 to create a new Section 13.9 Customer Content that reads:

13.9 Customer Content. It is Customer’s responsibility to determine the storage location for its Data. For Customer ArcGIS Online accounts Customer is able to choose between utilizing the US or EU region for storing their content. Therefore, customers that want their content stored on US servers must select the US region at set up. Customer Content or Customer data will only be stored on United States based servers, provided Customer selects United States as the region for Online Services servers and uses the enhanced endpoint option (if applicable). Customers are responsible for the backup of their datasets.

- 3.7. Article 15 is deleted in its entirety and replaced with the following:



Department of
Management

Geographic Information System
2025-BUS-7274

Article 15 MAINTENANCE.

US Customers: If the Department or Authorized Entity is in the United States, Vendor will provide Maintenance for Software and Online Services in accordance with the Esri Maintenance and Support Program provided in Attachment H and with this reference is incorporated into this Agreement. Provided the affected Department or Authorized Entity is current on payment of North America Regulated Industries Support (NORUS) fees, Vendor will provide technical support to the Department or its Authorized Entities solely in the continental United States of America; otherwise, technical support can be provided from Vendor domestically or by the Vendor's offshore partners, depending on load balance and staff availability.

- 3.8. Section 16.3 c. is amended by deleting it and replacing it with the following:

c. Task Orders may have the format shown in Attachment C attached herein and incorporated into to Agreement or any other agreed-upon format.
- 3.9. Section 16.7 is amended to include:

d. To the extent any Ordering Document calls for reimbursement of travel using Vendors travel policy in Sections 16.7.c and 19.7 in the Underlying Agreement. Travel expenses shall be included in Task Orders for a given project.

e. The Department or its Authorized Entity shall pay all approved invoices in arrears and, to the extent applicable, in conformance with Iowa Code section 8A.514 The Department or its Authorized Entities may pay in fewer than sixty (60) days, but an election to pay in fewer than sixty (60) days shall not, to the extent applicable, act as an implied waiver of Iowa Code section 8A.514. Pursuant to Iowa Code section 8A.514, subitem 3 if payment is not made within sixty (60) days after the date of receipt of a correct invoice an interest payment of one percent (1%) per month for the unpaid balance is mandated.
- 3.10. Section 19.3 is deleted in its entirety. The contacts for Contract Administrator and Billing can be found on the CD&E page.

Accounts Payable: IA Department of Management
Attn: Business Services
200 E. Grand Avenue, Ste.100 Des Moines, IA 50309
Email: ITContracts@dom.iowa.gov
- 3.11. Underlying Agreement Attachment A, Glossary of Terms, Customer Content is deleted in its entirety and replaced with the following meaning:

“Customer Content” means Customer’s original Content (including but not limited to metadata, layers) that Customer :
(a) provides, uploads, or makes accessible to Vendor by or on behalf of the Customer (including its contractors acting on the behalf of the Customer and other authorized users) in connections with Customer’s use of Esri Offerings or Services; or
(b) develops, creates, or uses through Customer’s use of Esri Offerings or Services.
(c) Customer Content excludes any feedback, suggestions, or requests for improvements that the Department or an Authorized Entity provides to Vendor.
- 3.12. Attachment B, Article 3.1 is amended to include the following:



**Department of
Management**

**Geographic Information System
2025-BUS-7274**

Pursuant to Iowa Code 13.2(1)(b), the Department shall have the right to participate in its own defense through a representative of the Iowa Department of Justice. Settlement offers made on behalf of the Department which requires monetary contribution from the Department or subjects the Department to any performance obligation must be approved by the applicable Department.

- 3.13. Attachment B, Article 3.3 is amended to include the following as the last sentence to this section:

Notwithstanding the foregoing, this section 3.3 is subject to Iowa Administrative Code rule 11-120.5.

- 3.14. Attachment B, Article 4(d) is amended to replace the indicated address with the following:

State of Iowa - Department of Management
200 East Grand Avenue
Des Moines, IA 50309

- 3.15. Attachment B, Article 7.12(c) is deleted in its entirety.

- 3.16. Attachment B, Article 7.15 is amended to replace the Delaware address with the Notice Address in the CD&E.

- 3.17. Attachment B, Article 7.18(g) is deleted in its entirety.

- 3.18. Attachment B, Article 7.18(h) is deleted in its entirety and replaced with the following:

Vendor shall maintain records that sufficiently and properly document the Vendor's performance under this Agreement, including records that document fees and other amounts charged to the Authorized Entities during the term of this Agreement, for a period of at least three years following the later of the date of final payment, termination, or expiration of this Agreement.

Department may inspect ESRI's books and records at commercially reasonable time during normal business hours with thirty (30) days prior written notice in order to monitor the performance of this Agreement or an Ordering Document.

- 3.19. Attachment B, Article 7.19(b) is deleted in its entirety.

- 3.20. Attachment B, Article 7.19(e) is deleted in its entirety.

4. Additional Terms.

4.1. Administrative Fees and Reporting.

- 4.1.1. Vendor shall provide a 1.00% administrative fee on all sales made through this Agreement, without affecting authorized prices/rates. This 1.00% administrative fee shall be paid quarterly to the Iowa Department of Management, Attn: Business Services Division Administrator, at the billing address located in CD&E section. Payment shall be made in accordance with the following schedule:

<u>Period End</u>	<u>Fee Due</u>
-------------------	----------------



Department of
Management

Geographic Information System
2025-BUS-7274

June 30
September 30
December 31
March 31

August 30
November 30
February 28
May 31

- 4.1.2. The Vendor shall submit a quarterly report within 30 days after Period End via email to ITContracts@dom.iowa.gov detailing all sales in the State of Iowa and identifying the Authorized Entity, the Ordering Document number, and the State of Iowa Contract number.
- 4.2. Set-off Against Sums Owed by Vendor. The State may offset payments owed Vendor under this Agreement by sums the Vendor owes the State or any of its subdivisions in any context. The Vendor agrees that this provision constitutes proper and timely notice under any applicable laws governing offset.



Department of
Management

Geographic Information System
2025-BUS-7274

ATTACHMENT C SAMPLE TASK ORDER

Esri Agreement No. _____
Iowa Agreement No. 2025-BUS-7274
Task Order No. _____

In accordance with the terms and conditions of the above-referenced Agreement between Environmental Systems Research Institute, Inc. (“Esri”), and _____ (“Customer”), _____ (“Customer Address”), this Task Order authorizes preparation and provision of the Deliverables described and in accordance with the terms, schedule, and start/end date(s) specified below.

1. Scope of Work: *[As applicable, specifically identify and describe Deliverables including custom code, map data, technical data (including technical assistance), and the resources to be provided by Customer (including Customer-supplied personnel, software, hardware, and digital or hard-copy data) and place of delivery and location where technical assistance will be provided.]*

In addition to the foregoing, Customer agrees that its employees, representatives, and subcontractors will cooperate and communicate with Esri during performance of this Task Order. Without cost to Esri, Customer shall provide, allow access to, or assist Esri in obtaining all data Esri requests for performance of this Task Order, including, but not limited to, (1) copies of previously prepared reports, maps, plans, surveys, records, and other documents in the control or possession of Customer and (2) copies of ordinances, codes, regulations, or other governmental documents.

2. Contract Type: Firm Fixed Price (FFP)
3. Total Firm Fixed Price Task Order Value: _____
4. Customer Address for the Receipt of Esri Invoices:
5. Delivery Schedule or Start/End Date(s) for Each Deliverable:
6. Special Considerations:
7. Esri Project Manager: *[insert name, telephone, and email address]*
Esri Contract Specialist: *[insert name, telephone, and email address]*
Customer Project Manager: *[insert name, telephone, and email address]*
Customer Contract Contact: *[insert name, telephone, and email address]*
Customer Accounts Payable Contact: *[insert name, telephone, and email address]*

ACCEPTED AND AGREED:

[sample only—do not sign]
(Customer)

ENVIRONMENTAL SYSTEMS
INSTITUTE, INC.
(Esri)

Signature: [sample only—do not sign]

Signature: [sample only—do not sign]

Printed Name: _____

Printed Name: _____

Title: _____

Title: _____

Date: _____

Date: _____

ATTACHMENT E DATA PROCESSING ADDENDUM

Data Processing Addendum



This Data Processing Addendum ("**Addendum**") is effective on the first date that Customer provides to Esri Personal Data (as defined below) subject to the applicable Privacy Law (as defined below) and forms part of the Master Agreement or other written or electronic agreement ("**Agreement**") by and between the organization signing or accepting below ("**Customer**") and **Environmental Systems Research Institute, Inc. ("Esri")**, and sets forth the terms and conditions relating to the privacy, confidentiality, and security of Personal Data associated with Online Services and subscription and maintenance services to be rendered by Esri to Customer pursuant to the Agreement. All terms defined or used in the Agreement shall have the same meaning in this Addendum unless otherwise specified. Terms used in this Addendum that are not defined herein or in the Agreement shall have the meaning set forth in the applicable Privacy Law.

Whereas Customer may provide Esri, a company located in the United States, with access to Personal Data to act as a Processor or Service Provider in connection with Online Services and subscription and maintenance services performed by Esri for or on behalf of Customer pursuant to the Agreement; and

Whereas Customer requires that Esri preserve and maintain the privacy and security of such Personal Data as a Processor according to the terms of this Addendum;

Now therefore, in consideration of the mutual covenants and agreements in this Addendum and the Agreement and for other good and valuable consideration, the sufficiency of which is hereby acknowledged, Customer and Esri agree as follows:

SECTION I—DEFINITIONS

- A. "**Privacy Laws**" means the European Union (EU) General Data Protection Regulation (GDPR) 2016/679 of the European Parliament and of the Council of 27 April 2016, the California Consumer Privacy Act of 2018 (CCPA) (as amended by the California Privacy Rights Act [CPRA]), or other privacy laws applicable to Esri.
- B. The terms "personal data," "data subject," "processing," "controller," "processor," and "supervisory authority" as used in this Addendum have the meanings given in the GDPR.
- C. "**Personal Data**" means personal data, personal information, or personally identifiable information as defined in applicable Privacy Laws about individuals located in the European Union; Switzerland; the United Kingdom; California, USA; or other locations covered by Privacy Laws and may include, but not be limited to, the following: (i) categories of data subjects: prospects, customers, business partners, and vendors; and (ii) types of personal data: name, title, position, email address, and location.
- D. "**Data Incident**" means a breach of Esri's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data on systems managed or otherwise controlled by Esri. Data Incidents will not include unsuccessful attempts or activities that do not compromise the security of Personal Data, including unsuccessful login attempts, pings, port scans, denial-of-service attacks, and other network attacks on firewalls or networked systems.
- E. "**Data Privacy Framework**" means the EU-U.S. Data Privacy Framework (EU-U.S. DPF), the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF).

SECTION II—PRIVACY, CONFIDENTIALITY, AND INFORMATION SECURITY

- A. Authority to Process Personal Data
 - i. Customer and Esri agree that Customer is the Controller and Esri is the Processor or Service Provider of Personal Data, except when Customer is a Processor of Personal Data, then Esri is a subprocessor.
 - ii These Addendum terms do not apply where Esri is a Controller of Personal Data (e.g., Personal Data received and Processed by Esri as needed for account setup, authorization, and sign-on in the My Esri self-service portal). Esri's Privacy Statement (available at <https://www.esri.com/en-us/privacy/privacy-statements/privacy-statement>), together with any related privacy notices or statements, and the Data Transfer Agreement apply where Esri is a Controller.

- iii. Esri will Process Personal Data only with Customer's written instructions (a) on behalf of and for the benefit of Customer; (b) for the purposes of Processing Personal Data in connection with the Agreement; and (c) to carry out its obligations pursuant to this Addendum, the Agreement, and applicable Privacy Laws and other law.
- iv. Customer will have the exclusive authority to determine the purposes for and means of Processing Personal Data. Esri will not (a) retain, use, or disclose Personal Data outside of the direct business relationship between the parties or for any purpose other than performing under the Agreement, except as otherwise permitted by this Addendum or the Privacy Laws; or (b) combine Customer's Personal Data with any other personal information received or collected from or on behalf of another person, provided that Esri may combine personal information for a business purpose (as defined under CCPA/CPRA).
- v. The subject matter and details of the processing are described in Annex I of Attachment 1, and this Addendum (including the Attachment and Annexes) and the Agreement are Customer's complete instructions to Esri for the Processing of Personal Data. Any alternative or additional instructions may only be by written amendment to this Addendum.
- vi. To the extent Customer discloses or otherwise makes available deidentified data (as defined in CCPA/CPRA or other Privacy Laws) to Esri or Esri creates deidentified data from Personal Data, Esri shall (a) implement reasonable measures to ensure that such deidentified data is not used to infer information about or otherwise be linked to a particular natural person or household; (b) publicly commit to maintain and use such deidentified data in a deidentified form and not attempt to reidentify the deidentified data; and (c) before sharing deidentified data with any affiliate or third party, including subprocessors, contractors, or any other persons ("**Recipients**"), contractually obligate any such Recipients to comply with all requirements of this section. Notwithstanding the prior sentence, Esri may attempt to reidentify the data solely for the purpose of determining whether its deidentification processes are compliant with Privacy Laws.

B. Disclosure of and Access to Personal Data

- i. Esri will hold in confidence all Personal Data. Esri will not Sell or Share (as defined in the CCPA/CPRA) Personal Data.
- ii. Esri will (a) provide at least the same level of privacy protection for Personal Data received from Customer, as is required by the GDPR, CCPA, and other applicable Privacy Laws, and the Data Privacy Framework principles that may be found on the Data Privacy Framework [website](#); (b) promptly notify Customer if at any time Esri determines that it can no longer meet its obligation to provide the same level of protection as is required by the Privacy Laws and the Data Privacy Framework and (c) take reasonable and appropriate steps to remediate the processing of such Personal Data. If, at any time, Customer notifies Esri that Customer has reasonably determined that Esri is not Processing the Personal Data in compliance with the Privacy Laws, Customer may take reasonable and appropriate steps to stop and remediate any unauthorized Processing of such Personal Data.
- iii. If Esri Processes Personal Data provided by Customer that is subject to the GDPR and Esri is established in, or transfers or makes accessible any Personal Data to any subprocessors in a country that does not ensure adequate data privacy safeguards are in place within the meaning of GDPR, then Esri will enter into the standard contractual clauses with Customer as set forth in Attachment 1 of this Addendum ("SCCs") or ensure that adequate data privacy safeguards are in place, such as binding corporate rules or the Data Privacy Framework certification. If applicable, each party's signature to this Addendum shall be considered a signature to the SCCs. If a subprocessor is a Data Importer (as that term is used in such SCCs), Esri shall either (a) enter into contractual obligations with subprocessor, where such obligations contain adequate privacy safeguards in accordance with GDPR, or (b) enter into the SCCs with Customer on behalf of such data importer. In the event the transfer is covered by more than one transfer mechanism, the transfer of personal data will be subject to a single transfer mechanism, as applicable, and in accordance with the following order of precedence: (a) the Data Privacy Framework; (b) the SCCs; and if neither of the preceding is applicable, then (c) other alternative data transfer mechanisms permitted under applicable Privacy Laws will apply.
- iv. Esri will not share, transfer, disclose, or otherwise provide access to any Personal Data to any third party, or contract any of Esri's rights or obligations concerning Personal Data to a third party, unless Customer has authorized Esri to do so in writing, except as required by law. Where Esri, with the consent of Customer, provides to a third party access to Personal Data or contracts such rights or obligations to a third party, Esri

will, with each third party, (a) enter into a written agreement that imposes obligations on the third party that are consistent with the GDPR, CCPA, and the other Privacy Laws; (b) transfer the Personal Data to the third party only for the limited and specified purposes as instructed by Customer; (c) require the third party to notify Esri if the third party determines that it can no longer meet its obligation to provide the same level of protection as is required by the applicable Privacy Laws; and (d) upon notice, take reasonable and appropriate steps to stop and remediate unauthorized Processing. Customer hereby provides its consent for Esri to use subprocessors as necessary to provide the services including, but not limited to, Microsoft Corporation; Amazon Web Services, Inc.; Salesforce, Inc.; and Akamai Technologies (including their affiliates) and Esri's technical support vendors. To the extent that Esri makes any changes with regard to the use of its subprocessors, it shall inform Customer and provide Customer with the right to object to such change. To the extent Customer has a reasonable objection to such change in subprocessors, the parties shall cooperate to address the objection in a reasonable manner.

- v. Esri will promptly inform Customer in writing of any requests with respect to Personal Data received from Customer's customers, consumers, employees, or other associates. Customer will be responsible for taking action on and responding to any such request, but Esri will reasonably cooperate with Customer to address any such request or a request by an individual about whom Esri holds Personal Data for access, rectification, objection, portability, restriction, erasure, or export of that individual's Personal Data. For clarity, Customer is a Controller of Named User Credentials, as defined in the Master Agreement. Customer is solely responsible for taking action on and responding to any data subject requests associated with Named User Credentials.
 - vi. Taking into account the state of the art; the costs of implementation; and the nature, scope, context, and purposes of Processing, as well as the risk of varying likelihood and severity of the rights and freedoms of natural persons, Esri will implement appropriate technical and organizational measures to protect the Personal Data from loss; misuse; and unauthorized access, disclosure, alteration, and destruction. Such measures are set forth in Annex II of Attachment 1. To this effect, Esri will limit internal access to Personal Data so that it is only accessible on a need-to-know basis to fulfill Esri's performance of services for or on behalf of Customer, by personnel who have agreed to comply with privacy and security obligations that are substantially similar to those required by this Addendum.
 - vii. Subject to applicable law, Esri will notify Customer immediately in writing of any subpoena or other judicial or administrative order by a government authority or proceeding seeking access to or disclosure of Personal Data. Customer may, if it so chooses, seek a protective order, and Esri will reasonably cooperate with Customer in such action, provided Customer reimburses Esri for all costs, fees, and legal expenses associated with the action. Esri will have the right to approve or reject any settlements that affect Esri.
 - viii. If Esri becomes aware of a Data Incident, Esri will (a) notify Customer of the Data Incident promptly and without undue delay after becoming aware of the Data Incident; and (b) promptly take reasonable steps to minimize harm and secure Personal Data. Notifications made pursuant to this section will describe, to the extent possible, details of the Data Incident, including steps taken to mitigate the potential risks and steps Esri recommends Customer take to address the Data Incident. Esri will not assess the contents of Personal Data in order to identify information subject to any specific legal requirements. Customer is solely responsible for complying with incident notification laws applicable to Customer and fulfilling any notification obligations to third parties related to any Data Incident(s). Esri's notification of or response to a Data Incident under this section will not be construed as an acknowledgement by Esri of any fault or liability with respect to the Data Incident.
- C. Esri currently has the third-party certifications and review processes in place as described at <https://trust.arcgis.com>. Esri participates in and has certified its compliance with Data Privacy Framework.
- D. Esri will comply with applicable data protection and privacy laws, including, but not limited to, the GDPR and CCPA, to the extent such laws apply to Esri in its role as Processor or Service Provider.
- E. Customer certifies that it has
- i. Obtained the written consent, affirmative opt-in, or other written authorization ("**Consent**") from applicable individuals or has another legitimate, legal basis for delivering or making accessible Personal Data to Esri (as well as its subsidiaries, affiliates, and subprocessors), and such Consent or other legitimate basis allows Esri (and its subsidiaries, affiliates, and subprocessors) to Process the Personal Data pursuant to the terms of the Agreement and this Addendum; and



Department of
Management

Geographic Information System
2025-BUS-7274

- ii. Ensured that the delivery and disclosure to Esri of Personal Data is in compliance with the GDPR, CCPA, and other Privacy Laws that are applicable to Customer.
- F. Esri will assist Customer in ensuring that its secure Processing obligations, as Controller, under the GDPR are met, which may include assisting Customer in a consultation with a supervisory authority where a data protection impact assessment indicates that the intended Processing would result in a high level of risk. Upon request, Esri shall make available to Customer the information necessary to demonstrate compliance with the GDPR and will allow for and contribute to audits, including inspections, to confirm Esri's compliance with this Addendum by Controller or another auditor mandated by Controller. At Customer's request to verify compliance, Esri will provide to Customer a summary of its most recent independent third-party audit results or similar self-assessment. The summary will be provided no more than once annually, and disclosure of the summary will be subject to a written nondisclosure agreement between the parties. An on-site audit may be conducted by Customer or an independent third-party auditor as agreed by the parties when (i) such an audit is required by Privacy Law or Customer's competent supervisory authority; and (ii) Customer has received a notice from Esri of a Data Incident affecting Customer's Personal Data. The scope and scheduling of such audit will be mutually agreed upon by the parties in advance. Any on-site audits will be limited to Customer Content processing and storage facilities operated by Esri. Customer acknowledges that Esri operates a multitenant cloud environment. Accordingly, Esri shall have the right to reasonably adapt the scope of any on-site audit to avoid or mitigate risks with respect to, and including, service levels, availability, and confidentiality of other Esri customers' information. All expenses resulting from this Subsection F will be incurred by Customer, unless Esri is found materially noncompliant. Customer must promptly notify Esri of any discovered noncompliance.
- G. Upon fulfillment of the purpose for which Customer provided Personal Data under this Addendum, Esri shall either return all Personal Data Processed on behalf of Customer or delete or destroy the Personal Data, including any existing copies, at Customer's expense, if any, unless Esri has a legal obligation to maintain such Personal Data.
- H. Trial, Evaluation, and Beta Program offerings may employ lesser or different privacy and security measures than those typically present in the Online Services. Unless otherwise noted, Customer should not use trial, evaluation, and beta program offerings to process Personal Data or other data that is subject to legal or regulatory compliance requirements. The following terms in this Addendum do not apply to trial, evaluation, and beta program offerings: Processing of Personal Data, GDPR, Data Security, and Health Insurance Portability and Accountability Act (HIPAA) Business Associate.

CUSTOMER CERTIFIES THAT IT AND ITS EMPLOYEES UNDERSTAND THESE RESTRICTIONS AND WILL COMPLY WITH THEM.

IN WITNESS WHEREOF, the parties acknowledge their agreement to the foregoing by due execution of this Addendum by their respective authorized representatives. The Addendum cannot be modified or amended by either party except with a separate written document signed by both parties.

_____	ENVIRONMENTAL SYSTEMS
(Customer)	RESEARCH INSTITUTE, INC.
By: _____	(Esri)
Authorized Signature	By: <u>Tamisa Greening</u>
Printed Name: _____	Authorized Signature
Title: _____	Printed Name: <u>Tamisa Greening</u>
Date: _____	Title: <u>Director, Contracts and Legal</u>
Customer Number: _____	

ATTACHMENT 1
STANDARD CONTRACTUAL CLAUSES IMPLEMENTATION

1. The Parties agree that, with respect to the implementation of the EU Standard Contractual Clauses (Commission Decision 2021/914) ("SCCs") under the Addendum, one or more of the following Modules of the SCCs will apply and are referenced herein: (i) Controller to Processor ("Module Two" or "C2P"); (ii) Processor to Processor ("Module Three" or "P2P").
2. To the extent one or more of the foregoing SCCs apply, the Parties agree to the following:
 - a) Clause 7 (Docking Clause) shall not apply;
 - b) The Option 2 (General Written Authorisation) provision of Clause 9(a) (Use of subprocessors) shall apply, and the specified time period shall be thirty (30) days;
 - c) The Clause 11(a) (Redress) option shall not apply;
 - d) Governing law under Clause 17 (Governing law) shall be law of the Republic of Ireland; and
 - e) Clause 18 (Choice of forum and jurisdiction) shall mean the courts of the Republic of Ireland.

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

1. **Name:** As identified in the Agreement and this Addendum
Address: Per Esri's customer service records
Contact person's name, position and contact details: Per Esri's customer service records
Activities relevant to the data transferred under these Clauses: Online Services and subscription and maintenance services to be rendered by Esri to Customer
Signature and date: Each party's signature of the Addendum shall be considered a signature to these Clauses.
Role (controller/processor): Controller

Data importer(s):

1. **Name:** Environmental Systems Research Institute, Inc. ("Esri")
Address: 380 New York Street, Redlands, CA 92373, USA
Contact person's name, position, and contact details: Chief Information Security Officer,
privacy@esri.com
Activities relevant to the data transferred under these Clauses: Online Services and subscription and maintenance services to be rendered by Esri to Customer
Signature and date: Each party's signature of the Addendum shall be considered a signature to these Clauses.
Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Data about individuals is provided to Esri via the Online Services and subscription and maintenance services by (or at the direction of) Customer or by Customer end users, who may include Customer's customers, employees, suppliers, and End Users.

Categories of personal data transferred

Data related to individuals is provided to Esri via the Online Services and subscription and maintenance services, by (or at the direction of) Customer or by Customer end users.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as strict purpose limitation, access restrictions (including access only for staff having followed specialised training), recordkeeping of access to the data, restrictions for onward transfers, or additional security measures

Considering that only Customer (not Esri) has full knowledge and control in relation to what data is provided to Esri via the Online Services and subscription and maintenance services, Esri treats all Customer Content to the standards of sensitive data by providing the technical and organizational measures described in Annex II. Customer is responsible for verifying that such measures are appropriate for the specific categories of data provided to Esri via the Online Services and subscription and maintenance services.

The frequency of the transfer (e.g., whether the data is transferred on a one-off or continuous basis)

The frequency of the transfer depends on the frequency at which Customer provides Personal Data to Esri via the Online Services and subscription and maintenance services. It is expected that transfers may be on a one-off and/or continuous basis.

Nature of the processing

Spatial analytics is accomplished through the following operations, dependent on Customer's choice of settings and actions performed: collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or other method of making available, alignment or combination, restriction, or erasure or destruction.

Purpose(s) of the data transfer and further processing

Esri will process Personal Data for the purposes of providing the Online Services and subscription and maintenance services to Customer in accordance with the Agreement.

The period for which the personal data will be retained or, if that is not possible, the criteria used to determine that period

The period for which the personal data will be retained depends on the duration of processing as determined by Customer and Customer's additional instructions.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

Cloud services and technical support services involve processing of the same nature and duration as described above.

C. COMPETENT SUPERVISORY AUTHORITY

As applicable, competent supervisory authority will be in accordance with Clause 13.

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Esri will maintain administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Personal Data uploaded to ArcGIS Online Services and subscription and maintenance services, as described in the Security and Privacy Documentation applicable to the specific ArcGIS Online Services and subscription and maintenance services purchased by the data exporter, as updated from time to time, and accessible via <https://trust.arcgis.com/en/security/security-overview.htm> or otherwise made reasonably available by Esri.

A. Technical Measures for ArcGIS Online Services. Esri implemented the following technical measures for the above-referenced ArcGIS Online Services:

- i. The state-of-the-art encryption algorithm and its parameterization (e.g., key length; operating mode, if applicable) are used for Customer data at rest.
- ii. The strength of the encryption takes into account the time period during which the confidentiality of the encrypted personal data must be preserved.
- iii. The encryption algorithm is implemented by properly maintained software, the conformity of which to the specification of the algorithm chosen has been verified by certification.
- iv. The keys are reliably managed (generated, administered, stored, linked to the identity of an intended recipient, and revoked).
- v. ArcGIS Online allows Customer (data exporter) to pseudonymize the fields (e.g., user credentials) in such a manner that the personal data can no longer be attributed to a specific data subject, nor be used to single out the data subject in a larger group, without the use of additional information exclusively held and controlled by Customer (data exporter), of which Customer (data exporter) retains sole control of the algorithm or repository that enables reidentification using additional information.
- vi. ArcGIS Online supports best practices for transport encryption protocols.
- vii. A trustworthy public key certification authority and infrastructure are used.
- viii. Specific protective and state-of-the-art measures are used against active and passive attacks.
- ix. The existence of backdoors (in hardware or software) has been ruled out.
- x. ArcGIS Online can be used in combination with ArcGIS Enterprise in a configuration that allows Customer (data exporter) to store and manage Personal Data under Customer's (data exporter's) control without transferring it to a third country, whereas a data exporter processes Personal Data in such a manner that it is split into two or more parts, and the part that is being transferred to the third country can no longer be interpreted or attributed to a specific data subject without the use of additional information under Customer's (data exporter's) control.

Additional information on technical measures can be found at <https://trust.arcgis.com/en/documents/>.

B. Organizational and Contractual Measures

- i. Esri's efforts around privacy are described at <https://www.esri.com/en-us/privacy/overview>.
- ii. Esri commits to treating Personal Data per its Privacy Statement (available at <https://www.esri.com/en-us/privacy/privacy-statements/privacy-statement>) and the Esri Products & Services Privacy Statement Supplement (available at <https://www.esri.com/en-us/privacy/privacy-statements/privacy-supplement>).
- iii. Esri provides a presigned Data Processing Addendum that contains Standard Contractual Clauses, available at <https://www.esri.com/en-us/privacy/privacy-gdpr>.
- iv. Esri maintains and enforces an internal personal information protection policy that requires employees to protect Personal Data that they access.
- v. Esri maintains a corporate security policy that addresses access controls and corporate security measures.

C. Adoption of Further Requirements and Right to Early Termination. If supervisory authorities adopt further requirements and measures with regard to the transfer of Personal Data to the US, Esri will amend this Addendum to fulfill the additional requirements. If Esri cannot meet the additional requirements, Customer shall have the right to terminate the Agreement for convenience (without termination fee or penalty) by giving written notice thereof to Esri.



Department of
Management

Geographic Information System
2025-BUS-7274

ATTACHMENT F FEDERAL CERTIFICATIONS

Federal Requirements. Vendor agrees to comply with the following federal obligations pursuant to 2 C.F.R. part 200, Appendix II:

1. Prohibition on Certain Telecommunications and Video Surveillance Services or Equipment.

In accordance with 2 CFR 200.216 and 2 CFR Pt. 200, App. II, Section K, Vendor is prohibited from obligating or expending loan or grant funds to: (1) Procure or obtain; (2) Extend or renew a contract to procure or obtain; or (3) Enter into a contract (or extend or renew a contract) to procure or obtain equipment, services, or systems that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system.

As described in Public Law 115-232, section 889, covered telecommunications equipment is telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities).

- a. For the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities).
- b. Telecommunications or video surveillance services provided by such entities or using such equipment.
- c. Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of the National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country.

2. Domestic Preferences for Procurements. As appropriate and to the extent consistent with law, and consistent with 2 CFR 200.317 and 2 C.F.R. Pt. 200, App. II, Sec. L, the Vendor should, to the greatest extent practicable, provide a preference for the purchase, acquisition, or use of goods, products, or materials produced in the United States (including but not limited to iron, aluminum, steel, cement, and other manufactured products). The requirements of this section must be included in all subawards including all contracts and purchase orders for work or products under this award. For purposes of this section: (1) "Produced in the United States" means, for iron and steel products, that all manufacturing processes, from the initial melting stage through the application of coatings, occurred in the United States; (2) "Manufactured products" means items and construction materials composed in whole or in part of non-ferrous metals such as aluminum; plastics and polymer-based products such as polyvinyl chloride pipe; aggregates such as concrete; glass, including optical fiber; and lumber.

3. Procurement of recovered materials. To the extent applicable, and in accordance with 2 CFR Pt. 200, App. II, Section J, the Vendor must comply with section 6002 of the Solid Waste Disposal Act, as amended by the Resource Conservation and Recovery Act. The requirements of Section 6002 include procuring only items designated in guidelines of the Environmental Protection Agency (EPA) at 40 CFR part 247 that contain the highest percentage of recovered materials



**Department of
Management**

**Geographic Information System
2025-BUS-7274**

practicable, consistent with maintaining a satisfactory level of competition, where the purchase price of the item exceeds \$10,000 or the value of the quantity acquired during the preceding fiscal year exceeded \$10,000; procuring solid waste management services in a manner that maximizes energy and resource recovery; and establishing an affirmative procurement program for procurement of recovered materials identified in the EPA guidelines.

4. **Contract Work Hours and Safety Standards Act (40 U.S.C. § 3701-3708).** In accordance with 2 CFR Pt. 200, App. II, Sec. E., to the extent that Vendor's contract is in excess of \$100,000 and involves the employment of mechanics or laborers, Vendor must act in compliance with 40 U.S.C. §§ 3702 and 3704, as supplemented by Department of Labor regulations (29 C.F.R. part 5). To the extent applicable, Vendor must compute the wages of every mechanic and laborer on the basis of a standard work week of 40 hours. Work in excess of the standard work week is permissible provided that the worker is compensated at a rate of not less than one and a half times the basic rate of pay for all hours worked in excess of 40 hours in the work week. The requirements of 40 U.S.C. § 3704 are applicable to construction work and provide that no laborer or mechanic must be required to work in surroundings or under working conditions which are unsanitary, hazardous or dangerous. These requirements do not apply to the purchases of supplies or materials or articles ordinarily available on the open market, or contracts for transportation or transmission of intelligence.
5. **Clean Air Act (42 U.S.C. §§ 7401-7671q.) and the Federal Water Pollution Control Act (33 U.S.C. §§ 1251-1387), as amended.** In accordance with 2 CFR Pt. 200, App. II, Section G, Vendor agrees to comply with all applicable standards, orders or regulations issued pursuant to the Clean Air Act (42 U.S.C. §§ 7401-7671q) and the Federal Water Pollution Control Act as amended (33 U.S.C. §§ 1251-1387). Vendor agrees to comply with these Applicable Laws, violations of which must be reported to the State and federal awarding agency and the regional office of the Environmental Protection Agency (EPA).
6. **Davis-Bacon Act, as amended (40 U.S.C. 3141-3148).** To the extent required by Federal program legislation, and in accordance with 2 CFR Pt. 200 App. II, Section D, all prime construction contracts in excess of \$2,000 awarded by non-Federal entities must include a provision for compliance with the Davis-Bacon Act (40 U.S.C. 3141-3144, and 3146-3148) as supplemented by Department of Labor regulations (29 CFR Part 5, "Labor Standards Provisions Applicable to Contracts Covering Federally Financed and Assisted Construction"). In accordance with the statute, and to the extent mandated under federal law, Vendor must pay wages to laborers and mechanics at a rate not less than the prevailing wages specified in a wage determination made by the Secretary of Labor. In addition, Vendor must pay wages not less than once a week. Vendor must place a copy of the current prevailing wage determination issued by the Department of Labor in each solicitation. The Agreement is conditioned upon the acceptance of the wage determination. Vendor must report all suspected or reported violations to the Federal awarding agency. Vendor must also comply with the Copeland "Anti-Kickback" Act (40 U.S.C. 3145), as supplemented by Department of Labor regulations (29 CFR Part 3, "Contractors and Subcontractors on Public Building or Public Work Financed in Whole or in Part by Loans or Grants from the United States"). Vendor is prohibited from inducing, by any means, any person employed in the construction, completion, or repair of public work, to give up any part of the compensation to which he or she is otherwise entitled. Vendor must report all suspected or reported violations to the Federal awarding agency.
7. **Rights to Inventions Made Under a Contract or Agreement.** To the extent applicable and in accordance with 2 C.F.R. Pt. 200 App. II, Section F, the Vendor must comply with the requirements of 37 CFR Part 401, "Rights to Inventions Made by Nonprofit Organizations and Small Business



Department of
Management

Geographic Information System
2025-BUS-7274

Firms Under Government Grants, Contracts and Cooperative Agreements,” and any implementing regulations issued by the awarding agency.

8. **Suspension and Debarment.** This certification is required by the provisions of Executive Orders 12549 and 12689 and 31 C.F.R. part 19 regarding Debarment, Suspension, and Other Responsibility. In accordance with 2 C.F.R. Pt. 200, App. II, Section H, Vendor certifies that it is not listed on the government-wide exclusions in the System of Award Management (“SAM”), in accordance with the OMB guidelines at 2 CFR 180 that implement Executive Orders 12549 (3 C.F.R. part 1986 Comp., p. 189) and 12689 (3 C.F.R. part 1989 Comp., p. 235), “Debarment and Suspension.” SAM Exclusions contains the names of parties debarred, suspended, or otherwise excluded by agencies, as well as parties declared ineligible under statutory or regulatory authority other than Executive Order 12549.
9. **Lobbying.** This certification is required by the provisions of Section 319 of Public Law 101-121, Government wide Guidance for New Restrictions on Lobbying, and 31 U.S.C. § 1352. These regulations require certification by Vendor (and its subcontractors) that they have not engaged in prohibited lobbying activities and/or have filed any required disclosures in accordance with these Applicable Laws. Submission of this certification is a prerequisite for making or entering into this transaction imposed by Section 1352, Title 31, U.S. Code; any person who fails to file the required certification may be subject to a civil penalty of not less than \$10,000 and not more than \$100,000 for each such failure. In accordance with 2 C.F.R. Pt. 200, App. II, Section I, Vendor certifies the following:
 - a. No federal funds have been paid or will be paid, by or on behalf of Vendor, to any person for influencing or attempting to influence an officer or employee of the Customer, a member of Congress, an officer or employee of Congress, or an employee of a member of Congress in connection with the awarding of any federal contract, the making of any federal grant, the making of any federal loan, the entering into of any cooperative agreement, or the extension, continuation, renewal, amendment, or modification of any federal contract, grant, loan, or cooperative agreement.
 - b. If any funds other than federal funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of the Customer, a member of Congress, an officer or employee of Congress, or an employee of a member of Congress in connection with any federal contract, grant, loan, or cooperative agreement, Vendor must complete and submit Standard Form-LLL, “Disclosure Form to Report Lobbying” in accordance with its instructions.
10. **Assurance of Compliance Nondiscrimination in Federally Assisted Programs & Equal Opportunity.** This certification requires Vendor to comply with any applicable federal nondiscrimination requirements or laws providing for or requiring equal opportunity in employment, in compliance with 2 CFR Pt. 200, Appendix II, Section C. Except as otherwise provided under 41 C.F.R. part 60, all contracts that meet the definition of “federally assisted construction contract” in 41 C.F.R. part 60-1.3 must include the equal opportunity clause provided under 41 CFR 60-1.4(b), in accordance with Executive Order 11246, “Equal Employment Opportunity” (30 FR 12319, 12935, 3 C.F.R. part, 1964-1965 Comp., p. 339), as amended by Executive Order 11375, “Amending Executive Order 11246 Relating to Equal Employment Opportunity,” and implementing regulations at 41 C.F.R. part 60, “Office of Federal Contract Compliance Programs, Equal Employment Opportunity, Department of Labor.” To the extent required by these Applicable Laws, Vendor certifies during the performance of this Agreement that:



- a. Vendor will not discriminate against any employee or applicant for employment because of race, color, religion, sex, sexual orientation, gender identity, or national origin. Vendor will take affirmative action to ensure that applicants are employed, and that employees are treated during employment without regard to their race, color, religion, sex, sexual orientation, gender identity, or national origin. Such action shall include, but not be limited to the following: Employment, upgrading, demotion, or transfer; recruitment or recruitment advertising; layoff or termination; rates of pay or other forms of compensation; and selection for training, including apprenticeship. Vendor agrees to post in conspicuous places, available to employees and applicants for employment, notices to be provided setting forth the provisions of this nondiscrimination clause.
- b. Vendor will, in all solicitations or advertisements for employees placed by or on behalf of Vendor, state that all qualified applicants will receive consideration for employment without regard to race, color, religion, sex, sexual orientation, gender identity, or national origin.
- c. Vendor will not discharge or in any other manner discriminate against any employee or applicant for employment because such employee or applicant has inquired about, discussed, or disclosed the compensation of the employee or applicant or another employee or applicant. This provision shall not apply to instances in which an employee who has access to the compensation information of other employees or applicants as a part of such employee's essential job functions discloses the compensation of such other employees or applicants to individuals who do not otherwise have access to such information, unless such disclosure is in response to a formal complaint or charge, in furtherance of an investigation, proceeding, hearing, or action, including an investigation conducted by the employer, or is consistent with Vendor's legal duty to furnish information.
- d. Vendor will send to each labor union or representative of workers with which he has a collective bargaining agreement or other contract or understanding, a notice to be provided advising the said labor union or workers' representatives of Vendor's commitments under this section, and shall post copies of the notice in conspicuous places available to employees and applicants for employment.
- e. Vendor will comply with all provisions of Executive Order 11246 of September 24, 1965, and of the rules, regulations, and relevant orders of the Secretary of Labor.
- f. Vendor will furnish all information and reports required by Executive Order 11246 of September 24, 1965, and by rules, regulations, and orders of the Secretary of Labor, or pursuant thereto, and will permit access to his books, records, and accounts by the administering agency and the Secretary of Labor for purposes of investigation to ascertain compliance with such rules, regulations, and orders.
- g. In the event of Vendor's noncompliance with the nondiscrimination clauses of this contract or with any of the said rules, regulations, or orders, this contract may be canceled, terminated, or suspended in whole or in part and Vendor may be declared ineligible for further Government contracts or federally assisted construction contracts in accordance with procedures authorized in Executive Order 11246 of September 24, 1965, and such other sanctions may be imposed and remedies invoked as provided in Executive Order 11246 of September 24, 1965, or by rule, regulation, or order of the Secretary of Labor, or as otherwise provided by law.
- h. Vendor will include the portion of the sentence immediately preceding paragraph (a) and the provisions of paragraphs (a) through (h) in every subcontract or purchase order unless exempted by rules, regulations, or orders of the Secretary of Labor issued pursuant to

section 204 of Executive Order 11246 of September 24, 1965, so that such provisions will be binding upon each subcontractor or vendor. Vendor will take such action with respect to any subcontract or purchase order as the administering agency may direct as a means of enforcing such provisions, including sanctions for noncompliance: Provided, however, that in the event a Vendor becomes involved in, or is threatened with, litigation with a subcontractor or vendor as a result of such direction by the administering agency, Vendor may request the United States to enter into such litigation to protect the interests of the United States.

- i. Vendor further agrees that it will be bound by the above equal opportunity clause with respect to its own employment practices when it participates in federally assisted construction work: provided that if Vendor so participating is a State or local government, the above equal opportunity clause is not applicable to any agency, instrumentality or subdivision of such government which does not participate in work on or under the contract.
- j. Vendor agrees that it will assist and cooperate actively with the administering agency and the Secretary of Labor in obtaining the compliance of Vendor and subcontractors with the equal opportunity clause and the rules, regulations, and relevant orders of the Secretary of Labor, that it will furnish the administering agency and the Secretary of Labor such information as they may require for the supervision of such compliance, and that it will otherwise assist the administering agency in the discharge of the agency's primary responsibility for securing compliance.

Vendor further agrees that it will refrain from entering into any contract or contract modification subject to Executive Order 11246 of September 24, 1965, with a contractor debarred from, or who has not demonstrated eligibility for, Government contracts and federally assisted construction contracts pursuant to the Executive Order and will carry out such sanctions and penalties for violation of the equal opportunity clause as may be imposed upon contractors and subcontractors by the administering agency or the Secretary of Labor pursuant to Part II, Subpart D of the Executive Order. In addition, Vendor agrees that if it fails or refuses to comply with these undertakings, the administering agency may take any or all of the following actions: Cancel, terminate, or suspend in whole or in part this grant (contract, loan, insurance, guarantee); refrain from extending any further assistance to the applicant under the program with respect to which the failure or refund occurred until satisfactory assurance of future compliance has been received from such applicant; and refer the case to the Department of Justice for appropriate legal proceedings.

ATTACHMENT G SECURITY ADDENDUM

1.0 SCOPE – ARCGIS ONLINE

The purpose of this Security Addendum (this “**Addendum**”) is to identify the security controls’ framework and capabilities that apply to Esri’s provision of FedRAMP Authorized ArcGIS Online Services as US-based operations (“**ArcGIS Online**”) to Customer. ArcGIS Online is a secure, reliable geographic information system (GIS) delivered using the software-as-a-service (SaaS) model. Esri’s obligations under this Addendum will continue until the Customer’s use of ArcGIS Online ends.

These security requirements do not apply to (i) Customer Content uploaded to servers located outside of the United States (see, Section 5.0 Regions - Redundancy); (ii) Customer’s equipment, network, infrastructure, information systems; (iii) Customer’s data that resides on the Customer’s side of the firewall; (iv) Customer’s data provided to Esri as part of a Professional Services engagement (e.g., development or consulting services); or (v) Customer’s data accessed by Esri as part of the provision of maintenance and tech support (please see the Maintenance and Support Program, available on Esri’s website via the following link: [Maintenance & Support Program and Product Lifecycle Support Policy | Esri Legal](#)).

2.0 SECURITY CAPABILITIES; SECURITY POLICIES

Esri publishes its security and privacy capabilities at <https://trust.arcgis.com>. Further, Esri has a formal security management system, policies, procedures and standards in place, authorized by Esri’s executive management, which establishes the responsibility and authority of Esri’s information security program. Esri has internal security policies and procedures designed to implement and support the requirements of FedRAMP, which are not shared with customers. In addition, Esri has implemented a Risk Assessment Process as part of its Continuous Monitoring Plan, which includes the generation of a Plan of Action and Milestones. Esri’s security policies and procedures are reviewed and updated at least annually.

Customer may reference the ArcGIS Online Cloud Security Alliance (CSA) [Consensus Assessments Initiative Questionnaire \(CAIQ\)](#) on the Documents page of the Trust Center website.

3.0 DEFINITIONS

Any capitalized term in this Addendum that is not specifically defined in this Addendum shall have the meaning ascribed to it in the agreement (the “Agreement”) to which this Addendum is attached.

“**ArcGIS Online**” means the secure mapping and spatial analysis ‘off-the-shelf’ software as a service platform offered by Esri to Customer as a web mapping platform.

“**Authorized Personnel**” means Esri’s employees, contractors, and Cloud Service Providers who access and/or process Customer Content in connection with Esri’s provisioning to Customer of ArcGIS Online. Esri’s ArcGIS Online operations team maintains records of access control grants to all Authorized Personnel.

“**Cloud Service Providers**” means Amazon Web Services and Microsoft Azure.

“**FedRAMP**” means the Federal Risk and Authorization Management Program that provides a standardized approach to security authorizations for cloud service offerings. A cloud service offering may be authorized through an individual agency or the Joint Authorization Board.

“**Information Security System**” means a discrete set of information resources organized for the storage, processing, maintenance, usage, transmittal, or disposition of information.

“**Security Incident**” means a breach of security that has occurred, as confirmed by Esri upon diligent investigation, and that involves the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Content, on information systems managed or otherwise controlled by



Department of Management

Geographic Information System
2025-BUS-7274

Esri. A Security Incident does not include unsuccessful attempts or activities that do not compromise the security of Customer Content, including unsuccessful login attempts, pings, port scans, denial-of-service attacks, and other network attacks on firewalls or networked systems.

4.0 FEDRAMP / NIST COMPLIANCE AND THE FEDRAMP MARKETPLACE

ArcGIS Online is certified as FedRAMP Moderate as shown on the FedRAMP Marketplace available at [FedRAMP Marketplace](#), and Esri's security framework is fully aligned with NIST SP 800-53 security controls (v4 and v5). Both FedRAMP and NIST SP 800-53 map to ISO 27001 security standards. FedRAMP Authorized is a designation provided to cloud service providers (CSPs) that have successfully completed the FedRAMP Authorization process with the Joint Authorization Board (JAB) or a federal agency. Esri's third-party Cloud Service Providers are fully compliant with FedRAMP and NIST SP 800-53 (v.4 and v.5) and are ISO 27001 certified.

FedRAMP is a United States government-wide program that offers a standardized approach in security assessment, authorization, and continuous monitoring in cloud products for all customers. FedRAMP includes an audit of an organization's security program by a certified independent auditor across security controls and is frequently considered as the gold standard for security assurance of cloud service offerings.

5.0 REGIONS – REDUNDANCY

Cloud Service Providers provide multiple availability zones as well as regions for redundancy. By default, all ArcGIS Online customer data resides on United States soil (US-based servers) within the confines of the Amazon Web Services US Regions (East, West), and Microsoft Azure US Regions (South Central, East, West). Customers are responsible for the backup of their datasets.

6.0 MULTITENANT ENVIRONMENT – AMAZON WEB SERVICES (AWS) AND MICROSOFT AZURE

ArcGIS Online is provided to customers as an off-the-shelf SaaS offering and is operated by the Cloud Service Providers, which provide the physical assets for ArcGIS Online as third-party cloud services providers and not as Esri's subcontractors. The Cloud Service Provider's policies are reviewed and approved by applicable company leadership at least annually or on an as needed basis. ArcGIS Online cloud infrastructure providers have physical security measures for their data centers that comply with high industry standards for physical security controls. For more information, visit their respective compliance sites.

7.0 ACCESS TO CUSTOMER'S SYSTEMS OR NETWORK

In its provision of ArcGIS Online, Esri does not access Customer networks, information systems, or equipment, except if requested by Customer in connection with maintenance and technical support.

8.0 SECURITY REQUIREMENTS – GENERAL

8.1 Application. The security requirements found in this Addendum apply to all Customer Content which is uploaded by Customer to ArcGIS Online and stored, processed and transmitted by Esri as part of its provision of ArcGIS Online to Customer. Customer Content will remain the sole property of Customer and Esri will not use the Customer Content for any purpose other than to perform its obligations in the provision of ArcGIS Online to Customer. Customer is responsible for management of the data that Customer uploads to ArcGIS Online.

8.2 Security control requirements. Esri shall implement and maintain, during the term of the Agreement and until the Customer's use of ArcGIS Online ends, security and privacy controls for its information systems designed to protect the confidentiality, integrity and availability of Customer Content, as well as the continuity of operations for information systems, in alignment with FedRAMP moderate security requirements and with NIST Special Publication 800-53 (v.4 and v.5) security controls. Changes to Esri's cybersecurity policy, including security updates and security patches applied to ArcGIS Online are available via Esri's Trust Center, under Overview, Announcements. Customer may subscribe to the RSS feed available on that webpage.

8.3 FedRAMP Assessment Report. Upon Customer's written request, which shall not be made more than once per calendar year, and pursuant to a mutually executed nondisclosure agreement provided by Esri, Esri will provide to Customer a copy of its FedRAMP Assessment Report.



Department of Management

Geographic Information System
2025-BUS-7274

8.4 Audits – Summary. As part of ArcGIS Online FedRAMP Authorization continued monitoring, Esri leverages an independent third-party auditor to perform testing. Upon Customer's written request, which shall not be made more than once per calendar year, and pursuant to a mutually executed nondisclosure agreement provided by Esri, Esri will provide to Customer a summary of such audit. Customer will not audit Esri's information systems or facilities.

9.0 NOTIFICATION OF A SECURITY INCIDENT TO CUSTOMER

9.1 Notification. Esri will notify the Customer within seventy-two (72) hours of a Security Incident. Esri will (a) assist and coordinate with Customer's designated employees to investigate the Security Incident, and (b) take commercially reasonable measures, based on Esri's assessment of risk, to mitigate the effects of the Security Incident. Notifications made pursuant to this section 9.1 – Notification will describe, to the extent possible, and if known, the details of the Security Incident, including (i) a description of the nature of the event that caused the Security Incident, (ii) the suspected amount of Customer Content exposed or compromised, (iii) information addressing any new facts and circumstances learned after initial notice to Customer, (iv) steps taken to mitigate potential risks, and (v) steps Esri recommends that Customer take to address the Security Incident. Esri acknowledges that, in some instances, Customer may have a reporting obligation to regulators and/or other third parties in the event of a Security Incident and that Esri's compliance with the foregoing notification obligation is necessary for Customer compliance with regulatory and other legal obligations. Esri will not inform any third party of a Security Incident without first obtaining Customer's prior written consent, unless required by law or by a court order.

As agreed to by the parties, Esri will provide Customer with a written report describing the Security Incident, actions taken by Esri during its response, and Esri's plans for future actions to prevent a similar Security Incident from occurring. Esri does not provide incident logs to its customers. Esri may provide a root cause analysis and remediation plan upon Customer's request.

9.2 Customer's e-mail address for notifications. Esri will notify Customer of a Security Incident by contacting Customer's point of contact listed below [Customer may provide an alias e-mail instead]:

Name: _____
Title: _____
Telephone Number: 515-281-4SOC (4762) _____
Email address: soc@iowa.gov

9.3 Customer notifications to Esri. Customer can report security issues or concerns via the Esri Trust Center by selecting the link "Report a Security or Privacy Concern" located on the Overview page. Customer will then be directed to the form available via [Report a Security or Privacy Concern | ArcGIS Trust Center | Documentation](#). Reported issues and concerns are managed by Esri's Product Security Incident Response Team (PSIRT).

10.0 ENCRYPTION

ArcGIS Online utilizes encryption at-rest and in transit by default. Customer Content is encrypted at rest with AES-256, which is a FIPS 140-2 compliant encryption algorithm and in transit with HTTPS via TLS 1.2, in alignment with FedRAMP requirements. ArcGIS Online encryption keys are maintained by the ArcGIS Online operations team, but stored in Esri's Key Management Service which is FIPS 140-2 compliant and also in alignment with FedRAMP requirements. In addition, endpoints are regularly validated against SSL Labs (Secure Socket Layer) and against dynamic scanners to test the SSL configurations and ensure encryption is in alignment with current industry recommendation.

11.0 MULTIFACTOR AUTHENTICATION

Customer is responsible to grant its employees access to its ArcGIS Online organizational subscription. All Customer ArcGIS Online administration personnel are required to have a unique user ID and password to access the system, as shared accounts are not leveraged. ArcGIS Online has the option to enable Multifactor Authentication (MFA) to identify credentials. For details, please review the resource provided via the following link: <https://doc.arcgis.com/en/arcgis-online/administer/configure-security.htm>.

ArcGIS Online aligns with NIST 800-63 identity management standards. Customer is responsible for



Department of Management

Geographic Information System 2025-BUS-7274

enforcing the minimum password requirements that meet Customer's applicable security policies. Customer should utilize ArcGIS Online organization specific logins to meet all organization username and password management requirements and for adherence to FedRAMP accreditation. Information regarding the configuration of customer-specific logins such as SAML (previously known as enterprise logins) is available through the following link: <http://doc.arcgis.com/en/arcgis-online/administer/enterprise-logins.htm>.

12.0 DISASTER RECOVERY / BUSINESS CONTINUITY

Esri has developed a Disaster Recovery Plan (DR) to ensure that it can restore its critical information systems with a minimum of interruption following a disaster. The DR test plans are exercised at least annually, results are documented, and processes or design changes are implemented. The plans include operation details and take into consideration several types of scenarios. Esri has implemented technological measures such as geographically separated server farms and distributed follow-the-sun technical support centers that further reduce the impact of a disaster. Esri also has established a Business Continuity planning team to develop, implement and maintain additional measures to ensure timely restoration of all critical business functions.

13.0 SERVICE LEVEL AGREEMENT

Esri publishes its ArcGIS Online Service Level Agreement (SLA) on the [Documents](#) page of the ArcGIS Trust Center.

14.0 SECURITY LOGS

Audit logs are reviewed weekly within the ArcGIS Online solution. Audit logs are retained as defined by the ArcGIS Online retention policy, which is in alignment with FedRAMP requirements. Customer may access application security logs for ArcGIS Online through the RESTful API, including Named User ArcGIS Online activity. Logging and monitoring policies are part of the FedRAMP program and reviewed annually. Customer is responsible for monitoring its own activity logs, which include user logs and activities.

15.0 PHYSICAL AND ENVIRONMENTAL SECURITY REQUIREMENTS

Esri facilities and secure data centers have physically secure perimeters; external endpoints are protected against unauthorized access and entry points are equipped with security measures, including cameras covering entry points, along with intrusion detection and alerting capabilities. Access to Esri facilities is limited to Esri personnel and authorized visitors, who are issued and must display unique identification cards while on the premises. Access to secure data centers and to Esri facility areas where Customer information is stored or can be accessed is restricted to authorized Esri personnel. Esri maintains logs of authorized access, which are stored for a period of at least twelve (12) months.



Department of
Management

Geographic Information System
2025-BUS-7274

ATTACHMENT H VENDOR MAINTENANCE AND SUPPORT PROGRAM

Maintenance and Support Program



Customers in the United States that keep their Maintenance or Subscription(s) current have access to support for Qualifying Products. Qualifying Products may be included in an Enterprise Agreement or licensed individually. Support may vary by product, license type, subscription, program, and in accordance with the Esri [Product Life Cycle Support Policy](#) found at <https://downloads2.esri.com/support/TechArticles/Product-Life-Cycle.pdf>, and may include some or all the following:

- Standard Technical Support
- New versions and Software Updates, Hot Fixes and Patches
- Self-Paced E-Learning
- Esri User Conference registration
- Access to ArcGIS Living Atlas Subscriber Content
- Access to the latest ArcGIS Solutions

For a current description of support by product, license type, subscription, or program, please visit <https://go.esri.com/qualifying-products>. For additional details about Esri's support program visit <https://www.esri.com/benefits> or contact Esri Customer Service.

Add-On Support Programs

Customers current on support may purchase one or more of the following add-on support programs on an annual basis ("Add-On Support Programs"), which will run concurrently with their support term:

- Premium Support Services ("PSS")
- Special Events Premium Support Services ("SEPPSS")
- North America Regulated Industries Support ("NORUS")
- After Hours Support
- Enablement Support Services ("ESS")

Esri reserves the right to change the Esri Maintenance and Support Program at any time and, if reasonable under the circumstances, Esri will provide thirty (30) days' advance written notice of any material alterations. Any material alterations will become effective upon renewal.

ARTICLE 1—DEFINITIONS

The terms used are defined as follows:

- a. **"Authorized Caller(s)"** means the Customer-designated individual who may contact Esri to request technical support (e.g., to report technical issues or request product assistance).
- b. **"Case(s)"** means the Esri record that contains technical notes and documentation of all related interactions between Customer and Esri Support Services for a given technical issue. Depending on how the request was initiated, Esri will provide phone, email, chat, or Esri Support App confirmation of the Case creation. The Case will be given a unique identification number for reference and tracking.
- c. **"Customer"** means Licensee or Customer as defined in the Master Agreement or Customer's signed Agreement with Esri.
- d. **"Customer Number"** means a unique number created by Esri to identify each Customer office or site, which is included on Esri invoices.
- e. **"Esri Support Services"** means the Esri technical support team.
- f. **"Hot Fix(es)"** means a single fix in one of the specific functional areas that is critical to Customer (e.g., Customer's production has stopped). Esri will send the Hot Fix to Customer as soon as Esri completes a technical feasibility assessment. With the Hot Fix, Esri will deliver documentation that will clearly identify the technical problems addressed and any limitations. Esri will conduct limited testing on Hot Fixes before providing them to Customer. Esri will incorporate Hot Fixes into subsequent Software Updates. Hot Fixes

do not provide new functionality. Hot Fixes will only function with the associated Esri product type and release.

- g. **"Patch(es)"** means a single fix [see Hot Fix(es)] or a set of related fixes that are in a specific functional area of the Esri product and will apply to multiple Esri customers. Once a Patch is released, it will be incorporated into a subsequent Software Update. Esri conducts limited testing on Patches before providing them to customers. Patches do not provide new functionality. Patches will only function with the associated Esri product type and release.
- h. **"Premium Licensee Authorized Contact" or "Premium LAC"** means up to two (2) individuals designated by Customer as its authorized caller(s) to report a PSS Case and work directly with the TAM.
- i. **"PSS Case(s)"** means a Case that is opened as or elevated to PSS and/or SEPSS via Customer request or technical support's elevation process.
- j. **"Qualifying Product(s)"** means Esri's unmodified products or products that were modified by Esri or under Esri's direction and are eligible for some or all of the support programs.
- k. **"Self-Paced E-Learning"** means a collection of self-paced learning resources for applicable Esri products accessible from the Esri Training website.
- l. **"Software Updates"** means a collection of files that enhance or correct a Qualifying Product and will be available for Customer to download during the support term.
- m. **"TAM"** means the technical account manager who will be the primary point of contact for the coordination and escalation of PSS Cases.

ARTICLE 2—PAYMENT, RENEWAL, REINSTATEMENT, AND EXPIRATION

2.1 Payment. Unless otherwise agreed to in another agreement between Customer and Esri, Esri will provide support for Qualifying Products during an Enterprise Agreement term, Maintenance term, or the term of a Subscription following Esri's acceptance of an order.

2.2 Renewals. Esri will issue a quote approximately ninety (90) days before the expiration date ("**Renewal Quote**"). The Renewal Quote will be sent via email and provide Customer with a breakdown of the Qualifying Products licensed and Support Program(s) due to expire and the associated fees to renew. If Customer has acquired multiple Qualifying Products and/or Support Programs throughout the course of a year, Esri will provide a single Renewal Quote with prorated fees and a common renewal term for all Qualifying Products and Support Program(s).

2.3 Past-Due Renewals (Subscriptions). If Customer does not renew a Subscription to a Qualifying Product prior to the renewal quote's expiration date, but at a later date wants to renew their Subscription, Esri will quote associated fees to renew at then-current pricing with any legacy or migration pricing forfeited.

2.4 Past-Due Renewals (Maintenance on Perpetual Licenses). If Customer does not renew Maintenance on a Qualifying Product prior to their renewal quote's expiration date, but at a later date wants to reinstate Maintenance, fees will include the fees that Customer would have paid since the expiration date. Esri will quote associated fees to renew at then-current pricing with any legacy or migration pricing forfeited.

2.5 Term Expiration. It is Customer's responsibility to renew Maintenance, Subscriptions, or Add-On Support Programs in order to be eligible to receive support. If Esri does not receive a purchase order or payment for renewal prior to the expiration date, Customer will no longer be eligible to receive support.

ARTICLE 3—ESRI USER CONFERENCE REGISTRATION; SELF-PACED E-LEARNING; LIVING ATLAS SUBSCRIBER CONTENT; ARCGIS SOLUTIONS

Support for Qualifying Products may include the following:

3.1 Esri User Conference Registration. Customer must submit a registration form for each individual attending the Esri User Conference. Registrations are assigned in the order received and are nontransferable. Customer may also purchase additional registrations.

3.2 Self-Paced E-Learning. Access to Self-Paced E-Learning requires each individual to have an Esri account, or ArcGIS Online account with Esri Access enabled; have a broadband Internet connection; and be an employee, agent, consultant, or contractor of Customer. For education accounts, individuals may include registered students.

3.3 Living Atlas Subscriber Content. Living Atlas Subscriber Content allows ArcGIS Named Users access to a collection of value-add layers from ArcGIS Online. These layers are denoted by a Living Atlas Subscriber Content badge on their item details pages.

3.4 Latest ArcGIS Solutions. ArcGIS Solutions are a library of prebuilt, industry-specific configurations of ArcGIS that are delivered through a subscription to ArcGIS Online or ArcGIS Enterprise.

ARTICLE 4—STANDARD TECHNICAL SUPPORT

4.1 Scope of Technical Support. As part of support for Qualifying Products, Customer will receive the level of technical support corresponding to the respective life cycle phase. Information on the Qualifying Product life cycle phase and the ArcGIS Product Life Cycle Support Policy can be found at <https://support.esri.com/en/content/productlifecycles>. Esri does not provide technical support for (a) customization of solutions, templates, or tools; (b) patches received outside of a life cycle; or (c) third-party software, hardware, technology, or similar peripherals that are not provided by Esri. However, Esri does answer questions about how to interface Esri products with supported devices. Further details on the scope of technical support are found at <https://support.esri.com/en/supportscope>.

4.2 Authorized Callers. Customer may designate a limited number of Authorized Callers per Qualifying Product. Customer may replace Authorized Callers at any time through the My Esri site.

4.3 Submitting a Case. As part of support for Qualifying Products, Authorized Callers may contact Esri as many times as needed. All requests for technical support must contain detailed information about the technical issue. Authorized Caller must be prepared to provide as much of the following information as possible:

- The Esri Customer Number
- The phone number and email address where Authorized Caller can be reached
- The version of the software and operating system in use
- The database in use, if applicable
- The Online Services, tools, and/or APIs in use, if applicable
- The Esri Global ID
- A description of what Customer was doing when the problem occurred and steps to reproduce the issue
- The exact wording of any error messages that appear on the screen

4.4 Telephone, Chat, Web Form and Esri Support App. If Customer needs help with a technical issue, an Authorized Caller may contact Esri by phone, chat, or web form.

- a. *By Telephone.* The Authorized Caller will be connected to a technical support analyst who will create a Case and be dedicated to work on the technical issue. If a technical support analyst is unavailable, the Authorized Caller may create a Case, which will be placed in a dispatch queue for the next available technical support analyst.
- b. *By Chat.* To initiate a chat consultation, the Authorized Caller must click the Chat with an Analyst button in an Esri Product or at <https://support.esri.com/en/webform-chat>. Chat-based requests can only be made during Esri Support Services operating hours, listed in Article 11 below. The Authorized Caller must create a Case and will be connected to a technical support analyst. If a technical support analyst is unavailable, the Authorized Caller can opt to receive an email notification when the next technical support analyst is available.
- c. *By Web Form.* The Authorized Caller may request technical support by completing an online web form available at My Esri. Requests made through this channel are received twenty-four (24) hours a day, seven (7) days a week, but are logged and assigned to a technical support analyst the next business day. Esri will respond on a first come, first served basis. All Cases reported by web form are given the same priority and level of attention as those reported by telephone.

- d. *By Esri Support App.* The Authorized Caller may create and manage Cases either by telephone or web form using the mobile app. The Esri Support Mobile app is available on Android and iOS devices.

4.5 Technical Support Website. Esri has created a self-help support website for customers to view technical articles, updated product documentation, blogs, links to forums, and technology announcements. Additionally, Authorized Callers may connect to My Esri to submit technical issues, chat with technical specialists, and track Cases. The Esri Support website can be found at <https://support.esri.com>.

4.6 Standard Technical Support Response Time. Esri will respond to a technical support request during Esri Support Services operating hours. Esri will make commercially reasonable efforts to respond according to the severity level of the technical issue as shown in the table below. An Authorized Caller may request that the technical support analyst change a technical issue severity level, but requests for critical and high-severity levels must be made via telephone.

Severity	Criteria	Initial Response Time
Critical	- Causes a severe impact to business operations (e.g., critical business processes are disabled) - No workaround available	Six (6) business hours
High	- Causes a noncritical impact to business operations (e.g., significant degradation of quality or handling of data) - No stable workaround available	Eight (8) business hours
Medium	Causes a minor impact to business operations	Two (2) business days
Routine	Causes little or no impact to business operations	Three (3) business days

4.7 Resolution. After the Case is logged, Esri will use commercially reasonable efforts to provide corrections to a technical issue or supply a workaround. While it is Esri's goal to provide an acceptable resolution to technical issues, Esri cannot guarantee that all technical issues can be fixed or resolved.

CUSTOMERS MAY PURCHASE ADD-ON SUPPORT FOR THE APPLICABLE FEES. DETAILS FOR ADD-ON SUPPORT ARE SET FORTH IN ARTICLES 5 THROUGH 8 BELOW.

ARTICLE 5—PREMIUM SUPPORT SERVICES (PSS) (US AND DIRECT INTERNATIONAL CUSTOMERS) AND SPECIAL EVENTS PREMIUM SUPPORT SERVICES (SEPSS) (US CUSTOMERS ONLY)

PSS or SEPSS includes (i) access to a designated TAM; (ii) the ability for the Premium LAC to convert a Case into a PSS/SEPSS Case at any time; (iii) priority Case management; (iv) the ability to request Cases twenty-four (24) hours a day, three hundred sixty-five (365) days a year; and (v) additional enhanced support and services.

5.1 Technical Account Manager. Esri will assign a TAM to Customer to work directly with the Premium LAC to oversee open Cases.

- TAM will endeavor to (i) conduct quarterly reviews with Customer to align on support goals and objectives; (ii) become familiar with Customer's geographic information system (GIS) software architecture and infrastructure; (iii) verify that all open PSS/SEPSS Cases are prioritized above Standard Technical Support Cases; (iv) coordinate and facilitate priority technical support issues between the Customer and Esri technical teams, and provide escalation management, as needed; (v) identify potential areas of concern, before they arise, to improve Customer's overall operational excellence and stability; and (vi) make reasonable efforts to be available from 5:00 a.m. to 5:00 p.m. (Pacific time), Monday through Friday, except on Esri holidays.
- Esri may replace TAM with another technical account manager of similar skill and background, by written notice to Customer.

- c. All communications will be conducted in the English language unless by written agreement of both parties.

5.2 Priority Case Management. Cases submitted via telephone and web form may be converted to a PSS/SEPSS Case by the Premium LAC and will be given priority handling.

5.3 Case Response Time. In addition to the response times outlined in Article 4.6, Esri will make commercially reasonable efforts to call or send an email response within one (1) business hour of receipt of a new PSS/SEPSS Case, regardless of its severity level. Esri will provide a status report every business day until closure of the PSS/SEPSS Case.

ARTICLE 6—NORTH AMERICA REGULATED INDUSTRIES SUPPORT (US CUSTOMERS ONLY)

NORUS includes technical support from technical support analysts who are confirmed US citizens located in the United States. Cases and Customer data created or collected under the NORUS program are secured within a restricted case management system within Esri Support Services. To assist Customer with data security or regulatory compliance requirements, access is limited to NORUS technical support analysts and those with US Department of Defense (DoD)-level security clearances, when applicable. Staff are located in facilities designed to provide physical, informational, and operational security.

ARTICLE 7—AFTER HOURS SUPPORT (US CUSTOMERS ONLY)

After Hours Support includes the ability to request a Case twenty-four (24) hours a day, three hundred sixty-five (365) days a year. Esri will make commercially reasonable efforts to call or send an email response within one (1) business hour of receipt of a new Case, regardless of its severity level.

ARTICLE 8—ENABLEMENT SUPPORT SERVICES (US CUSTOMERS ONLY)

ESS includes the following four types of activities ("Enablement Activities") for Esri Qualifying Products as documented in the ESS proposal: (i) Installation Support; (ii) Configuration Support; (iii) Enterprise Integration; and (iv) Operations and Administration support. Enablement Activities will be periodically scheduled by Esri and Customer by their respective points of contact. ESS also includes an annual performance review, ongoing technical exchanges throughout the term and monthly reporting.

ARTICLE 9—ARCGIS PLATFORM TECHNICAL SUPPORT (US AND DIRECT INTERNATIONAL CUSTOMERS)

Customers with a current ArcGIS Developer Subscription may purchase ArcGIS Platform Technical Support on an annual basis. Upon payment for ArcGIS Platform Technical Support, Customer will receive all benefits described in Article 4 above and may purchase Add-On Support Programs as described in Articles 5, 6 and 7 above. ArcGIS Platform Technical Support is a stand-alone offering and the benefits described in Article 3 are not included.

ARTICLE 10—CONFIDENTIALITY

All data, conversations, and Cases are confidential in nature. Esri will treat all Cases as confidential, using the same degree of care, but no less than reasonable care, as Esri uses to protect its own confidential information of a similar nature. After ninety (90) days of closing a Case, Esri will delete or destroy all Customer digital data provided to triage the Case, unless otherwise requested by Customer in writing. This obligation to delete or destroy excludes information retained in backup media or other archival records maintained in the ordinary course of business by Esri.



**Department of
Management**

**Geographic Information System
2025-BUS-7274**

ARTICLE 11—CONTACTING ESRI

Esri Support Services

<https://www.esri.com/contactus>

Web: <https://support.esri.com>

Tel.: 909-793-3774

Toll-Free Phone: 888-377-4575, extension 2

Support Web Form: <https://support.esri.com/en/webform>

My Esri: <https://my.esri.com>

Chat: <https://support.esri.com/en/webform-chat>

Esri Corporate Offices

Tel.: 909-793-2853

Fax: 909-793-5953

Email: info@esri.com

Esri Customer Service

Tel.: 888-377-4575, extension 5

Email: service@esri.com

Web: <https://my.esri.com>

Operating Hours: 5:00 a.m. to 5:00 p.m. (Pacific time), Monday through Friday, except Esri holidays.