Revised March 28, 2025
IMPORTANT—READ CAREFULLY

Esri Contractor Data Privacy and Security Terms

These Privacy and Security Terms (the "**Terms**") establish Esri's and Contractor's rights and obligations regarding privacy, security and related matters under the agreement or Task Order (as defined below) that references them (the "**Agreement**"). Except for Section I ("**Definitions**") and Section II ("**Terms Applicable to All Contractors**"), Esri has designed these Terms to be utilized in a modular manner, and only the applicable Terms sections are incorporated by reference into the Agreement.

In the event of any conflict between the Terms and the Agreement or any associated base or other agreement between the parties, the Terms, including any Data Processing Addendum, will prevail. Notices required by these Terms will be made in accordance with the notice provisions of the Agreement or to legalnotices@esri.com.

Esri may amend these Terms to address any requirement under applicable law or to reflect any development in security best practices, or as Esri believes necessary to protect Esri Systems or Esri. Contractor shall provide prompt written notice to Esri if Contractor is unable to comply with the amended Terms; Esri and Contractor shall then negotiate in good faith to further amend the Terms so that they are acceptable to both parties. If the parties are unable to come to mutually agreeable terms, then Esri may at its election either withdraw the amendment or terminate the underlying agreement(s) to which these Terms are attached without penalty to either party.

Table of Contents

Esri and Contractor agree as follows:

I. Definitions

- **Business Contact Information** ("**BCI**") means Personal Data that a party to the Agreement holds and that are used to contact, identify, or authenticate that party's Personnel in a professional or business capacity. Typically, BCI includes an individual's name, business e-mail address, physical address, telephone number or similar attributes.
- **Cloud Service(s)** means software as a service, platform as a service, or infrastructure as a service.
- **Contractor means** Esri's counterparty in the Agreement, which may be referred to as Consultant, Contractor, Supplier, Vendor or as otherwise referenced in the Agreement.
- **Critical IT Deliverables** means deliverables that are critical to Esri operations. This includes Deliverables that could have a catastrophic impact on Esri in the event of loss of confidentiality, integrity, availability, or privacy. Critical IT Deliverables include (but are not limited to) Deliverables that:
  - Are used for security or privacy operations,
  - will host personal information included with Article 9 of GDPR,
  - provide high availability for Esri business operations, or
  - store or process usable financial data.
- **Customer** means a customer of Esri or of an Esri affiliated company.
- **Data Processing Addendum means** an agreement or portion of an agreement that sets forth terms and conditions relating to the privacy, confidentiality, and security of Personal Data associated with the products and services that Contractor provides to Esri.
- **Deliverable(s)** means Services and/or anything that Contractor delivers to Esri under a Task Order including, but not limited to, commercial off-the-shelf Software, custom Software, Hosted Services, technical data, or hardware.
- **Device(s)** means a device that is used for audio, video, or text communication or any other type of computer or computer-like instrument. Examples include, but are not limited to, laptop computers, smart phones, and tablets.
- **Error Correction** means bug fixes and revisions that correct errors or deficiencies, including Security Vulnerabilities, in Deliverables.
- **Esri Content** means data, images, photographs, animations, video, audio, text, maps, databases, data models, spreadsheets, user interfaces, graphics components, icons, software (whether in source code or compiled format), other code, description languages, firmware, software, tools, designs, schematics, graphical representations, embedded keys, certificates and other information, materials, assets, documents and technology that Esri, Esri Personnel, a Customer, Customer employee, or any other person or entity, in connection with the Agreement, provides to Contractor, uploads to or stores in a Hosted Service, or to which Contractor otherwise has access, and that Contractor is accessing, using, or storing on Esri's behalf.
- **Esri System(s)** means an Esri owned or licensed information technology system, platform, application, network, or the like that Esri relies upon for its business, including those located on or accessible through Esri intranet, the Internet, or otherwise.
- **Facility** means a physical location where Contractor stores, uses or otherwise accesses Esri Content.
- **Hosted Service(s)** means any data center service, application service, IT service, or Cloud Service that Contractor hosts or manages

- **Industry Best Practices means** practices that are consistent with those recommended or required by the National Institute of Standards and Technology or International Standards Organization, or any other body or organization of similar reputation.
- **Mitigation** means any known means of lessening or avoiding the risks of a Security Vulnerability.
- **On-Premises Software** means Software that Esri or a third party contractor runs, installs or operates on Esri's or the contractor's servers or systems. For clarity, On-Premises Software is a Contractor Deliverable.
- **Personal Data** means personal data, personal information or personally identifiable information as defined in applicable privacy laws.
- **Personnel** means individuals who are employed by or are on-premises contractors of a party or a party's distributors or affiliated companies.
- **Prohibited Country** means any country: (a) that the US Government has designated as a foreign adversary under the May 15, 2019, Executive Order on Securing the Information and Communications Technology and Services Supply Chain, (b) listed in accordance with Section 1654 of the U.S. National Defense Authorization Act of 2019, or (c) identified as a "Prohibited Country" in the Agreement.
- **Security Breach** means a breach of security leading to the: loss, destruction, alteration, or accidental, unlawful, or unauthorized access, use, or storage of Esri Content.
- **Security Vulnerability means** a state in the design, coding, development, implementation, testing, operation, support, maintenance, or management of a Deliverable that allows an attack by anyone that could result in unauthorized access or exploitation, including: (a) access to, controlling or disrupting operation of a system, (b) access to, deleting, altering or extracting data or (c) changes of identity, authorizations or permissions of users or administrators. A Security Vulnerability may exist regardless of whether a Common Vulnerabilities and Exposures (CVE) ID or any scoring or official classification is assigned to it.
- **Service(s)** means work performed as described in the Agreement or in Task Order.
- **Software** means any software that Contractor provides to Esri under these Terms, whether in Source Code, compiled, or other form.
- **Source Code** means human readable programming code that developers use to develop or maintain a product or that Esri otherwise:
  (i) uses or
  (ii) provides for use in conjunction with a product or Service.
- **Task Order** means a statement of work, task order, work authorization, or other ordering document under which Contractor provides Services, Hosted Services, or Deliverables.

II. Terms Applicable to ALL Contractors

The following Sections A - D requirements apply to ALL Contractors providing ANY Services or Deliverables to Esri.

A. General

1. Contractor will comply with Esri's Vendor Code of Business Conduct, as found here: https://www.esri.com/content/dam/esrisites/en-us/media/legal/vendor-code-conduct/vendor-code-conduct.pdf#:~:text=Esri%20does%20not%20use%20forced,working%20hours%20laws%20and%20regulations. Contractor may offer proof of adherence to said Vendor Code of Business Conduct, industry

certification and/or otherwise provide information to demonstrate compliance with these Terms, upon Esri's request.

2. If Esri requests, Contractor will timely provide information on the countries where its Deliverables and the components of those Deliverables were manufactured, developed, or otherwise sourced.
3. Contractor will work with Esri's Third Party Risk Management Team to assess the presence and effectiveness of enterprise privacy and security controls by either:
   a. Providing ongoing annual security and privacy control assessments through Esri's third party risk tool at the appropriate level of fidelity, or
   b. Providing security and privacy control assessment results mutually agreed upon substantially equivalent industry standard on an annual basis.
4. Contractor will work with Esri's Third Party Risk Management Team to mitigate any issues associated with enterprise privacy and security controls indicated by the annual security and privacy control assessment.
5. Employee Background Check. Where permitted by law, Contractor agrees to perform and ensure successful completion/clearance of background checks: (i) upon hire for each Contractor employee, and (ii) for all new Contractor contract employees that are assigned to perform work at Esri's premises and/or who have access to Esri Information ("Applicable Personnel") as further described herein. This background check will, to the extent permitted by applicable law, at minimum include an investigation for, and review of (i) any state/territory and federal/national convictions, (ii) any convictions involving identity theft, access device fraud, credit card fraud, or financial crimes and (iii) any deferred adjudications with respect to any of the above (collectively "Convictions"). Contractor shall be responsible for obtaining any necessary consent for the background checks and tests from such individuals and to provide proof that Contractor has conducted same. Contractor agrees, to the extent permitted by law, to keep all such reports for a period of at least three years past the last date the individual was assigned to Esri. Upon request, Contractor shall submit a certification letter to Esri via a mutually agreeable format, certifying Contractor's compliance with the foregoing requirements.
6. Eligibility to Work. Contractor agrees to verify that (i) all Applicable Personnel are eligible to work in the United States or the country in which they are contracted to work, and (ii) that no Applicable Personnel is included in the current Office of Foreign Assets Control Specially Designated Nationals and Blocked Persons list ("OFAC List") or other similar blocked persons list of a country in which the contracted work will take place.
7. Removal of Ineligible Personnel. If Contractor discovers that any Applicable Personnel have a Conviction, evidence of illegal drug use, or are ineligible to work as noted herein, then Contractor shall, immediately upon receipt of said information, remove such Applicable Personnel from assignment on Esri premises and shall prohibit such Applicable Personnel from entering Esri's premises or facilities, or accessing Esri Information. Contractor shall notify Esri in writing within two business days of gaining such knowledge.

B. Protection of Business Contact Information

1. Esri and Contractor may access, use, and store the other's BCI in connection with Contractor's delivery of Services and Deliverables.
2. A party: (a) will not sell, rent, release, disclose, disseminate, make available, transfer, or otherwise communicate orally, in writing, or by electronic or other means the other party's BCI for any other purpose without the other party's prior written consent, and the prior written consent of affected data subjects, and (b) will delete, modify, correct, return, provide information about the use of, restrict the

use of, or take any other reasonably requested action in respect of the other's BCI, promptly on written request from the other party.

3. The parties are not entering a joint controller relationship regarding each other's BCI and no provision of the Agreement will be interpreted or construed as indicating any intent to establish a joint controller relationship.
4. The parties have implemented and will maintain technical and organizational security measures to protect the other's BCI against loss, destruction, alteration, accidental or unauthorized disclosure, or accidental or unauthorized access, use, or storage.

C. Compliance Verification

1. Contractor will maintain an auditable record demonstrating compliance with these Terms.
2. Esri, by itself or with an external auditor, may, upon 30 days prior written notice to Contractor, verify Contractor's compliance with these Terms. Verification may include accessing any Facility or Facilities for such purposes, though Esri will not access any data center where Contractor accesses, uses, or stores Esri Content unless it has a good faith reason to believe that doing so would provide relevant information. Contractor will cooperate with Esri's verification, by timely and fully responding to requests for information, whether through documents, other records, interviews of relevant Contractor Personnel, or the like.
3. Esri will not request Contractor verify its compliance with these Terms more than once in any 12-month period, unless: (a) Esri is validating Contractor's remediation of concerns resulting from a previous verification during the 12-month period or (b) a Security Breach has arisen and Esri wishes to verify compliance with obligations relevant to the breach. In either case, Esri will provide the same 30 days prior written notice as specified in Section C.2 above, but the urgency of addressing a Security Breach may necessitate Esri conducting a verification on less than 30 days prior written notice.
4. If Esri has a reasonable basis for concluding that Contractor is not compliant with any of these Terms (whether such basis arises from a verification under these Terms or otherwise), then Contractor will promptly remediate such non-compliance. Without prejudice to any remedies that Esri might have under the Agreement or these Terms, Esri may terminate the Agreement without any penalties if Contractor does not promptly remediate such non-compliance and Contractor will refund any prepayments upon such termination.

D. Security Event/Vulnerability, Response & Remediation

1. Contractor will promptly (and in no event any later than 72 hours) notify Esri after becoming aware of any Security Breach. Contractor will provide notification through Esri's ArcGIS Trust Center at https://trust.arcgis.com/en/security-concern. Contractor will provide Esri with reasonably requested information about the breach and the status of any Contractor remediation and restoration activities. By way of example, reasonably requested information may include logs demonstrating privileged, administrative, and other access to Devices, systems or applications, forensic images of Devices, systems or applications, and other similar items, to the extent relevant to the breach or Contractor's remediation and restoration activities.
2. If Esri has reason to question whether any Services or Deliverables may result in a Security Breach or Security Vulnerability, then Contractor will reasonably cooperate with Esri regarding such concern, including by timely and fully responding to requests for information, whether through documents, other records, interviews of relevant Contractor Personnel, or the like.

3. If Contractor fails to comply with any of its obligations under these Terms, and that failure causes a Security Breach, then Contractor will correct the failure in its performance and remediate the harmful effects of the Security Breach, with such performance and remediation at Esri's reasonable direction and schedule. However, if the Security Breach arises from Contractor's provision of a multi-tenant Hosted Service, and consequently impacts many Contractor customers, including Esri, then Contractor will, given the nature of the Security Breach, timely and appropriately correct the failure in its performance and remediate the harmful effects of the Security Breach, while affording due consideration to any Esri input on such corrections and remediation.
4. Esri will have the right to participate in the remediation of any Security Breach and Contractor will be responsible for its costs and expenses in correcting its performance and for the remediation costs and expenses that the parties incur with respect to any such Security Breach.
5. By way of example, remediation costs and expenses associated with a Security Breach could include those for detecting and investigating a Security Breach, determining responsibilities under applicable laws and regulations, providing breach notifications, establishing and maintaining call centers, providing credit monitoring and credit restoration services, reloading data, correcting product defects (including through Source Code or other development), retaining third-parties to assist with the foregoing or other relevant activities, and other costs and expenses that are necessary to remediate the harmful effects of the Security Breach. For clarity, remediation costs and expenses would not include Esri's loss of profits, business, value, revenue, goodwill, or anticipated savings.

III. Supplemental Terms for Specialized Use Cases

Unless otherwise noted, Contractor may be subject to more than one of the following specialized use cases, depending on the nature of the Deliverables that the Contractor provides.

A. Esri Systems Access

This Section III.A applies if Contractor employees will have access to any Esri System.

1. General Terms

a. Esri will identify how Contractor employees may access Esri Systems, including whether such employees will access Esri Systems through Esri or Contractor provided Devices.
b. Contractor employees may only access Esri Systems and may only use the Devices that Esri authorizes for that access, to provide Services. Contractor employees may not use the Devices that Esri authorizes to provide services to any other person or entity, or to access any Contractor or third-party IT systems, networks, applications, websites, email tools, collaboration tools, or the like for or in connection with the Services.
c. Upon request, Contractor will confirm, by employee name, the specific Esri Systems that its employees are authorized to access, and have accessed, over any time period that Esri identifies.
d. Contractor will notify Esri within twenty-four (24) hours after any Contractor employee with access to any Esri System is no longer: (a) employed by Contractor or (b) working on activities that require such access. Contractor will work with Esri to ensure that access for such former or current employees is immediately revoked.
e. Contractor will immediately report any actual or suspected security incidents (such as loss of an Esri or Contractor Device or unauthorized access to a Device or data, materials or other information of any kind) to Esri and cooperate with Esri in the investigation of such incidents.

f. Contractor may not permit any agent, independent contractor or subcontractor employee to access any Esri System, without Esri's prior written consent; if Esri provides that consent, then Contractor will contractually commit those persons and their employers to comply with the requirements of this Section III.A as if those persons were Contractor employees, and will be responsible to Esri for all actions and omissions to act by any such person or employer with respect to such Esri System access.
g. Contractor will direct its employees to timely install all Device software that Esri requires to facilitate access to Esri Systems in a secure manner. Neither Contractor nor its employees will interfere with the operations of that software or the security features that the software enables.
h. Esri may revoke access to Esri Systems at any time, for any Contractor employee or all Contractor employees, without prior notice to Contractor or any Contractor employee or others, if Esri believes that doing so is necessary to protect Esri.
i. Contractor will comply with the terms set forth in in Attachment 1 ("**Esri General Security Requirements for Contractors that Access Esri Systems or Esri Content or Manage IT Applications, Platforms or Infrastructure on Behalf of Esri**").

2. Esri-Provided Devices

a. Esri may provide Devices for Contractor use. In no event may Contractor, or its employees, use Esri Devices for any other Contractor customer or for any purpose other than providing Services to Esri.
b. Contractor employees may not use Esri Devices for any personal reason (e.g., Contractor employees may not store personal files such as music, videos, pictures or other like items on such Devices and cannot use the Internet from such Devices for personal reasons).
c. Contractor employees are prohibited from sharing Esri Devices, user credentials, or any access information with others.
d. Esri may monitor and remediate potential intrusion and other cyber security threats without prior notice to Contractor or any Contractor employee or others.
e. Esri retains ownership of all Esri Devices. Contractor is responsible for any loss or damage to Esri Devices while in Contractor's possession. Any alteration to Esri Devices requires Esri's written consent.
f. Esri will provide support, including inspections and maintenance, for Esri Devices, with Contractor promptly notifying Esri of the need for remedial service.
g. For software programs that Esri owns or has the right to license, Esri grants Contractor a temporary right to use, store, and make sufficient copies to support its authorized use of Esri Devices. Contractor may not transfer programs to anyone, make copies of software license information, or disassemble, decompile, reverse engineer, or otherwise translate any program unless expressly permitted by applicable law without the possibility of contractual waiver.
h. Upon completion of services, Contractor must return all Esri Devices within five business days and if Esri requests, destroy all data, materials and other information of any kind on those Devices at the same time, without retaining any copy, by following Industry Best Practices to permanently erase all such data, materials and other information. Contractor's failure to comply with any obligation in this paragraph constitutes a material breach of the Agreement and associated base agreement and any related agreement between the parties, with the understanding that an agreement is "related" if access to any Esri System facilitates Contractor's tasks or other activities under that agreement.

3. Contractor-Provided Devices

a. If Esri authorizes Contractor employees to access Esri Systems using Contractor Devices, then Contractor will install and run an operating system on those Contractor Devices that Esri approves and will upgrade to a new version of that operating system or a new operating system within a reasonable time after Esri so instructs.
b. Contractor and its employees will adhere to configuration rules that Esri sets for the Device and otherwise work with Esri to help ensure that the software functions as Esri intends. For example, Contractor will not override software website blocking or automated patching features.

B. Esri Content Access

This Section III.B applies if Contractor accesses, uses, or stores Esri Content, other than Esri's BCI. If Contractor will provide Hosted Services, Section III.C will also apply.

1. General Terms

a. Contractor employees will not copy or transfer Esri Content that is accessible through an Esri System without Esri's prior written approval.
b. Contractor may not use Esri Content in any form, aggregated or otherwise, for any purpose other than providing Services and Deliverables (by way of example, Contractor is not permitted to use or reuse Esri Content to evaluate the effectiveness of or means of improving Contractor's offerings, for research and development to create new offerings, or to generate reports regarding Contractor's offerings). Unless expressly permitted in the Agreement, Contractor is prohibited from selling or sharing Esri Content.
c. Contractor assures Esri that: (a) only those of its employees who need access to Esri Content to provide Services or Deliverables will have that access, and then only to the extent necessary to provide those Services and Deliverables; and (b) it has bound its employees to confidentiality obligations that require those employees to only use and disclose Esri Content as these Terms permit.
d. Contractor will not embed any web tracking technologies in the Deliverables or as part of the Services (such technologies include HTML5, local storage, third party tags or tokens, and web beacons) unless expressly permitted in the Agreement.
e. Contractor will not disclose Esri Content to any third party, unless authorized in advance by Esri in writing. If a government, including any regulator, demands access to Esri Content (e.g., if the U.S. government serves a national security order on Contractor to obtain Esri Content), or if a disclosure of Esri Content is otherwise required by law, Contractor will notify Esri in writing of such demand or requirement and afford Esri a reasonable opportunity to challenge any disclosure (where law prohibits notification, Contractor will take the steps that it reasonably believes are appropriate to challenge the prohibition and disclosure of Esri Content through judicial action or other means and commits to providing the minimum amount of information permissible when responding, based on a reasonable interpretation of the demand or requirement). If, regardless of all such steps, Contractor is prohibited by law from notifying Esri, upon request of Esri and in accordance with

applicable law, Contractor will provide Esri general information relative to any such request received from a government or regulatory authority during the preceding 12-month period.

f. Contractor will, at Esri's choice, either delete or return Esri Content to Esri upon termination or expiration of the Agreement, or earlier upon request from Esri. If Esri requires deletion, then Contractor will, consistent with Industry Best Practices, render the data unreadable and unable to be reassembled or reconstructed, and will certify the deletion to Esri. If Esri requires the return of Esri Content, then Contractor will do so on Esri's reasonable schedule and per Esri's reasonable written instructions.

g. Contractor will comply with the terms set forth in in Attachment 1 ("**Esri General Security Requirements for Contractors that Access Esri Systems or Esri Content or Manage IT Applications, Platforms or Infrastructure on Behalf of Esri**").

2. Personal Data

This Section III.B.2 applies if the Contractor processes Esri Personal Data.

Contractor will process Personal Data in compliance with the terms of the Data Processing Addendum between the parties, which Esri will provide if needed and, if required, is incorporated here by reference. Log files typically include Personal Data, so even if a Contractor is limited to reviewing log files from Esri systems then Personal Data requirements apply and Esri will require the Contractor to execute a Data Processing Addendum.

C. Contractor Provides Equipment, Software, Hosted Services, or Related Services

This Section III.C applies if Contractor provides equipment, Software, Hosted Services, or related Services. Specific additional terms apply if Contractor is delivering Software, is a Hosted Services provider, is providing Critical IT Deliverables or Deliverables for Customer's use or has access to Esri Source Code.

1. General Terms

a. Contractor will: (a) use Industry Best Practices to identify Security Vulnerabilities, including through continuous static and dynamic Source Code application security scanning, open source security scanning and system vulnerability scanning, and (b) comply with the requirements of these Terms to help prevent, detect and correct Security Vulnerabilities in Deliverables and in all IT applications, platforms, and infrastructure in and through which Contractor creates and provides Services and Deliverables.

b. Contractor will not provide to Esri:
   (1) covered telecommunications equipment or services under 2019 NDAA §889; or
   (2) hardware, software, or Services developed or provided by Kaspersky Lab, any entity that controls, is controlled by, or is under common control with Kaspersky Lab, or any entity of which Kaspersky Lab has a majority ownership.

2. Delivered Software Provider

This Section III.C.2 applies when Contractor is delivering software to Esri other than as part of a Hosted Services offering.

a. Contractor has implemented and will maintain throughout the term of the Agreement, in accordance with Industry Best Practices, the network, platform, system, application, Device, physical infrastructure, incident response, and Personnel-focused security policies, procedures, and controls that are necessary to protect: (a) the development, build, test and operations systems and environments that Contractor or any third-party engaged by Contractor operates, manages, uses or otherwise relies upon for or with respect to the Deliverables and (b) all Deliverable Source Code against loss, destruction, alteration, accidental or unauthorized disclosure, or accidental, unlawful, or unauthorized access, use, or storage.

3. Hosted Services Provider

This Section III.C.3 applies if Contractor operates or manages IT applications, platforms or infrastructure on behalf of Esri.

a. Contractor will comply with the requirements of this Section and by doing so protect: (a) Esri Content against loss, destruction, alteration, accidental or unauthorized disclosure, or accidental, unlawful, or unauthorized access, use, or storage. The requirements of this Section extend to all IT applications, platforms, and infrastructure that Contractor operates or manages in providing Deliverables and Services and in accessing, using, or storing Esri Content, including all development, testing, hosting, support, operations, and data center environments.
b. Contractor will comply with the terms set forth in Attachment 1 ("**Esri General Security Requirements for Contractors that Access Esri Systems or Esri Content or Manage IT Applications, Platforms or Infrastructure on Behalf of Esri**").
c. Contractor will obtain the following certifications or reports within the time frames set forth below:

Certifications / Reports	Time Frame
Contractor's Hosted Services to be utilized as part of a FedRAMP authorized offering from Esri: If the data to be processed is considered either "direct-impact" or "indirect-impact" as defined by current FedRAMP guidelines, then the Hosted Service must be FedRAMP Moderate authorized or Higher. **Else** For "low/minimal-impact" data FedRAMP authorization is still preferred, however, alternative certifications as listed below can be utilized instead.	FedRAMP authorization must be in place for Contractor's Hosted Services BEFORE any direct or indirect impact data is to be processed and such authorization must be maintained for the term of the Agreement. FedRAMP or alternative certification timeframes as specified below are applicable for "low/minimal-impact" data. Contractor will obtain the ISO 27001 certification by 120 Days after the effective date of the Agreement* or Assumption Date** and then renew the certification based on the assessment of a reputable independent auditor every 12 months thereafter (with each renewal against the then most current version of the standard)
Contractor's Hosted Services to be used for other purposes by Esri: Certification of compliance with ISO 27001, Information technology, Security techniques, Information security management systems,	Contractor will obtain the SOC 2 Type 2 report by 240 Days after the effective date of the Agreement* or Assumption Date** and then obtain a new report by a reputable independent auditor

Certifications / Reports	Time Frame
with such certification based on the assessment of a reputable independent auditor **Or** SOC 2 Type 2: A report by a reputable independent auditor demonstrating its review of Contractor's systems, controls and operations in accordance with a SOC 2 Type 2 (including, at a minimum, security, confidentiality, and availability)	demonstrating its review of Contractor's systems, controls and operations in accordance with a SOC 2 Type 2 (including, at a minimum, security, confidentiality, and availability) every 12 months thereafter * If, as of such effective date, Contractor provides a Hosted Service ** The date that Contractor assumes an obligation to provide a Hosted Service

(1) If Contractor requests in writing, and Esri approves in writing, Contractor may obtain a substantially equivalent certification or report to those referenced above, with the understanding that the time frames set forth in the table above would apply unchanged with respect to the substantially equivalent certification or report.

(2) Contractor will: (i) upon request, promptly provide to Esri a copy of each certification and report Contractor is obligated to obtain and (ii) promptly resolve any internal control weaknesses noted during the SOC 2 or substantially equivalent (if Esri so approves) reviews.

4. Providing Critical IT Deliverables or Deliverables for Customer Use

This Section III.C.4 applies if any of Contractor's Deliverables are Critical IT Deliverables or will be provided to a Customer as part of an Esri product or service.

a. Contractor will comply with the terms set forth in Attachment 1 ("**Esri General Security Requirements for Contractors that Access Esri Systems or Esri Content or Manage IT Applications, Platforms or Infrastructure on Behalf of Esri**").

b. Contractor will use the Common Vulnerability Scoring System (CVSS) to assess the severity level of vulnerabilities, as well as CISA's Known Exploitable Vulnerability (KEV) catalog and US Emergency Operational Directives defining emergency security vulnerabilities.

c. Mitigation Timeframes

(1) Hosted Service – If Contractor becomes aware of a Security Vulnerability in a Hosted Service, Contractor will provide Esri with an Error Correction and Mitigations in accordance with the Severity Levels and time frames defined in the table below:

Severity Level	Urgency	Timeframes (calendar days) [a]
Emergency	US EOD[b]	4 days
Critical/High	CVSS 7 – 10	30 days
Medium	CVSS 4 – 6.9	90 days
Low	CVSS 2– 3.9	180 days

(a) Timeframes are based on CVSS/FedRAMP guidelines as those guidelines are updated from time to time.

(b) EOD means Emergency Operational Directive

(2) Software/On-Premises – If Contractor becomes aware of a Security Vulnerability in a Deliverable or any such IT application, platform, or infrastructure, Contractor will provide Esri with an Error Correction and Mitigations for all supported versions and releases of the Deliverables in accordance with the Severity Levels and time frames defined in the table below:

Severity Level	Urgency	Timeframes (calendar days) [a]
Emergency	CVSS 9-10 + KEV[b]	15 days
Critical	CVSS 9 – 10	90 days
High	CVSS 7 – 8.9	180 days
Medium	CVSS 4 – 6.9	365 days
Low	CVSS 1 – 3.9	Best effort next release

(a) Timeframes are based on CVSS/FedRAMP guidelines as those guidelines are updated from time to time.
(b) KEV means Known Exploited Vulnerability

d. In any case where a Security Vulnerability does not have a readily assigned CVSS Base Score, Contractor will apply a Severity Level that is appropriate for the nature and circumstances of such vulnerability.
e. For a Security Vulnerability that has been publicly disclosed and for which Contractor has not yet provided any Error Correction or Mitigation to Esri, Contractor will implement any technically feasible additional security controls that may mitigate the risks of the vulnerability.
f. If Esri is dissatisfied with Contractor's response to any Security Vulnerability in a Deliverable or any application, platform, or infrastructure referenced above, then without prejudice to any other rights of Esri, Contractor will promptly arrange for Esri to discuss its concerns directly with a Contractor Vice President or equivalent executive that is responsible for delivery of the Error Correction.
g. Examples of Security Vulnerabilities include third-party code or end-of-service (EOS) open-source code, where these types of code no longer receive security fixes.
h. Secure Development Requirements.
Contractor will provide Esri evidence of secure supply chain practices through either:
(1) obtaining a certification or attestation of compliance with either:

(a) ISO 20243, or
(b) a substantially equivalent industry standard addressing secure development and supply chain practices that Esri has approved in writing for Contractor's use,

within 180 Days after the effective date of the Agreement and then renewing the certification or attestation every 12 months thereafter (with each renewal against the then most current version of the selected standard); or

(2) providing Esri a conformance statement attesting that their Software development processes follow Secure Software Development Framework (SSDF) practices – NIST SP-800-218 and the following security and privacy requirements based on OWASP guidelines:
(a) Input Validation and Encoding – The requirements shall specify the rules for canonicalizing, validating, and encoding each input to the application, whether from users, file systems, databases, directories, or external systems. The default rule shall be that all input is invalid

unless it matches a detailed specification of what is allowed. In addition, the requirements shall specify the action to be taken when invalid input is received. Specifically, the application shall not be susceptible to injection, overflow, tampering, or other corrupt input attacks.

(b) Authentication and Session Management – The requirements shall specify how authentication credentials and session identifiers will be protected throughout their lifecycle. Requirements for all related functions, including forgotten passwords, changing passwords, remembering passwords, logout, and multiple logins, shall be included.

(c) Access Control – The requirements shall include a detailed description of all roles (groups, privileges, authorizations) used in the application. The requirements shall also indicate all the assets and functions provided by the application. The requirements shall fully specify the exact access rights to each asset and function for each role. An access control matrix is the suggested format for these rules.

(d) Error Handling - The requirements shall detail how errors occurring during use will be handled. Some applications should provide best effort results in the event of an error, whereas others should terminate use immediately.

(e) Logging – The requirements shall specify what events are security-relevant and need to be logged, such as detected attacks, failed login attempts, and attempts to exceed authorization. The requirements shall also specify what information to log with each event, including time and date, event description, application details, and other information useful in forensic efforts.

(f) Connections to External Systems – The requirements shall specify how authentication and encryption will be handled for all external systems, such as databases, directories, and web services. All credentials required for communication with external systems shall be stored outside the code in a configuration file in encrypted form.

(g) Encryption – The requirements shall specify what data must be encrypted, how it is to be encrypted (at least AES-256 bit if not otherwise specified), and how all certificates and other credentials must be handled. The application shall use a currently NIST authorized, standard algorithm implemented in a widely used and tested encryption library (FIPS 140-2 compliant unless otherwise specified).

(h) Availability – The requirements shall specify how it will protect against denial of service attacks. All likely attacks on the application should be considered, including authentication lockout, connection exhaustion, and other resource exhaustion attacks.

(i) Secure Configuration – The requirements shall specify that the default values for all security relevant configuration options shall be secure. For audit purposes, the Software should be able to produce an easily readable report showing all the security relevant configuration details.

(j) Specific Vulnerabilities – The requirements shall include a set of specific vulnerabilities that shall not be found in the Software. If not otherwise specified, then the Software shall not include any moderate or higher risk flaws described in the current “OWASP Top Ten Most Critical Web Application Vulnerabilities.”

(k) Privacy – The requirements shall ensure that all contractor Software and services delivered as part of the Task Order meet privacy assurance as stated in the Esri Product and Services Privacy Statement Supplement.

(l) Secure Coding – Contractor shall disclose what tools are used in the Software development environment to encourage secure coding.

(m) Configuration Management - Contractor shall use a Source Code control system that authenticates and logs the team member associated with all changes to the Software baseline and all related configuration and build files.

(n) Distribution – Contractor shall use a build process that reliably builds a complete distribution from source. This process shall include a method for verifying the integrity of the Software delivered to Esri.

(o) No Malicious Code – Contractor's Software will not contain any code that does not support a Software requirement and weakens the security of the application, including computer viruses, worms, time bombs, back doors, Trojan horses, Easter eggs, and all other forms of malicious code.

(p) Third-party Evaluation – Contractor shall make reasonable efforts to ensure that third party software meets all the terms of this Addendum and is as secure as custom developed code developed under this Addendum.

i. Contractor will, upon request, promptly provide to Esri a copy of the certifications or attestation that Contractor is obligated to obtain, per Section III.C.4.g above.

j. Contractor will provide to Esri a Software Bill of Materials (SBOM) for Software delivered meeting all requirements/standards as specified by the National Telecommunications and Information Administration (NTIA), within "The Minimum Elements for a Software Bill of Materials (SBOM)" as described under EO 14028. The SBOM will disclose all third-party software used in the Software, including all libraries, frameworks, components, and other products, whether commercial, free, open-source, or closed-source.

5. Accessing Esri Source Code

This Section III.C.5 applies if Contractor has access to Esri Source Code. Contractor will comply with the requirements of this Section to protect Esri Source Code against loss, destruction, alteration, accidental or unauthorized disclosure, or accidental, unlawful, or unauthorized access, use, or storage. The requirements of this Section extend to all IT applications, platforms, and infrastructure that Contractor operates or manages in providing Deliverables and Services and in accessing, using, or storing Esri Content, including all development, testing, hosting, support, operations, and data center environments.

(a) **Systems allowed**- Source Code must only be cloned, modified, or committed from Contractor-managed or Esri-managed Devices. Home/personally-managed computers must NOT be used to work with Esri Source Code

(1) All systems connecting to Esri Source Code via VPN must utilize Esri's VPN agent and pass ongoing system security posture checks prior to logging on to the Esri network. Contractor will submit a request to Esri for approval of all Devices connecting to the Esri VPN for the contract duration. Contractor will not attempt to establish remote connections to the Esri network if there is no contractual need, if the connecting Device has not been previously approved by Esri, or the contract has ended.

(2) Source Code must NOT travel on any Device (i.e. laptop, USB stick, mobile drive) outside of Contractor's secured work locations. Examples – No Source Code on a laptop in a backpack in a car, on a bike, in checked baggage or in the airport lobby while traveling anywhere.

(b) **Daily Updates** – Any Source Code worked on must be uploaded to Esri systems at least daily.

(c) **Code Reviews** - Every change in the Source Code revision's history is agreed to by two people prior to submission – Contractor serving as uploader and Esri employee serving as reviewer (being two different persons). When GitHub is utilized for code, this requirement must be enforced through the following GitHub Repo Policy settings being enabled:

(1) Pull requests are required to commit to main/master
(2) Approvals are required to commit to main/master
(3) Dismiss stale approvals on new commits to main/master –

See the following for details on items (i) through (iii) above:

https://docs.github.com/en/repositories/configuring-branches-and-merges-in-your-repository/managing-protected-branches/about-protected-branches#require-pull-request-reviews-before-merging

(d) **Commits Signed** – GPG must be used to sign commits locally for repositories. See the following for details:

https://docs.github.com/en/authentication/managing-commit-signature-verification/about-commit-signature-verification

Vigilant mode must be utilized for at least GitHub cloud services. See the following for details:

https://docs.github.com/en/authentication/managing-commit-signature-verification/displaying-verification-statuses-for-all-of-your-commits#about-vigilant-mode

When GitHub is utilized for code, this requirement must be enforced through the following GitHub Repo Policy setting being enabled:

Require signed commits to main/master. See the following for details:

https://docs.github.com/en/repositories/configuring-branches-and-merges-in-your-repository/managing-protected-branches/about-protected-branches#require-signed-commits

(e) **Unit & Integration Testing** – Prior to committing to main, code must be checked for sanity via automated (unit) tests. Code failing unit tests must be resolved prior to committing to the main code branch. When GitHub is utilized for code, this requirement must be enforced through the following GitHub Repo Policy setting being enabled:

Require status checks to pass before merging to main/master. See the following for details:

https://docs.github.com/en/repositories/configuring-branches-and-merges-in-your-repository/managing-protected-branches/about-protected-branches#require-status-checks-before-merging

(f) **No Hardcoded Secrets** – Secrets must not be hardcoded into Source Code and should never be uploaded/committed to a code repository, such as GitHub. Secrets include passwords, API keys, SSH keys, certificates, access tokens among other similar items. Prevention of secrets on push for code repo MUST be enabled.

(g) **Encryption Modules** – No custom encryption modules/algorithms should be utilized – Esri has a standard agile crypto library for select languages available. FIPS 140-2 or FIPS 140-3 compliant modules and algorithms must be utilized unless contractually agreed as an exception requirement.

(h) **Third-party Components** – Any such components must undergo licensing and security review by Esri before being considered for incorporation into an Esri product.

(i) Alerts - Any GitHub cloud repos utilized and managed by the Contractor must enable Dependabot alerts and Dependabot Security Updates.

(j) **Multi-factor authentication** – Multifactor authentication is required for human (non-machine) access to repositories. When GitHub is utilized for code, this requirement must be enforced through the following GitHub Repo Policy setting being enabled:

Require multifactor authentication for all product repos – See the following for details:

https://docs.github.com/en/organizations/keeping-your-organization-secure/managing-two-factor-authentication-for-your-organization/requiring-two-factor-authentication-in-your-organization

(k) **Support Lifecycle** – All software utilized when working with Esri Source Code must be covered by support and NOT be in mature or deprecated support state. Code written by Contractor should never require a dependency on hardware in a mature or deprecated state to work.

(l) **Coding Training** – Secure development training must be taken at least annually by any contractor employee accessing Esri Source Code. (ex. How to avoid CVE Top 25 Most Dangerous Software Weaknesses - https://cwe.mitre.org/top25)

(m) **Location Restrictions**

(1) Contractor will not distribute or place any Esri Source Code in escrow for the benefit of any third party.

(2) Contractor will not permit any Esri Source Code to reside on servers located in a Prohibited Country without an Esri Director's prior written consent. Contractor will not permit anyone, including its Personnel, located in a Prohibited Country or visiting a Prohibited Country (for the extent of any such visit), for any reason whatsoever, to access or use any Esri Source Code, regardless of where that Esri Source Code is located globally, and Contractor will not permit any development, testing, or other work to occur in a Prohibited Country that would require such access or use.

(3) Contractor will not place or distribute Esri Source Code in any jurisdiction where law or interpretation of law requires disclosure of Source Code to any third party. If there is a change of law or interpretation of law in a jurisdiction where Esri Source Code is located that may cause Contractor to be required to disclose such Source Code to a third party, Contractor will immediately destroy or immediately remove such Esri Source Code from such jurisdiction, and will not place any additional Esri Source Code in such jurisdiction if such law or interpretation of law remains operative.

(n) **Disclosure Restrictions -** Contractor will not, directly or indirectly, take any action, including entering into any agreement, that would cause Contractor, Esri or any third-party to incur a disclosure obligation under Sections 1654 or 1655 of the U.S. National Defense Authorization Act of 2019. For clarity, except as may be expressly permitted in the Agreement or associated base agreement

between the parties, Contractor is not permitted to disclose Esri Source Code to any third-party, under any circumstance, without Esri's prior written consent.

(o) **Notices** - If Esri notifies Contractor, or a third party notifies either party that: (a) Contractor has allowed Esri Source Code to be brought into a Prohibited Country or any jurisdiction subject to Section III.C.5.m(3) above, (b) Contractor has otherwise released, accessed, or used Esri Source Code in a manner not permitted by the Agreement or associated base or other agreement between the parties or (c) Contractor has violated Section III.C.5.n above, then without limiting Esri's rights to address such non-compliance at law or in equity or under the Agreement or associated base or other agreement between the parties: (i) if such notification is to Contractor, then Contractor will promptly share the notification with Esri; and (ii) Contractor, at Esri's reasonable direction, will investigate and remediate the matter on the schedule that Esri reasonably determines (after consultation with Contractor).

Attachment 1: Esri General Security Requirements for Contractors that Have Esri Systems Access or Esri Content Access, are Hosted Services Providers, or Provide Critical IT Deliverables or Deliverables for Customer Use

1. Security Policies

a. Contractor will maintain and follow IT security policies and practices that are integral to Contractor's business, mandatory for all Contractor Personnel, and consistent with Industry Best Practices.

b. Contractor will review its IT security policies and practices at least annually and amend them as Contractor deems necessary to protect the Esri Content.

c. Contractor will provide security and privacy education to its employees annually and require all such employees to certify each year that they will comply with Contractor's confidentiality, and security policies. Contractor will provide additional policy and process training to persons with administrative access to any components of the Services, Deliverables or Esri Content, with such training specific to their role and support of the Services, Deliverables and Esri Content, and as necessary to maintain required compliance and certifications.

d. Contractor will design security and privacy measures to protect and maintain the availability of Esri Content, including through its implementation, maintenance, and compliance with policies and procedures which require security and privacy by design, secure engineering, and secure operations, for all Services and Deliverables and for all access, use, or storage of Esri Content.

2. Security Incidents

a. Contractor will maintain and follow documented incident response policies consistent with Industry Best Practices for Computer Security Incident Response Team (CSIRT) handling of general business operations, and Product Security Incident Response Team (PSIRT) handling of Software products and services provided by the contractor.

b. Contractor will investigate unauthorized access or unauthorized use of Esri Content and will define and execute an appropriate response plan.

c. Contractor will provide Esri with reasonable assistance to satisfy any legal obligations (including obligations to notify regulators or data subjects) of Esri, Esri affiliates and Customers (and their customers and affiliates) in relation to a Security Breach.

d. Contractor will not inform or notify any third party that a Security Breach directly or indirectly relates to Esri or Esri Content unless Esri approves doing so in writing or where required by law. Contractor will notify Esri in writing prior to distributing any legally required notification to any third-party, where the notification would directly or indirectly reveal Esri's identity.

e. In case of a Security Breach which arises from Contractor's breach of any obligation under these Terms:

(1) Contractor will be responsible for any costs it incurs, as well as actual costs that Esri incurs (including without limitation, attorney fees), in providing notification of the Security Breach to applicable regulators, other government and relevant industry self-regulatory agencies, the media (if required by applicable law), data subjects, Customers, and others, (2) if Esri requests, Contractor will establish and maintain at Contractor's own expense a call-center to respond to questions from data subjects about the Security Breach and its consequences, for 1 year after the date on which such data subjects were notified of the Security Breach, or as required by any applicable data protection law, whichever affords greater protection. Esri and Contractor will work together to create the

scripts and other materials to be used by call-center staff when responding to inquiries. Alternatively, on written notice to Contractor, Esri may establish and maintain its own call-center, in lieu of having Contractor establish a call-center, and Contractor will reimburse Esri the actual costs that Esri incurs in establishing and maintaining such call-center, and (3) Contractor will reimburse Esri the actual costs that Esri incurs in providing credit monitoring and credit restoration services for 1 year after the date on which individuals affected by the breach who choose to register for such services were notified of the Security Breach, or as required by any applicable data protection law, whichever affords greater protection.

3. Physical Security and Entry Control

a. Contractor will maintain appropriate physical entry controls, such as barriers, card-controlled entry points, surveillance cameras, and manned reception desks, to protect against unauthorized entry into Facilities.
b. Contractor will require authorized approval for access to Facilities and controlled areas within Facilities, including any temporary access, and will limit access by job role and business need. If Contractor grants temporary access, its authorized employee will escort any visitor while in the Facility and any controlled areas.
c. Contractor will implement physical access controls, including multi-factor access controls that are consistent with Industry Best Practices, to appropriately restrict entrance to controlled areas within Facilities, will log all entry attempts, and retain such logs for at least one year.
d. Contractor will revoke access to Facilities and controlled areas within Facilities upon (1) separation of an authorized Contractor employee or (2) the authorized Contractor employee no longer having a valid business need for access. Contractor will follow formal documented separation procedures that include prompt removal from access control lists and surrender of physical access badges.
e. Contractor will take precautions to protect all physical infrastructure used to support the Services and Deliverables and safeguard Esri Content against environmental threats, both naturally occurring and man-made, such as excessive ambient temperature, fire, flood, humidity, theft, and vandalism.

4. Access, Intervention, Transfer, and Separation Control

a. Contractor will maintain documented security architecture of networks that it manages in its operation of the Services, its provision of Deliverables and its accessing, using, or storage of Esri Content. Contractor will separately review such network architecture and employ measures to prevent unauthorized network connections to systems, applications, and network Devices, for compliance with secure segmentation, isolation, and defense in-depth standards. Contractor may not use wireless technology in its hosting and operations of any Hosted Services; otherwise, Contractor may use wireless networking technology in its delivery of Services and Deliverables and in its access, use, or storage of Esri Content, but Contractor will encrypt and require secure authentication for any such wireless networks.
b. Contractor will maintain measures that are designed to logically separate and prevent Esri Content from being exposed to or accessed by unauthorized persons. Further, Contractor will maintain appropriate isolation of its production, non-production, and other environments, and, if Esri Content is already present within or are transferred to a non-production environment (for example to reproduce an error), then Contractor will ensure that the security and privacy protections in the non-production environment are equal to those in the production environment.

c. Contractor will encrypt Esri Content in transit and at rest (unless Contractor demonstrates to Esri's reasonable satisfaction that encrypting Esri Content at rest is technically infeasible). Contractor will also encrypt all physical media, if any, such as media containing backup files. Contractor will maintain documented procedures for secure key generation, issuance, distribution, storage, rotation, revocation, recovery, backup, destruction, access, and use associated with data encryption. Contractor will ensure that the specific cryptographic methods used for such encryption align with Industry Best Practices (such as NIST SP 800-131a).
d. If Contractor requires access to Esri Content, Contractor will restrict and limit such access to the least level required to provide and support the Services and Deliverables. Contractor will require that such access, including administrative access to any underlying components (i.e., privileged access), will be individual, role based, and subject to approval and regular validation by authorized Contractor employees following separation of duty principles. Contractor will maintain measures to identify and remove redundant and dormant accounts. Contractor will also revoke accounts with privileged access within twenty-four (24) hours after the account owner's separation or the request by Esri or any authorized Contractor employee, such as the account owner's manager.
e. Consistent with Industry Best Practices, Contractor will maintain technical measures enforcing timeout of inactive sessions, lockout of accounts after multiple sequential failed login attempts, strong password or passphrase authentication, and measures requiring secure transfer and storage of such passwords and passphrases. Additionally, Contractor will utilize multi-factor authentication for all non-console based privileged access to any Esri Content.
f. Contractor will monitor use of privileged access and maintain security information and event management measures designed to: (1) identify unauthorized access and activity, (2) facilitate a timely and appropriate response to such access and activity, and (3) enable audits by Contractor, Esri (pursuant to its verification rights in these Terms and audit rights in the Agreement or associated base or other related agreement between the parties) and others of compliance with documented Contractor policy.
g. Contractor will retain logs in which it records, in compliance with Industry Best Practices, all administrative, user, or other access or activity to or with respect to systems used in providing Services or Deliverables and in accessing, using, or storing Esri Content (and will provide those logs to Esri upon request). Contractor will maintain measures designed to protect against unauthorized access, modification, and accidental or deliberate destruction of such logs.
h. Contractor will maintain computing protections for systems that it owns or manages, including end-user systems, and that it uses in providing Services or Deliverables or in accessing, using, or storing Esri Content, with such protections including: endpoint firewalls, full disk encryption, signature and non-signature based endpoint detection and response technologies to address malware and advanced persistent threats, time based screen locks, and endpoint management solutions that enforce security configuration and patching requirements. In addition, Contractor will implement technical and operational controls that ensure only known and trusted end-user systems are allowed to use Contractor networks.
i. Consistent with Industry Best Practices, Contractor will maintain protections for data center environments where Esri Content are present or processed, with such protections including intrusion detection and prevention and denial of service attack countermeasures and mitigation.

5. Service and Systems Integrity and Availability Control

a. Contractor will: (1) perform security and privacy risk assessments at least annually, (2) perform security testing and assess vulnerabilities, including automated system and application security scanning and manual ethical hacking, before production release and annually thereafter as it concerns Services and Deliverables and annually with respect to its accessing, using, or storing Esri Content, (3) enlist a qualified independent third-party to perform penetration testing consistent with Industry Best Practices at least annually, with such testing including both automated and manual testing, (4) perform automated management and routine verification of compliance with security configuration requirements for each component of the Services and Deliverables and with respect to its accessing, using, or storing of Esri Content, and (5) remediate identified vulnerabilities or noncompliance with its security configuration requirements based on associated risk, exploitability, and impact. Contractor will take reasonable steps to avoid disruption of Services when performing its tests, assessments, scans, and execution of remediation activities. Upon Esri's request, Contractor will provide Esri with a written summary of Contractor's then-most recent penetration testing activities, which report will at a minimum include the name of the offerings covered by the testing, the number of systems or applications in-scope for the testing, the dates of the testing, the methodology used in the testing, and a high-level summary of findings.

b. Contractor will maintain policies and procedures designed to manage risks associated with the application of changes to the Services or Deliverables or to the access, usage, or storage of Esri Content. Prior to implementing such a change, including to affected systems, networks, and underlying components, Contractor will document in a registered change request: (1) a description of and reason for the change, (2) implementation details and schedule, (3) a risk statement addressing impact to the Services and Deliverables, customers of the Services, or Esri Content, (4) expected outcome, (5) rollback plan, and (6) approval by authorized Contractor employees.

c. Contractor will maintain an inventory of all IT assets it uses in operating the Services, providing Deliverables and in accessing, using, or storing Esri Content. Contractor will continuously monitor and manage the health (including capacity) and availability of such IT assets, Services, Deliverables and Esri Material, including the underlying components of such assets, Services, Deliverables and Esri Content.

d. Contractor will build all systems that it uses in the development or operation of Services and Deliverables and in its access, usage, or storage of Esri Content from predefined system security images or security baselines, which satisfy Industry Best Practices, such as the Center for Internet Security (CIS) benchmarks.

e. Without limiting Contractor's obligations or Esri's rights under the Agreement or associated base agreement between the parties with respect to business continuity, Contractor will separately assess each Service and Deliverable and each IT system used in accessing, using, or storing Esri Content for business and IT continuity and disaster recovery requirements pursuant to documented risk management guidelines. Contractor will ensure that each such Service, Deliverable and IT system has, to the extent warranted by such risk assessment, separately defined, documented, maintained, and annually validated business and IT continuity and disaster recovery plans consistent with Industry Best Practices. Contractor will ensure that such plans are designed to deliver the specific recovery times that are set forth in Section 5.f below.

f. The specific recovery point objectives ("RPO") and recovery time objectives ("RTO") with respect to any Hosted Service are: 24 hours RPO and 72 hours RTO; nevertheless, Contractor will comply with

any shorter duration RPO or RTO that Esri has committed to a Customer, promptly after Esri notifies Contractor in writing of such shorter duration RPO or RTO (an email constitutes a writing). As it concerns all other Services provided by Contractor to Esri, Contractor will ensure that its business continuity and disaster recovery plans are designed to deliver RPO and RTO that enable Contractor to remain in compliance with all of its obligations to Esri under the Agreement and associated base agreement between the parties, and these Terms, including its obligations to timely provide testing, support, and maintenance.

g. Contractor will maintain measures designed to assess, test, and apply security advisory patches to the Services and Deliverables and associated systems, networks, applications, and underlying components within the scope of those Services and Deliverables, as well as the systems, networks, applications, and underlying components used to access, use, or store Esri Content. Upon determining that a security advisory patch is applicable and appropriate, Contractor will implement the patch pursuant to documented severity and risk assessment guidelines. Contractor's implementation of security advisory patches will be subject to its change management policy.
h. If Esri has a reasonable basis for believing that hardware or Software that Contractor provides to Esri may contain intrusive elements, such as spyware, malware, or malicious code, then Contractor will timely cooperate with Esri in investigating and remediating Esri's concerns.

6. **Service Provisioning** – Contractor will support industry common methods of federated authentication for any Esri user or Customer accounts, with Contractor following Industry Best Practices in authenticating such Esri user or Customer accounts (such as by Esri centrally managed multi-factor Single Sign-On, using OpenID Connect or Security Assertion Markup Language).
7. **Subcontractors** – Without limiting Contractor's obligations or Esri's rights under the Agreement or associated base agreement between the parties with respect to the retention of subcontractors, Contractor will ensure that any subcontractor performing work for Contractor has instituted governance controls to comply with the requirements and obligations that these Terms place on Contractor.
8. **Physical Media** – Contractor will securely sanitize physical media intended for reuse prior to such reuse, and will destroy physical media not intended for reuse, consistent with Industry Best Practices for media sanitization.