COALFIRE CONTROLS

Report on Environmental Systems Research Institute, Inc.'s Esri Managed Cloud Services (EMCS) Advanced System Relevant to Security, Availability, Confidentiality, and Privacy Throughout the Period May 1, 2025 to April 30, 2026

SOC 3® - SOC for Service Organizations: Trust Services Criteria for General Use Report

Disclosure Statement:

This document contains confidential and proprietary information of both Environmental Systems Research Institute, Inc. and Coalfire Controls, LLC.

© 2026 Coalfire Controls, LLC. All rights reserved.

Table of Contents

Section 1

Independent Service Auditor's Report 3

Section 2

Assertion of Environmental Systems Research Institute, Inc. Management 6

Attachment A

Environmental Systems Research Institute, Inc.'s Description of the Boundaries of Its Esri Managed Cloud Services (EMCS) Advanced System 8

Attachment B

Principal Service Commitments and System Requirements 17

Section 1
Independent Service Auditor’s Report

Independent Service Auditor's Report

To: Environmental Systems Research Institute, Inc. ("Esri")

Scope

We have examined Esri's accompanying assertion titled "Assertion of Environmental Systems Research Institute, Inc. Management" (assertion) that the controls within the Esri Managed Cloud Services (EMCS) Advanced System (system) were effective throughout the period May 1, 2025 to April 30, 2026, to provide reasonable assurance that Esri's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, confidentiality, and privacy (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022)*, in AICPA, *Trust Services Criteria*.

The description of the boundaries of the system indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Esri, to achieve Esri's service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system presents the complementary user entity controls assumed in the design of Esri's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Esri uses subservice organizations to provide data center colocation services and endpoint and server protection services. The description of the boundaries of the system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Esri, to achieve Esri's service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system presents the types of complementary subservice organization controls assumed in the design of Esri's controls. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Service Organization's Responsibilities

Esri is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Esri's service commitments and system requirements were achieved. Esri has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Esri is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is

fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.
- Assessing the risks that controls were not effective to achieve Esri's service commitments and system requirements based on the applicable trust services criteria.
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Esri's service commitments and system requirements based on the applicable trust services criteria.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within Esri's EMCS Advanced System were effective throughout the period May 1, 2025 to April 30, 2026, to provide reasonable assurance that Esri's service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls and complementary user entity controls assumed in the design of Esri's controls operated effectively throughout that period is fairly stated, in all material respects.

Coalfire Controls LLC

Louisville, Colorado
July 2, 2026

Section 2
Assertion of Environmental Systems Research Institute, Inc. Management

Assertion of Environmental Systems Research Institute, Inc. (“Esri”) Management

We are responsible for designing, implementing, operating and maintaining effective controls within the Esri Managed Cloud Services (EMCS) Advanced System (system) throughout the period May 1, 2025 to April 30, 2026, to provide reasonable assurance that Esri’s service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, confidentiality, and privacy (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022)*, in AICPA, *Trust Services Criteria*. Our description of the boundaries of the system is presented in attachment A and identifies the aspects of the system covered by our assertion.

The description of the boundaries of the system indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Esri, to achieve Esri’s service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system presents the complementary user entity controls assumed in the design of Esri’s controls.

Esri uses subservice organizations for data center colocation services and endpoint and server protection services. The description of the boundaries of the system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Esri, to achieve Esri’s service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system presents the types of complementary subservice organization controls assumed in the design of Esri’s controls. The description of the boundaries of the system does not disclose the actual controls at the subservice organizations.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period May 1, 2025 to April 30, 2026, to provide reasonable assurance that Esri’s service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls and complementary user entity controls assumed in the design of Esri’s controls operated effectively throughout that period. Esri’s objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in attachment B.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period May 1, 2025 to April 30, 2026, to provide reasonable assurance that Esri’s service commitments and system requirements were achieved based on the applicable trust services criteria.

Environmental Systems Research Institute, Inc.

Attachment A
Environmental Systems Research Institute, Inc.'s Description of the Boundaries of Its Esri Managed Cloud Services (EMCS) Advanced System

Type of Services Provided

The Environmental Systems Research Institute, Inc. (“Esri” or “the Company”) Esri Managed Cloud Services Advanced (“EMCS Advanced”) system provides a managed cloud environment for storing and publishing geospatial data content (e.g., vector maps, associated attribute data) and hosting custom applications. It can also serve as a portal for collaboration, self-service mapping, and web-based data editing workflows. This offering applies a modern web Geographic Information System (GIS) pattern with secure and reliable web services that support applications and access points. It provides the capability to host and publish content that can be consumed by GIS applications, such as ArcGIS Online, ArcGIS Pro clients, and other GIS web and mobile applications.

There are three common patterns that a customer may choose to deploy within the EMCS Advanced environment:

1. **Content:** The Content deployment pattern provides a managed cloud environment for storing and publishing geospatial data content, such as vector maps and associated attribute data. It provides the capability to host and publish content that can be consumed by GIS applications, such as ArcGIS Online, ArcGIS Pro clients, and other GIS web and mobile applications.
2. **Application:** The Application deployment pattern stores and publishes geospatial data content and provides a managed cloud environment for hosting custom applications that consume GIS content.
3. **WebGIS:** The WebGIS deployment pattern provides a managed cloud environment that includes a portal for collaboration and self-service mapping as well as storing and publishing geospatial data content. This offering applies a modern enterprise GIS solution with secure and reliable web services that support applications and access points.

EMCS Advanced infrastructure is designed and architected to meet customer-specific requirements, such as the number of users of the system and requirements for high availability.

The boundaries of the system in this section details EMCS Advanced. Any other Company services are not within the scope of this report.

The Boundaries of the System Used to Provide the Services

The boundaries of EMCS Advanced are the specific aspects of the Company’s infrastructure, software, people, procedures, and data necessary to provide its services and that directly support the services provided to customers. Any infrastructure, software, people, procedures, and data that indirectly support the services provided to customers are not included within the boundaries of EMCS Advanced.

The components that directly support the services provided to customers are described in the subsections below.

Infrastructure

EMCS Advanced consists of a scalable cloud infrastructure created to host ArcGIS-powered geospatial solutions in a secure cloud environment. EMCS Advanced enables organizations to leverage the benefits of ArcGIS in the cloud, so they can securely develop and deploy their GIS applications and data assets for access by their user community.

The EMCS Advanced information system capabilities are implemented around the following four information system layers:

1. **Application Infrastructure Layer (platform-as-a-service [PaaS] or software-as-a-service [SaaS])**: The foundational component of this layer includes ArcGIS Enterprise, which provides tools that allow for mapping and spatial reasoning, so users can explore data and share location-based insights. In addition to ArcGIS Enterprise, the file geodatabase and enterprise geodatabase are containers that hold a collection of datasets either stored as folders in a file system or in a relational database. These are the core application components that an organization uses to develop and deploy its geospatial solutions in the cloud.
2. **Customer Infrastructure Layer**: These components are provided by the customer and can include customer client applications, eAuthentication Security Assertion Markup Language (SAML) 2.0 Identity Provider (IdP), and secure domain name systems (DNSs).
3. **Security Infrastructure or Software Layer**: This layer includes the central management and administration functions of EMCS Advanced, as well as threat management, including a security information and event management (SIEM) service powered by Splunk.
4. **Cloud Infrastructure Layer (infrastructure-as-a-service [IaaS])**: This layer is provided by Amazon Web Services (AWS) and Microsoft Azure (Azure) and includes the physical infrastructure and hypervisor.

The Company utilizes AWS and Azure IaaS to provide the resources to host EMCS Advanced. The Company leverages the experience and resources of AWS and Azure to scale quickly and securely as necessary to meet current and future demand. However, the Company is responsible for designing and configuring the EMCS Advanced architecture within AWS and Azure to help ensure the availability, security, and resiliency requirements are met.

The in-scope hosted infrastructure also consists of multiple supporting tools, as shown in the table below:

Infrastructure		
Production Tool	**Business Function**	**Hosted Location**
Databases	Customer data storage	AWS, Azure
Web and application servers	System processing	AWS, Azure

Software

ArcGIS Enterprise is a key component of the Commercial Off the Shelf (COTS) Esri ArcGIS platform. It provides organizations with a complete GIS that runs on-premises or in the cloud and works with the organization's enterprise systems and policies. ArcGIS Enterprise is a full-featured mapping and analytics platform that includes a powerful GIS server plus a dedicated web-based GIS infrastructure to organize and share GIS.

ArcGIS Enterprise consists of four software components:

1. **ArcGIS Server:** Powers mapping and analysis in GIS.
2. **Portal for ArcGIS:** Enables customers to create, share, and manage maps, applications, and data with collaborators in the organization.
3. **ArcGIS Data Store:** Provides data storage for hosting and federated servers used with a customer's deployment.

4. **ArcGIS Web Adapter (optional):** Integrates ArcGIS Server and Portal for ArcGIS with a customer's existing web servers and the organization's security infrastructure.

Software consists of the programs and software that support EMCS Advanced (operating systems, middleware, and utilities). The list of software and ancillary software used to build, support, secure, maintain, and monitor EMCS Advanced include the following business functions, as shown below:

- Application monitoring
- Backup and replication, infrastructure monitoring
- SIEM, logging system
- Patch management
- Antivirus
- Program security documentation repository

People

The Company develops, manages, and secures EMCS Advanced via separate departments. The responsibilities of these departments are defined in the following table:

People	
Group/Role Name	**Function**
System Owner	System Owner is responsible for defining the business value and mission of the system, its users and functionality. They work with the EMCS Information System Security Officer (ISSO) and other EMCS staff and administrators so that the EMCS Advanced and Advanced Plus systems are compliant with the controls, policies and procedures required to meet FedRAMP Moderate and AICPA Trust Services Criteria compliance. The System Owner also works with Esri executive management to define business objectives and external communication of the value and mission of the EMCS Advanced and Advanced Plus programs. The System Owner is responsible for obtaining justification for system changes driven by business needs.
Information System Security Officer (ISSO)	Responsible for maintaining the appropriate operational security posture for EMCS Advanced, establishing risk mitigation strategies, and ensuring compliance.
Program Manager	Coordinates with teams across the organization to achieve program-level objectives; oversees contracts with third-party vendors; defines EMCS Advanced product capabilities; and works with technical, change, and security teams.
Change Manager	Responsible for the change process is being followed and properly implemented for all production changes to EMCS Advanced systems. Coordinates with the Esri Change Advisory Board (CAB) to submit, review, and approve change requests.
Delivery Manager	Responsible for the onboarding and ongoing operations of customers in EMCS Advanced and coordinating changes to customer systems including overseeing scope, schedule, and budget. Also responsible for communication and facilitation with the customer.

People	
Group/Role Name	**Function**
Application Administrators	Deploys customer applications and data onto the EMCS Advanced systems. Performs maintenance, Esri COTS upgrades, remediation, and functional validation of systems.
Security Administrators	Implements security on customer systems running within EMCS Advanced. Performs scans, applies patches, and advises application and infrastructure administrators when vulnerabilities are detected.
Infrastructure Administrators	Provisions cloud infrastructure and services offered by EMCS Advanced cloud service providers (AWS and Azure).
Solution Advisors	Provides ad-hoc consulting support (technical, business, security, compliance).
Personnel Screening Manager	Screens individuals prior to authorizing access to the information system, verifies individuals sign appropriate access agreements, and establishes sanctions for personnel failing to comply with established security policy and procedures.
Consultant	Provides ad-hoc consulting support (technical, business, security, compliance) determining who may view limited customer information via screen share and discusses customer solutions in confidential settings with other members of the EMCS Advanced program
Training Coordinator	Assigns training to all EMCS Advanced personnel and maintains and tracks training records for EMCS Advanced personnel.
Security Services	Individuals with limited access to EMCS systems and tools that have security monitoring and operations subject matter expertise and responsibilities.

Procedures

Procedures include the automated and manual procedures involved in the operation of EMCS Advanced. Procedures are developed and documented by the respective teams for a variety of processes, including those relating to product management, engineering, technical operations, security, information technology (IT), and human resources. These procedures are drafted in alignment with the overall information security policies and are updated and approved as necessary for changes in the business, but no less than annually.

The following table details the procedures as they relate to the operation of EMCS Advanced:

Procedures	
Procedure	**Description**
Policy Management and Communication	Policies are maintained by EMCS Advanced staff and communicated via annual training. The information security policies are hosted on an internal site available to all EMCS Advanced staff.
Operations Security	Esri has established procedures on the proper management of IT production, including change management, capacity management, malware, backup, logging, monitoring, installation, and vulnerabilities.

Procedures	
Procedure	**Description**
Network Operations	Communications security is governed by procedures that define controls related to network security, segregation, network services, transfer of information, and messaging.
Enterprise Change Management	Changes to the architecture and the configuration of servers are managed by EMCS Advanced administrators and overseen by the EMCS Advanced Change Manager, EMCS Advanced Application Administrators, and EMCS Advanced ISSO.
Incident and Problem Management	Esri has established incident management procedures, including reporting events and weaknesses, defining responsibilities, response procedures, and collection of evidence.
Backup and Storage	Backups are routinely carried out to help ensure that the EMCS Advanced system can be recovered from unforeseen events, system failure, and accidental or deliberate loss of information or facilities.
Systems Development	The EMCS Advanced security team manages the information systems by following the guidance provided in the 6 Pillars of the AWS Well-Architected Framework: operational excellence, security, reliability, performance efficiency, cost optimization, and sustainability. This framework is used when developing tools and procedures that are implemented to optimize EMCS Advanced systems and customer deployments. A systems development life cycle (SDLC) is in place for Esri COTS software deployed within the environment. The SDLC is a process followed for software projects that consists of a detailed plan describing how to develop, maintain, replace, and enhance software.

Data

Data refers to transaction streams, files, data stores, tables, and output used or processed by the Company. Through the application programming interface (API), the customer or end user defines and controls the data they load into and store in the EMCS Advanced production network. Once stored in the environment, the data is accessed remotely from customer systems via the Internet.

Esri supports EMCS Advanced customers with the management, security, and availability of their geospatial content. Acceptable data formats are those compatible with Esri COTS software. EMCS Advanced customers are expected to evaluate the EMCS Advanced security controls and determine whether the system has adequate security in place to meet their specific data classification and information system security needs.

Customer data is managed, processed, and stored in accordance with relevant data protection and other regulations and with specific requirements formally established in client contracts.

The Company has deployed secure methods and protocols for transmission of confidential or sensitive information over public networks. Encryption is enabled for databases housing sensitive customer data.

The following table details the types of data contained in the production application for EMCS Advanced:

Data	
Production Application	**Description**
EMCS Advanced Customer Data	EMCS Advanced stores customer data in cloud storage.
EMCS Advanced System Data	EMCS Advanced system data is stored in the SIEM.

Complementary User Entity Controls (CUECs)

The Company's controls related to EMCS Advanced cover only a portion of overall internal control for each user entity of EMCS Advanced. It is not feasible for the service commitments, system requirements, and applicable criteria related to the system to be achieved solely by the Company. Therefore, each user entity's internal control should be evaluated in conjunction with the Company's controls, taking into account the related CUECs identified for the specific criterion. In order for user entities to rely on the controls reported herein, each user entity must evaluate its own internal control to determine whether the identified CUECs have been implemented and are operating effectively.

The CUECs presented should not be regarded as a comprehensive list of all controls that should be employed by user entities. Management of user entities is responsible for the following:

Criteria	Complementary User Entity Controls
CC2.1 C1.1	• User entities identify categorization of their datasets – The organization identifies categorization of its datasets to be utilized within EMCS Advanced and provides dataset categorization information to the EMCS Advanced security team. • User entities identify dependencies – The organization specifies third-party dependencies for monitoring and interconnection security agreements. If the organization requires incorporating other services that are critical for the usage of its EMCS Advanced application components, each dependency should be listed and provided to the EMCS Advanced security team. This includes base maps from other service providers such as ArcGIS Online, analytics tools such as Google Analytics, and external font services.

CC2.3	• It is the responsibility of the user entity to have policies and procedures to:
	  – Inform their employees and users that their information or data is being used and stored by the Company.
	  – Determine how to file inquiries, complaints, and disputes to be passed on to the Company.

CC6.1	• SAML – User entities provide and manage SAML IdP infrastructure and associated accounts utilizing two-factor authentication. The user entities are to confirm with the EMCS Advanced security team if the organization wants to utilize only SAML 2.0 accounts. • Upload Tools – User entities should use approved software to upload datasets and restrict access to the account to roles authorized to upload the organization's data. • User Access Levels – User entities restrict access to EMCS Advanced to appropriate personnel. The default EMCS Advanced application permission is user-level only (or none if the application requires no login). Other levels of access available include publisher and administrator, which would need to be discussed with the EMCS Advanced security team as they present increasing levels of risk and responsibilities for the user entity.

Criteria	Complementary User Entity Controls
CC6.2 CC6.3	• User Provisioning – User entities have processes and procedures for provisioning and managing user and administrator access for their respective applications.
CC6.4 CC6.5 CC7.2 A1.2	• User entities deploy physical security and environmental controls for all devices and access points residing at their operational facilities, including remote employees or at-home agents for which the user entity allows connectivity.
CC6.7	• Certificates – The user entities may be responsible for providing Transport Layer Security (TLS) certificates to be deployed to web application firewall Federal Information Processing Standard (FIPS) endpoints. User entities should confirm with the EMCS Advanced security team if they would like to provide certificates from their organization or if they would like the Company to provide certificates for their site. • DNS Selection – User entities are responsible for confirming with the EMCS Advanced security team if they would like to utilize their own DNS Secure (DNSSEC) server or other EMCS Advanced-managed DNS servers for their public sites. • Fully Qualified Domain Name (FQDN) Selection – User entities are responsible for defining DNS FQDNs for desired endpoints and providing them to the EMCS Advanced security team. • Certificate Authority – User entities are responsible for choosing a certificate authority (related to DNS namespace) that is either Esri-provided or customer-provided and for informing the EMCS Advanced security team of the choice. • Cross-Domain Whitelist – It is recommended that the user entities provide a whitelist of approved URLs and domains that they would like to allow for incorporation with their application (common for geospatial mashups). By default, Silverlight and Adobe cross-domain access is not allowed, and JavaScript Cross-Origin Resource Sharing (CORS) access is limited by the whitelist provided by the customer to the EMCS Advanced security team. • IP Address Restrictions – If the user entities application is not meant for public consumption, user entities are responsible for providing a list of the required IP address ranges that are approved for accessing the application to the EMCS Advanced technical team. • Token Lifetime – If the user entities application requires authentication and is utilizing the ArcGIS token service, the customer is responsible for specifying the lifetime of the token for users. The default time for EMCS Advanced is 15 minutes; however, this can be disruptive for the user experience. User entities are responsible for providing their recommended token lifetime to the EMCS Advanced security team.
P2.1 P3.1 P3.2	• User entities are responsible for managing the methods of collecting personal information of their data subjects, including ensuring that the methods of collection of personal information is collected fairly, without intimidation or deception, and lawfully • User entities are responsible for informing data subjects if the user entity develops or acquires additional information about them for its use. • User entities are responsible for ensuring that third parties from whom personal information is collected from are reliable sources and collected the information fairly and lawfully.
P4.3	• User entities have controls in place to identify personal information that needs to be purged or removed while an active customer.
P6.1	• User entities have policies and procedures in place to notify data subjects of disclosures of personal information to third parties and obtain these disclosures from Esri.
P5.2 P6.7 P7.1	• User entities are responsible for the management and handling of data subject inquiries and disclosures, as well as the completeness and accuracy of the data subjects' personal data, including correcting, appending, and amending personal data where applicable.

Subservice Organizations and Complementary Subservice Organization Controls (CSOCs)

The Company uses AWS and Azure as subservice organizations for data center colocation services. The Company also uses ESRI Corporate for endpoint and server protection services. The Company's controls related to EMCS Advanced cover only a portion of the overall internal control for each user entity of EMCS Advanced.

Although the subservice organizations have been carved out for the purposes of this report, certain service commitments, system requirements, and applicable criteria are intended to be met by controls at the subservice organizations. CSOCs are expected to be in place at AWS and Azure related to physical security and environmental protection, as well as backup, recovery, and redundancy controls related to availability. AWS and Azure's physical security controls should mitigate the risk of unauthorized access to the hosting facilities. AWS and Azure's environmental protection controls should mitigate the risk of fires, power loss, climate, and temperature variabilities. ESRI Corporate's media protection controls should mitigate the risk of unauthorized access to customer data through endpoints and decommissioned servers.

Company management receives and reviews the AWS, Azure, and ESRI Corporate SOC 2 reports annually. In addition, through its operational activities, Company management monitors the services performed by AWS, Azure, and ESRI Corporate to determine whether operations and controls expected to be implemented are functioning effectively. Management also communicates with the subservice organizations to monitor compliance with the service agreement, stay informed of changes planned at the hosting facility, and relay any issues or concerns to AWS, Azure, and ESRI Corporate management.

It is not feasible for the service commitments, system requirements, and applicable criteria related to EMCS Advanced to be achieved solely by the Company. Therefore, each user entity's internal control must be evaluated in conjunction with the Company's controls, taking into account the related CSOCs expected to be implemented at AWS, Azure, and ESRI Corporate as described below.

Criteria	Complementary Subservice Organization Controls
CC6.1 C1.1	• AWS and Azure are responsible for encrypting databases in their control.
CC6.4	• AWS and Azure are responsible for restricting data center access to authorized personnel. • AWS and Azure are responsible for the 24/7 monitoring of data centers by closed circuit cameras and security personnel.
CC6.5 C1.2	• AWS and Azure are responsible for securely decommissioning and physically destroying production assets in their control.
CC6.7	• ESRI Corporate is responsible for managing mobile devices and encrypting portable and removable media devices.
CC7.2 A1.2	• AWS and Azure are responsible for the installation of fire suppression and detection and environmental monitoring systems at the data centers. • AWS and Azure are responsible for protecting data centers against a disruption in power supply to the processing environment by an uninterruptible power supply (UPS). • AWS and Azure are responsible for overseeing the regular maintenance of environmental protections at data centers.

Attachment B
Principal Service Commitments and System Requirements

Principal Service Commitments and System Requirements

Commitments are declarations made by management to customers regarding the performance of EMCS Advanced. Commitments are communicated in master service agreements (MSAs) and privacy statements/policies.

System requirements are specifications regarding how EMCS Advanced should function to meet the Company's principal commitments to user entities. System requirements are specified in the Company's policies and procedures.

The Company's principal service commitments and system requirements related to EMCS Advanced include the following:

Trust Services Category	Service Commitments	System Requirements
Security	• Esri will implement, use, and maintain reasonable administrative, technical, and physical safeguards to protect data and guard against accidental loss, destruction, alteration, or unauthorized access.	• Employee provisioning and deprovisioning standards • Logical access controls, such as user IDs and passwords to access systems • Protection of data in transit • Risk assessment and risk mitigation standards • Threat prevention • Infrastructure security
Availability	• Esri will use commercially reasonable efforts to make the covered services available.	• System backups • System monitoring
Confidentiality	• Esri will treat customer data as confidential in accordance with terms of customer orders for products and services. • Esri will not access, use, or disclose customer data without written permission except as necessary to provide the services to the customer.	• Data classification • Data handling standards • Internal confidentiality standards • Information sharing standards
Privacy	• Esri will, at the customer's request, delete or return all customer personal data to the customer and delete all existing copies unless required by applicable law to retain customer personal data. • Esri will protect and respect customer privacy during the customer's relationship with Esri. • Esri will ensure that all personnel who have access to and/or process customer personal data are required to keep the customer personal data confidential.	• Privacy statement • Sensitive data handling procedures • System security plan