Report on Environmental Systems Research Institute, Inc.'s Esri Managed Cloud Services (EMCS) Advanced System Relevant to Security, Availability, and Confidentiality Throughout the Period January 1, 2023 to December 31, 2023

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

Table of Contents

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 January 1, 2023 to December 31, 2023, to provide reasonable assurance that Esri's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (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)* (2017 TSC).

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. 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 service 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 the EMCS Advanced System were effective throughout the period January 1, 2023 to December 31, 2023, 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

Greenwood Village, Colorado
February 6, 2024

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 January 1, 2023 to December 31, 2023, to provide reasonable assurance that Esri's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (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)* (2017 TSC). 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. 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 January 1, 2023 to December 31, 2023, 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 January 1, 2023 to December 31, 2023, 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”) Managed Cloud Services (EMCS) Advanced system (“EMCS Advanced”) 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 Desktop 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 Desktop 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 report 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.

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:** 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).

People

The Company develops, manages, and secures EMCS Advanced via separate departments. Functional roles are established for individuals and teams supporting EMCS Advanced. Access is restricted based on the defined role of the individual.

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 HR. 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.

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.

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 user entity 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 user entity specifies third-party dependencies for monitoring and interconnection security agreements. If the user entity 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 like ArcGIS Online, analytics tools like Google Analytics, and external font services.

Criteria	Complementary User Entity Controls
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 identity provider infrastructure and associated accounts utilizing two-factor authentication. The customer is 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 customer.
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 – User entities may be responsible for providing TLS certificates to be deployed to web application firewall Federal Information Processing Standard (FIPS) 140-2 endpoints. Customers 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 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 customer 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 customer application requires authentication and is utilizing the ArcGIS token service, user entities are responsible for specifying the lifetime of the token for users. The default time for EMCS is 15 minutes; however, this can be disruptive for user experience. User entities are responsible for providing their recommended token lifetime to the EMCS Advanced security team.

Subservice Organizations and Complementary Subservice Organization Controls (CSOCs)

The Company uses AWS and Microsoft Azure as subservice organizations for data center colocation 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.

Company management receives and reviews the AWS and Azure SOC 2 reports annually. In addition, through its operational activities, Company management monitors the services performed by AWS and Azure 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 and Azure 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 and Azure as described below.

Criteria	Complementary Subservice Organization Controls
CC6.1	• AWS and Azure encrypt databases in their control.
CC6.4	• AWS and Azure restrict data center access to authorized personnel. • AWS and Azure monitor data centers 24/7 by closed circuit cameras and security personnel.
CC6.5 CC6.7	• AWS and Azure securely decommission and physically destroy production assets in their control.
CC7.2 A1.2	• AWS and Azure install fire suppression and detection and environmental monitoring systems at their data centers. • AWS and Azure protect data centers against a disruption in power supply to the processing environment by an uninterruptible power supply (UPS). • AWS and Azure oversee the regular maintenance of environmental protections at their 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.

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