

ACCESS CIG, LLC

SOC 3 REPORT

FOR THE

ACCESS CLASSIC AND ACCESS UNIFY SYSTEMS

FOR THE PERIOD OF JUNE 1, 2025, TO JULY 31, 2026

Attestation and Compliance Services



Proprietary & Confidential
Reproduction or distribution in whole or in part without prior written consent is strictly prohibited.

INDEPENDENT SERVICE AUDITOR'S REPORT

To Access CIG, LLC:

Scope

We have examined Access CIG, LLC's ("Access") accompanying assertion titled "Assertion of Access CIG, LLC Service Organization Management" ("assertion") that the controls within Access's Access Classic and Access Unify systems ("system") were effective throughout the period June 1, 2025, to July 31, 2026, to provide reasonable assurance that Access's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, and confidentiality (applicable trust services criteria) set forth in TSP section 100, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).*

Access uses various subservice organizations for data center hosting, cloud hosting, and monitoring 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 Access, to achieve Access's service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system does not disclose the actual controls at the subservice organizations. 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

Access 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 Access's service commitments and system requirements were achieved. Access has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Access 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 whether 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 (AICPA) and in accordance with International Standard on Assurance Engagements 3000 (Revised), Assurance Engagements Other Than Audits or Reviews of Historical Financial Information, issued by the International Auditing and Assurance Standards Board (IAASB). 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.

Our examination included the following:

- 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 Access's service commitments and system requirements based on the applicable trust services criteria; and
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Access'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.

Service Auditor's Independence and Quality Management

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the examination engagement, including the Code of Professional Conduct established by the AICPA and the International Ethics Standards Board for Accountants' Code of Ethics for Professional Accountants.

We applied the Statement on Quality Management Standards established by the AICPA and the International Standard on Quality Management established by the IAASB and, accordingly, maintain a comprehensive system of quality management including documented policies and procedures regarding compliance with ethical requirements, professional standards, and applicable legal and regulatory requirements.

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 Access's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, 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 Access's Access Classic and Access Unify systems were effective throughout the period June 1, 2025, through July 31, 2026, to provide reasonable assurance that Access's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Schellman & Company, LLC

Columbus, Ohio
October 20, 2026

ASSERTION OF ACCESS SERVICE ORGANIZATION MANAGEMENT

We are responsible for designing, implementing, operating, and maintaining effective controls within the Access Classic and Access Unify systems ("system") throughout the period June 1, 2025, to July 31, 2026, to provide reasonable assurance that Access's service commitments and system requirements relevant to security, availability, processing integrity, and confidentiality were achieved. Our description of the boundaries of the system is presented below and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period June 1, 2025, to July 31, 2026, to provide reasonable assurance that Access's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, and confidentiality (applicable trust services criteria) set forth in TSP section 100, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*. Access'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 below.

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 June 1, 2025, to July 31, 2026, to provide reasonable assurance that Access's service commitments and system requirements were achieved based on the applicable trust services criteria.

DESCRIPTION OF THE BOUNDARIES OF THE ACCESS CLASSIC AND ACCESS UNIFY SYSTEMS

Company Background

Access provides records and information management solutions to organizations across a broad range of industries. Access provides services and technology supporting the management of physical and digital information throughout the information lifecycle, including records storage and retrieval, digitization, information governance, data archiving, retention and disposition management, and secure destruction.

Access combines physical records management services with technology-enabled information management solutions through its Access Classic and Access Unify product families. These capabilities enable customers to securely store, access, digitize, manage, govern, retain, and dispose of information in accordance with their business, contractual, legal, and regulatory requirements.

Description of Services Provided

The services and supporting technologies within the scope of the consolidated system include physical records management and related digitization services, digital records management, information governance and retention management, healthcare data archiving, and energy information management. These services are delivered through the Access Classic and Access Unify product families and their applicable supporting environments.

Access Classic represents Access' traditional records and information management services. The in-scope Access Classic services include Access Classic | Storage, Access Classic | Scan, Access Classic | Shred, Access Classic | Media Vault, and Access Classic | Services Portal, together with the applicable facilities, technology, operational processes, personnel, and information used to provide those services.

Access Unify represents Access' advanced managed services and technology solutions. The in-scope Access Unify services include Access Unify | Records, Access Unify | Lifecycle, Access Unify | Health, Access Unify | Energy, and Access Unify | Services Portal, together with the applicable technology, operational processes, personnel, and information used to provide those services.

Access Classic | Services Portal

Access Classic | Services Portal provides customer-facing access to Access' physical records and information management services. The service is supported by commercially licensed records management applications used to manage customer inventory, work orders, record location, chain of custody, and related records management activities. Separate implementations support the United States and Canadian operating environments.

The United States implementation utilizes the Total Recall records management application provided by DHS Worldwide. Total Recall is a commercial off-the-shelf (COTS) application used by Access to manage and track customer records and related service requests within Access facilities.

The Canadian implementation utilizes the Envision records management application provided by DHS Worldwide. Envision is a COTS application used by Access to manage and track customer records and related service requests within Access facilities.

Access provides physical records storage, retrieval, delivery, digitization, media vault, and secure destruction services through its applicable facilities. Physical records and media are managed and tracked throughout the service lifecycle using established operational procedures and supporting records management technologies.

Access Classic | Media Vault

Access Classic | Media Vault provides secure physical storage for customer media. Media is maintained in controlled facilities and managed in accordance with Access physical security, records management, and handling requirements.

Access Unify | Records

Access Unify | Records provides records and information management capabilities supporting the management of physical and digital customer information. The solution provides customers with capabilities to search, access, manage, and request information associated with records maintained through Access services.

Access Unify | Energy

Access Unify | Energy provides information management capabilities designed to support the organization, management, search, retrieval, and visualization of energy-related physical and digital information. The solution enables customers to manage information associated with energy assets, including wells, seismic surveys, lines, geological records, and related business information throughout the applicable asset lifecycle. Access Unify | Energy operates on the Access Unify | Records platform and utilizes the supporting application and infrastructure capabilities of that environment.

Access Unify | Lifecycle

Access Unify | Lifecycle provides information governance and retention management capabilities that enable customers to develop, maintain, communicate, and operationalize records retention schedules. The solution supports regulatory citation information, retention requirements, record series, content types, organizational and jurisdictional information, and related governance information used to support customer records and information management programs.

Access Unify | Health

Access Unify | Health provides healthcare data archiving and information management capabilities that enable healthcare organizations to retire legacy clinical, financial, and business systems while maintaining secure and controlled access to historical information. The solution supports the migration, archival, retention, search, reporting, retrieval, and authorized export of structured and unstructured information originating from legacy healthcare systems.

System Boundaries

A system is designed, implemented, and operated to achieve specific business objectives in accordance with management-specified requirements. The purpose of the system description is to delineate the boundaries of the system, which includes the services outlined above and the five components described below: infrastructure, software, people, procedures, and data.

The in-scope applications' SOC 2 criteria applicability matrix is shown in the table below:

In-Scope Service / Process	Security	Availability	Confidentiality	Processing Integrity
Access Classic Services	✓	✓	✓	✓
Access Unify | Records	✓	✓	✓	✓
Access Unify | Energy	✓	✓	✓	—
Access Unify | Health	✓	✓	✓	—
Access Unify | Lifecycle	✓	✓	—	—

Principal Service Commitments and System Requirements

Access designs its processes and procedures to meet its objectives based on the service commitments made to its customers. Security, availability, processing integrity, and confidentiality commitments to customers are documented and communicated in standardized contracts. Security, availability, processing integrity, and confidentiality commitments are standardized and include, but are not limited to, the following:

Security

Access protects systems, facilities, and customer information against unauthorized access, use, disclosure, or modification through administrative, physical, and technical safeguards appropriate to the applicable service and operating environment.

Availability

Access maintains processes, infrastructure, and operational procedures designed to support the availability of applicable services and supporting systems in accordance with established service commitments. Applicable systems and services are monitored, and business continuity and disaster recovery capabilities are maintained to support recovery following disruptive events.

Processing Integrity for the Access Classic Services and Access Unify | Records Systems

For in-scope document scanning and conversion services, Access maintains processes and controls designed to support the complete, valid, accurate, timely, and authorized processing of customer records and document images. Documented scanning and conversion procedures, record tracking, validation activities, and operational reviews are used throughout the imaging process to help ensure that customer records are processed and delivered in accordance with authorized customer work orders and applicable service requirements.

Confidentiality for the Access Classic Services, Access Unify | Records, Access Unify | Energy, and Access Unify | Health Systems

Access protects information designated as confidential or otherwise subject to applicable confidentiality requirements throughout its lifecycle. Access maintains controls governing access, use, disclosure, retention, handling, and secure disposition of confidential information and customer records. Physical and electronic customer records are retained and managed in accordance with applicable customer instructions, contractual requirements, and Access policies and procedures. Where customers authorize records for destruction, documented authorization, record tracking, validation, and destruction procedures are used to help ensure that the appropriate records are securely destroyed in accordance with the authorized customer request and applicable service requirements. Evidence of completed destruction is generated and maintained as applicable.

In accordance with our assertion, and the description criteria, the aforementioned service commitments and requirements are those principal service commitments and requirements common to the broad base of users of the system and may therefore not fully address the specific service commitments and requirements made to all system users, in each individual case.

Infrastructure and Software

Primary application and infrastructure components are summarized below. Detailed operational procedures and shared security controls are described in subsequent sections.

Access Classic | Services Portal

The Access Classic | Services United States production environment is hosted within DataBank data center facilities in the United States. Access owns and manages the applicable computing infrastructure hosted within the DataBank environment. DataBank is responsible for the underlying data center facilities and supporting physical and environmental safeguards, including applicable facility access, power, environmental protection, and connectivity services.

The United States environment is supported as follows:

- Production infrastructure is managed by authorized Access personnel with targeted assistance from designated third-party service providers.
- Total Recall operates on Windows-based infrastructure using virtualized systems.
- Application data is maintained within Microsoft structured query language (SQL) databases and protected in accordance with Access information security requirements.
- Customer-facing authentication is provided through Auth0.

- DHS Worldwide develops, maintains, and supports the Total Recall application. Access does not develop or maintain the Total Recall source code. Vendor-provided releases, patches, features, configuration changes, and other modifications affecting the Access production environment are managed through Access' established change management processes before implementation, as applicable.

The Canadian production environment is hosted using Amazon Web Services (AWS) infrastructure within Canada. Access operates the application and supporting resources within the AWS environment under the AWS shared responsibility model. AWS is responsible for the underlying cloud infrastructure and associated physical and environmental safeguards, while Access is responsible for the configuration and security of the application, customer information, identity and access controls, and other components within Access' responsibility.

The Canadian environment is supported as follows:

- Production infrastructure is managed by authorized Access personnel with targeted assistance from designated third-party service providers.
- Envision operates on Windows-based infrastructure using AWS compute services.
- Application data is maintained within Microsoft SQL databases and protected in accordance with Access information security requirements.
- Customer-facing authentication is provided through Auth0.
- DHS Worldwide develops, maintains, and supports the Envision application. Access does not develop or maintain the Envision source code. Vendor-provided releases, patches, features, configuration changes, and other modifications affecting the Access production environment are managed through Access' established change management processes before implementation, as applicable.

Access Unify | Records

The Access Unify | Records production environment is hosted using AWS cloud infrastructure, with separate production instances maintained in the United States and Canada. Access operates the applications and supporting resources within the AWS environments under the AWS shared responsibility model. AWS is responsible for the security and operation of the underlying cloud infrastructure, while Access is responsible for the configuration and security of the applications, customer information, identity and access controls, network and application configurations, and other components within Access' responsibility.

- Production infrastructure is hosted within AWS and managed by authorized Access personnel with targeted assistance from designated third-party service providers.
- Customer information and application data are maintained using applicable AWS storage and database services and are encrypted in accordance with Access information security requirements.
- Customer-facing authentication is provided through application identity and access management capabilities appropriate to the service.
- Access-developed software is governed through Access' secure software development lifecycle and change management processes. Application changes are developed, reviewed, tested, approved, and deployed through established development and release processes.

Access Unify | Energy

The Access Unify | Energy production environment is hosted using AWS cloud infrastructure, with separate production instances maintained in the United States and Canada. Access Unify | Energy operates within the Access Unify | Records platform and the applicable AWS environments under the AWS shared responsibility model. AWS is responsible for the security and operation of the underlying cloud infrastructure, while Access is responsible for the configuration and security of the application, customer information, identity and access controls, network and application configurations, and other components within Access' responsibility.

- Customer information and application data are maintained using applicable AWS storage and database services and are encrypted in accordance with Access information security requirements.
- Customer-facing authentication is provided through application identity and access management capabilities appropriate to the service.

- Access-developed software is governed through Access' secure software development lifecycle and change management processes. Application changes are developed, reviewed, tested, approved, and deployed through established development and release processes.

Access Unify | Lifecycle

The Access Unify | Lifecycle production environment is hosted using AWS cloud infrastructure. Access operates the application and supporting resources within the AWS environment under the AWS shared responsibility model. AWS is responsible for the security and operation of the underlying cloud infrastructure, while Access is responsible for the configuration and security of the application, customer information, identity and access controls, network and application configurations, and other components within Access' responsibility.

- Production infrastructure is hosted within AWS and managed by authorized Access personnel with targeted assistance from designated third-party service providers.
- Customer information and application data are maintained using applicable AWS storage and database services and are encrypted in accordance with Access information security requirements.
- Customer-facing authentication is provided through application identity and access management capabilities appropriate to the service.
- Access-developed software is governed through Access' secure software development lifecycle and change management processes. Application changes are developed, reviewed, tested, approved, and deployed through established development and release processes.

Access Unify | Health

The Access Unify | Health production environment is hosted using Microsoft Azure (Azure) cloud infrastructure. Access operates the application and supporting resources within the Azure environment under the Microsoft Azure shared responsibility model. Microsoft is responsible for the security and operation of the underlying cloud infrastructure, while Access is responsible for the configuration and security of the application, customer information, identity and access controls, network and application configurations, and other components within Access' responsibility.

- Production infrastructure is hosted within Azure and managed by authorized Access personnel with targeted assistance from designated third-party service providers.
- Customer information and application data are maintained using applicable Azure storage and database services and are encrypted in accordance with Access information security requirements.
- Customer-facing authentication is provided through application identity and access management capabilities appropriate to the service.
- Access-developed software is governed through Access' secure software development lifecycle and change management processes. Application changes are developed, reviewed, tested, approved, and deployed through established development and release processes.

Shared Security and Infrastructure Controls

Access employs common enterprise security and infrastructure controls across applicable in-scope production environments. Production environments and customer-facing applications are logically segregated from Access' internal corporate information systems through applicable network, identity, access control, and security mechanisms.

Internal Access personnel authenticate through Access' enterprise identity and access management environment, including Microsoft Entra ID / Active Directory (AD), as applicable. Administrative access to in-scope production environments is restricted to authorized personnel and protected through Access' network, identity, and privileged access controls.

Security-relevant activity from applicable infrastructure, applications, and systems is collected and monitored through Access' centralized security monitoring capabilities.

People

The personnel that contribute to the operation of the system include the following:

- Executive management – responsible for overseeing company-wide activities, establishing, and accomplishing goals, and overseeing objectives.
- Information technology (IT) department – manages, monitors, and supports user entities' information and systems from unauthorized access and use while maintaining integrity and availability.
- Accounting department – performs reconciliations related to services provided to user entities and provides financial and regulatory reporting and operational quality assurance (QA) and compliance.
- Conversion services department – responsible for the retrieving, indexing, scanning, and delivering of clients' document images.
- Customer support and service desk – responsible for responding to customer inquiries and issues.
- Client services – responsible for fulfilling client needs.
- DevOps – supports application deployment, cloud infrastructure, and production environments.
- Human resources (HR) – manages personnel lifecycle processes supporting applicable security controls.
- Information security – manages and monitors information security controls and security operations.
- Operations – performs physical records and media storage, retrieval, handling, transportation, and destruction activities.
- Software engineering – develops and maintains Access-developed applications.

Procedures

Access, Authentication, and Authorization

Documented information security policies and procedures define requirements for authentication, authorization, and secure access to Access information systems. Access is granted based on business need, job responsibilities, and the principles of least privilege and segregation of duties.

Internal Access personnel authenticate through Access' enterprise identity and access management environment, including Microsoft Entra ID / AD, as applicable. Authentication requirements are centrally managed and include established password and account security requirements. Multi-factor authentication (MFA) is required for applicable system, remote, and privileged access.

Customer users authenticate through identity and access management capabilities appropriate to the applicable service. Customer access is restricted to authorized customer accounts, information, and functionality based on assigned roles and permissions.

Administrative and privileged access to in-scope production environments, applications, infrastructure, and data is restricted to authorized personnel. A privileged access management tool is utilized to restrict privileged access and log the activities of administrator accounts within the in-scope systems. Privileged access is subject to authorization and authentication requirements, and applicable privileged access sessions are monitored and recorded. Privileged access sessions to the in-scope systems are recorded and monitored.

Access employs layered network and access security controls to restrict remote and administrative connectivity to production environments. Remote access is limited to authorized personnel and protected through Zero Trust Network Access (ZTNA) and MFA as applicable. ZTNA provides secure access to authorized resources based on established identity, device, and access requirements without exposing production environments through traditional remote-access methods.

Access maintains information protection requirements governing the transmission and storage of sensitive information. Sensitive information transmitted over external or untrusted networks is protected using approved encryption and secure transmission methods. Applicable customer information and system data are encrypted at rest in accordance with Access information security requirements.

Access Requests and Access Revocation

Access requests for employees, contractors, and third parties are formally documented by operations personnel in a request form through the ticketing system. Access requests for employees, contractors, and third parties to the Access infrastructure and application are granted based on individual job responsibilities and require approval from IT personnel. A termination checklist is completed as part of the employee termination process, which includes employees, contractors and third parties. System administrators revoke user privileges to in-scope systems upon notification from HR or operations personnel of a termination or pending termination. On a quarterly basis, security personnel perform a review of terminated employees to help ensure terminated user accounts are deleted / disabled at the AD level, and to verify that current production AD access for employees, contractors, and third parties is still appropriate. If changes are required as a result of the review, corrective action is taken, as necessary.

Physical Security for the Access Classic Records Facilities

Documented physical security policies and procedures are in place to guide personnel in facility security, employee access, visitor access, and vendor access throughout the Access facilities. Physical access to the record and destruction centers is restricted by a badge access system or physical keys. Privileged access to the badge access system is restricted to authorized personnel. Facilities personnel perform a review of physical access to the record and destruction centers on at least a quarterly basis. Changes resulting from the review follow the revocation process. A log of visitors who access the record and destruction centers is maintained by facilities personnel and logs are retained for at least one year. Facilities personnel escort visitors throughout the record and destruction centers. Closed-circuit television (CCTV) is in place throughout the record and destruction centers to monitor and record activity throughout the Access facilities. CCTV system recordings are retained for at least 90 days and available for review. In addition, alarm systems are in place within the record and destruction centers to detect unauthorized access. Inspections are performed on the security systems on a weekly and monthly basis and inspection logs are retained for at least a year.

Documented vehicle operation and security policies are in place to guide personnel to ensure that vehicle cab and storage boxes are locked when unattended and vehicles are inspected in accordance with applicable state laws and regulations.

Policies and procedures are in place to guide personnel in operations and security related to record center operations, document transportation, and document destruction. Additionally, media handling and disposal procedures are in place to guide personnel in performing data sanitization procedures to ensure data and software is unrecoverable prior to retiring the physical asset.

Environmental Security for the Access Classic Records Facilities

Access record center facilities are protected by fire detection and suppression controls that include audible and visual fire alarms, fire suppression, fire and smoke detectors, and hand-held fire extinguishers. Access contracts with third-party specialists to inspect and maintain the fire detection and suppression equipment within each record center facility on at least an annual basis to help ensure that the systems are functioning properly. Heating, ventilation, and air conditioning (HVAC) units are in place to cool the record center facilities and provide redundancy. Third-party specialists inspect and maintain the HVAC units on at least an annual basis to help ensure that the systems are functioning properly. Equipment within the Access record center facilities requiring uninterrupted power for operation is connected to backup power systems to provide temporary electricity in the event of a power outage and mitigate the risk of power surges impacting the record center facilities. Third-party specialists inspect and maintain the backup power systems within each record center facility requiring uninterrupted power for operation on at least an annual basis to help ensure that the systems are functioning properly.

Network Security

Documented information security policies, standards, and procedures are in place to govern network security and the protection of in-scope production environments. Access employs layered network security controls designed to restrict unauthorized connectivity, protect production resources, and provide segmentation between applicable systems and environments.

Remote access to applicable production environments is restricted to authorized personnel and protected through encrypted ZTNA and MFA. Access to production resources is granted based on established identity, device, and authorization requirements. The ability to modify remote access and network security configurations is restricted to authorized personnel.

Access maintains network and cloud security controls to protect applicable production environments from unauthorized external access. These controls include redundant or highly available network security capabilities, firewalls, WAFs, cloud-native security controls, and network segmentation, as applicable to the environment. Network traffic is restricted based on defined security rules, and traffic that is not explicitly authorized is denied.

Production environments are segmented from Access' internal corporate information systems and from other applicable network resources through network, cloud, identity, and access control mechanisms. Network address translation (NAT) and other network security capabilities are utilized where applicable to protect internal network addressing and restrict unauthorized connectivity.

Vulnerability scans are performed on at least a monthly basis to identify vulnerabilities within applicable systems and infrastructure. Identified vulnerabilities are evaluated, prioritized, tracked, and remediated in accordance with established vulnerability management requirements. Management and security personnel monitor identified vulnerabilities through resolution.

Applicable web applications and externally accessible services utilize Transport Layer Security (TLS) encryption to protect information transmitted over external or untrusted networks.

Antivirus

Artificial intelligence (AI) antivirus software is utilized on production servers and workstations to detect and eliminate data or files that contain viruses or malicious programs recognized by the software. It is configured to monitor for updates to definitions and update registered clients on at least a daily basis. Real time scans occur on registered clients and the software is configured to auto-terminate any known threats. Additionally, the software is configured to scan all registered files upon access or modification based on hash values. Access operations personnel are notified via e-mail of potential viral activity that requires investigation and remediation.

Change Management

Access maintains documented policies, procedures, and standards to govern changes to in-scope applications, infrastructure, systems, and configurations. Change management requirements include, as applicable, documentation of the requested change, risk and impact assessment, testing and validation, approval prior to implementation, implementation planning, rollback or recovery considerations, and post-implementation validation. Documented coding standards are in place to guide personnel in application development activities.

Changes are documented and tracked through established change management processes and are reviewed and approved by authorized personnel prior to implementation in production. Development, testing, and production activities are appropriately separated based on the nature of the system and change. Access to develop, approve, and implement changes is restricted based on assigned responsibilities and applicable segregation of duties requirements. Emergency changes are managed through established expedited change procedures and are subject to appropriate authorization and subsequent review.

Access-Developed Applications

Access-developed applications, including Access Unify | Records, Access Unify | Energy, Access Unify | Lifecycle, and Access Unify | Health, are governed through Access' secure software development lifecycle and change management processes.

Application requirements and changes are documented prior to development. Source code is maintained using controlled version management capabilities, with access restricted to authorized development personnel. Changes undergo code review and applicable automated and manual testing prior to implementation. Testing may include functional, integration, security, regression, and user acceptance testing based on the nature and risk of the change.

Application changes require appropriate review and approval prior to deployment to production. Development and testing activities are separated from production, and production deployment capabilities are restricted to authorized personnel.

Commercial Off-the-Shelf Applications

Total Recall and Envision, which support Access Classic | Services Portal, are COTS applications developed and maintained by DHS Worldwide. Access does not develop or maintain the application source code.

DHS Worldwide is responsible for developing and maintaining vendor-provided application changes. Releases, patches, features, configuration changes, and other modifications affecting the Access production environment are evaluated and managed through Access' established change management process, as applicable. Changes are tested and validated by Access prior to production implementation, as appropriate, and require authorization before deployment.

Infrastructure and Configuration Changes

Changes to infrastructure and supporting technology, including cloud resources, operating systems, databases, network components, security configurations, and other production infrastructure, are governed through Access' established change management processes.

Infrastructure and configuration changes are documented, assessed for risk and impact, tested or validated as appropriate, and approved prior to implementation. Applicable planned production changes are reviewed through the Change Advisory Board (CAB) or product team specific to each application, which meets on at least a weekly basis. Access to implement production infrastructure changes is restricted to authorized personnel. Post-implementation validation is performed as appropriate to confirm that changes were implemented successfully and did not adversely affect the production environment.

Data Backup and Disaster Recovery

Documented policies and procedures are established to define requirements for data backup, protection of backup data, replication, recovery, and disaster recovery of in-scope systems and services. Backup and recovery capabilities are implemented based on the applicable system, data, hosting environment, and recovery requirements.

Access utilizes automated backup capabilities for applicable production systems and data. Backups are performed according to defined schedules established for the applicable production environments. Backup data is protected against unauthorized access and modification, and access to backup data and recovery capabilities is restricted to authorized personnel. Backup activities are monitored to help ensure scheduled backups complete successfully.

Applicable production environments maintain replication and geographically separate recovery capabilities to support resiliency and recovery following a disruptive event. Replication activities are configured and monitored, and identified replication failures or exceptions are investigated and addressed. Access Unify | Lifecycle does not have data replication procedures in place because it does not store customer data.

Documented disaster recovery plans are maintained for the in-scope production environments and define applicable roles, responsibilities, escalation requirements, recovery procedures, system dependencies, and activities necessary to restore systems and services following a disruptive event. Disaster recovery plans and recovery capabilities are reviewed and tested on at least an annual basis. Test results are documented and evaluated, and identified issues or opportunities for improvement are tracked and addressed through established processes.

Incident Response

Documented incident management and response policies and procedures are maintained to guide personnel in identifying, reporting, escalating, investigating, and responding to security, availability, confidentiality, and processing integrity incidents.

Personnel are required to report suspected or identified incidents through established reporting and escalation processes. Reported incidents are evaluated and prioritized based on their nature, severity, and potential impact, and are assigned to appropriate personnel for investigation and response.

Incident response procedures include applicable activities for detection, analysis, containment, eradication, recovery, and post-incident review. Incidents are documented and tracked through resolution.

Access maintains defined communication and escalation processes for incidents that may affect customer information, materials, or services. Applicable internal stakeholders are engaged based on the nature and severity of the incident, and affected customers are notified in accordance with applicable contractual, legal, and regulatory requirements.

System Monitoring

Access maintains centralized monitoring capabilities to monitor the availability, performance, health, capacity, and security of applicable production systems, applications, infrastructure, and network resources.

Monitoring capabilities are configured with defined conditions, thresholds, and alerting criteria to identify service interruptions, performance degradation, resource constraints, security events, and other conditions requiring investigation. Automated alerts are generated and communicated to appropriate personnel when defined conditions or thresholds are triggered.

Alerts and identified events are evaluated, investigated, and tracked through resolution in accordance with established operational and security processes. Events requiring escalation are routed to appropriate technical, security, or management personnel based on their nature and potential impact.

Where investigation or remediation requires a change to a production system, application, infrastructure component, or configuration, the change is managed through Access' established change management processes.

Data Retention and Disposal for the Access Classic Services, Access Unify | Records, Access Unify | Energy, and Access Unify | Health Systems

Documented policies and procedures regarding physical and electronic record retention and destruction are in place to guide personnel in retention and destruction activities. Access retains and manages customer records in accordance with applicable customer instructions, contractual requirements, and established retention and destruction procedures.

The physical record destruction process begins when a customer or authorized member of the customer team places a work order requesting that a specific record or item be destroyed. Once an authorized destruction order is placed, an Access team member retrieves the applicable record or item from its storage location and places it in a designated holding location for destruction. The record or item is scanned within the records management system to update its location and maintain tracking through the destruction process.

Prior to final destruction, an Access team member compares the work order to the applicable record or item identifier to confirm that the correct customer material has been retrieved and authorized for destruction. Identified discrepancies are resolved before destruction proceeds.

Upon completion of destruction, a certified destruction work order report is generated documenting the customer, work order, service date, and applicable item identifiers for the materials destroyed.

Documented scan on demand procedures are in place to guide personnel in processing customer requests for electronic images of physical records. The procedures are reviewed by operations management on an ongoing basis and updated as necessary.

The scan on demand process begins when a customer or authorized member of the customer team places a work order requesting retrieval and scanning of records stored by Access. Once an order is placed, a pick ticket is generated containing applicable information including the work order number, parent item or container, storage location, and reference identifier of the requested file.

An Access team member retrieves the requested file from its storage location and provides the file and pick ticket to an item processor. The item processor scans the pick ticket and reviews the work order within the records management system to confirm that the retrieved file corresponds to the customer request. Once validated, the pick ticket is associated with the file, and the file is scanned to the applicable transfer location. The work order and scanning barcode accompany the file to provide additional identification and validation throughout the scanning process.

The records management application is configured to perform data entry and validation checks designed to identify errors or exceptions, including duplicate item numbers, duplicate work order numbers, and incorrect item numbers associated with a work order. Identified errors and exceptions are flagged for review and resolution.

The file is transferred to Conversion Services, where an Access team member scans the file barcode to update its location within the records management system. Prior to imaging, the work order and scanning barcode are reviewed to confirm that the correct file was received for scanning.

The file is prepared for imaging in accordance with documented procedures. Preparation activities include, as applicable, removing staples and paper clips, securing loose or damaged pages, unfolding pages, and reviewing barcodes to help ensure that the documents can be scanned completely and accurately.

Using the applicable scanning software, the Access team member scans the file to create the requested electronic images. The scanning process requires valid work order and item information before the file can be processed.

Upon completion of scanning, the Access team member reconciles the applicable work order identifier, item identifier, and facility identifier within the scanning system against the information associated with the physical file to help ensure that the requested records were scanned accurately and completely. Identified discrepancies are escalated for investigation and resolution before the work order is completed.

When no discrepancies remain, the work order is marked complete and the customer is notified through the applicable customer communication process. The physical file is then scanned to the applicable refile holding location within the records management system, indicating that the file is ready to be returned to storage within the Access facility.

Data

Access classifies and protects information in accordance with its data classification policy. Customer records and information, whether physical or electronic, are classified as highly confidential and are subject to the highest level of protection established by Access.

The following table describes the information used and supported by the system.

Data Used and Supported by the System		
Data Description	**Data Reporting**	**Classification**
Index and Reference Information	Customer record identifiers, metadata, reference fields, barcode information, and physical rack and facility location information used to manage and track customer records and media.	Highly Confidential
Scan-on-Demand Images	Customer-requested electronic images created from physical records through Access Classic | Scan services.	
Physical Customer Records and Media	Customer physical records and media maintained within applicable Access Classic | Storage and Access Classic | Media Vault facilities.	
Access Unify | Records Customer Information	Digital customer records, associated metadata, retrieval information, work orders, and related information used to support records and information management services.	
Access Unify | Energy Customer Information	Customer energy-related records, metadata, and information associated with energy assets and related information management activities.	
Access Unify | Lifecycle Information	Customer retention schedules, record series, content types, regulatory citations, retention requirements, organizational information, and related information governance data.	
Access Unify | Health Customer Information	Historical healthcare, clinical, financial, business, and related information archived and managed on behalf of customers.	
User Account and Role Information	User identity, account, role, permission, authentication, and related access management information for applicable in-scope services.	
System Configuration and Security Information	System, application, infrastructure, and security configuration information used to operate and protect the in-scope environments.	Confidential

Subservice Organizations

The data center hosting, cloud hosting, and monitoring services provided by AWS, Azure, eSentire, DataBank, DHS Worldwide, and Thrive were not included within the scope of this examination.

The following table presents the applicable Trust Services criteria that are intended to be met by controls at AWS, Azure, eSentire, DataBank, DHS Worldwide, and Thrive, alone or in combination with controls at Access, and the types of controls expected to be implemented at AWS, Azure, eSentire, DataBank, DHS Worldwide, and Thrive to achieve Access' principal service commitments and system requirements based on the applicable trust services criteria.

Ref.	Control Activities Expected to be Implemented by Subservice Organizations	Applicable Trust Services Criteria
CSOC.01	AWS and Azure are responsible for monitoring the underlying cloud infrastructure supporting applicable Access-hosted services, including provider-managed compute, network, storage, and virtualization infrastructure.	CC2.1, CC7.1, CC7.2, A1.1, A1.2
CSOC.02	eSentire is responsible for collecting data from system infrastructure components and endpoint systems to monitor system performance, potential security vulnerabilities, resource utilization and alerting the information security team upon detection of unusual system activity or service requests.	CC2.1, CC4.2, CC7.1, CC7.2, A1.1, A1.2
CSOC.03	AWS and Azure are responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Access systems reside.	CC6.1, CC6.2, CC6.3, CC6.5, CC6.6
CSOC.04	AWS, Azure, and DataBank are responsible for restricting physical access to data center facilities, offline storage and backup media, and other system components such as firewalls, routers, and servers.	CC6.4, CC6.5
CSOC.05	eSentire is responsible for providing applicable managed security capabilities supporting the monitoring and filtering of unauthorized or potentially malicious inbound network and application traffic.	CC6.6
CSOC.06	eSentire is responsible for providing applicable intrusion detection and prevention monitoring capabilities designed to identify and respond to suspicious or anomalous network activity.	
CSOC.07	AWS and Azure are responsible for implementing controls for the transmission, movement, and removal of the underlying storage devices for its cloud hosting services where Access systems reside.	CC6.7
CSOC.08	eSentire is responsible for implementing controls to prevent, detect, and respond to the introduction of unauthorized or malicious software.	CC6.8
CSOC.09	AWS and Azure are responsible for monitoring any changes to the logical access controls system for the underlying network, virtualization management, and storage devices where the Access systems reside.	CC7.1, CC7.2
CSOC.10	AWS, Azure, and DataBank are responsible for monitoring physical access to applicable data center facilities and provider-managed infrastructure supporting the in-scope services.	CC7.2
CSOC.11	AWS and Azure are responsible for monitoring logical access to provider-managed network, virtualization, storage, and supporting infrastructure for applicable hosted services.	CC7.2

Ref.	Control Activities Expected to be Implemented by Subservice Organizations	Applicable Trust Services Criteria
CSOC.12	AWS and Azure are responsible for implementing security patches and updates for infrastructure components that are managed by the applicable service provider under the applicable shared-responsibility or service model.	CC8.1
CSOC.13	DHS Worldwide is responsible for maintaining and supporting vendor-provided changes to the Total Recall and Envision commercial off-the-shelf applications.	
CSOC.14	AWS, Azure, and DataBank are responsible for ensuring the data center facilities are equipped with environmental security safeguards and utilizing an environmental monitoring application to monitor for environmental events.	A1.2
CSOC.15	Thrive is responsible for monitoring, managing, and responding to any backup and replication issues.	A1.2, PI1.5

Complementary User Entity Controls

Access' controls are designed to provide reasonable assurance that the principal service commitments and system requirements can be achieved without the implementation of complementary controls at user entities. As a result, complementary user entity controls are not required, or significant, to achieve the principal service commitments and system requirements based on the applicable trust services criteria.

Trust Services Criteria Not Applicable to the In-Scope System

All criteria within the security, availability, processing integrity, and confidentiality categories are applicable to the Access Classic and Access Unify systems. No trust services criteria within the security, availability, processing integrity, or confidentiality categories have been excluded from this examination. As reflected in the applicability matrix in the System Boundaries section, the extent to which specific trust services categories apply varies by in-scope product; processing integrity and confidentiality are not applicable to certain Access Unify products, as noted in that table.