System and Organization Controls (SOC) 1, Type II

Report on Agent Production Library, Inc.'s Description of Its Information Technology General Control System and the Suitability of the Design and Operating Effectiveness of Controls

For the Period October 1, 2023 to September 30, 2024

Table of Contents

Section I

Independent Service Auditor’s Report

MeredithCPAs

222 W. Las Colinas Blvd, Suite 1150E, Irving, Texas 75039 | 214.492.1986 fax 972.887.9996

Independent Service Auditor's Report on Agent Production Library, Inc.'s Description of Its Information Technology General Control System and the Suitability of the Design and Operating Effectiveness of Controls

To: Management of Agent Production Library, Inc.

Scope

We have examined management of Agent Production Library, Inc.'s description of its information technology general control system entitled "Management of Agent Production Library, Inc.'s Description of Its Information Technology General Control System" for agency management and commission software as a service throughout the period October 1, 2023 to September 30, 2024 (description) and the suitability of the design and operating effectiveness of the controls included in the description to achieve the related control objectives stated in the description, based on the criteria identified in "Management of Agent Production Library, Inc.'s Assertion" (assertion). The controls and control objectives included in the description are those that management of Agent Production Library, Inc. believes are likely to be relevant to user entities' internal control over financial reporting, and the description does not include those aspects of the information technology general control system for agency management and commission software as a service that are not likely to be relevant to user entities' internal control over financial reporting.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of Agent Production Library, Inc.'s controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not extend to such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Agent Production Library, Inc. uses subservice organizations for managed services, including firewall, antivirus, network monitoring, infrastructure change implementation and patching, and backup configuration and monitoring. The description includes only the control objectives and related controls of Agent Production Library, Inc. and excludes the control objectives and related controls of the subservice organizations. The description also indicates that certain control objectives specified by Agent Production Library, Inc. can be achieved only if complementary subservice organization controls assumed in the design of Agent Production Library, Inc.'s controls are suitably designed and operating effectively, along with the related controls at Agent Production Library, Inc. Our examination did not extend to controls of 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

In Section II, Agent Production Library, Inc. has provided an assertion about the fairness of the presentation of the description and suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description. Management of Agent Production Library, Inc. is responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion, providing the services covered by the description, specifying the control objectives and stating them in the description, identifying the risks that threaten the achievement of the control objectives, selecting the criteria stated in the assertion, and designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve the related control objectives stated in the description.

Service auditor's responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on our examination.

Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether, in all

material respects, based on the criteria in management's assertion, the description is fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description throughout the period October 1, 2023 to September 30, 2024. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of controls involves—

- performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on the criteria in management's assertion.
- assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the description.
- testing the operating effectiveness of those controls that management considers necessary to provide reasonable assurance that the related control objectives stated in the description were achieved.
- evaluating the overall presentation of the description, suitability of the control objectives stated in the description, and suitability of the criteria specified by the service organization in its assertion.

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

Inherent limitations

The description is prepared to meet the common needs of a broad range of user entities and their auditors who audit and report on user entities' financial statements and may not, therefore, include every aspect of the system that each individual user entity may consider important in its own particular environment. Because of their nature, controls at a service organization may not prevent, or detect and correct, all misstatements in its information technology general control system. Also, the projection to the future of any evaluation of the fairness of the presentation of the description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives, is subject to the risk that controls at a service organization may become ineffective.

Description of tests of controls

The specific controls tested and the nature, timing, and results of those tests are listed in Section IV.

Opinion

In our opinion, in all material respects, based on the criteria described in management of Agent Production Library, Inc.'s assertion—

a) the description fairly presents the information technology general control system for the agency management and commission software as a service that was designed and implemented throughout the period October 1, 2023 to September 30, 2024.

b) the controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period October 1, 2023 to September 30, 2024 and subservice organizations and user entities applied the complementary user entity controls assumed in the design of Agent Production Library, Inc.'s controls throughout the period October 1, 2023 to September 30, 2024.

c) the controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period October 1, 2023 to September 30, 2024 if complementary subservice organizations and user entity controls assumed in the design of Agent Production Library, Inc.'s controls operated effectively throughout the period October 1, 2023 to September 30, 2024.

Restricted use

This report, including the description of tests of controls and results thereof in Section IV, is intended solely for the information and use of Agent Production Library, Inc., user entities of Agent Production Library, Inc.'s information

technology general control system for the agency management and commission software as a service during some or all of the period October 1, 2023 to September 30, 2024, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities themselves, when assessing the risks of material misstatement of user entities' financial statements. This report is not intended to be, and should not be, used by anyone other than these specified parties.

MeredithCPAs

Irving, Texas
November 05, 2024

Section II

Management of Agent Production Library, Inc.’s Assertion

Management of Agent Production Library, Inc.'s Assertion

We have prepared the description of Agent Production Library, Inc.'s information technology general control system entitled "Management of Agent Production Library, Inc.'s Description of Its Information Technology General Control System", throughout the period October 1, 2023 to September 30, 2024 for the agency management and commission software as a service (description) for user entities of the system during some or all of the period October 1, 2023 to September 30, 2024, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities of the system themselves when assessing the risks of material misstatement of user entities' financial statements.

Agent Production Library, Inc. uses subservice organizations for managed services, including firewall, antivirus, network monitoring, infrastructure change implementation and patching, and backup configuration and monitoring. The description includes only the control objectives and related controls of Agent Production Library, Inc. and excludes the control objectives and related controls of the subservice organizations. The description also indicates that certain control objectives specified in the description can be achieved only if complementary subservice organization controls assumed in the design of our controls are suitably designed and operating effectively, along with the related controls. The description does not extend to controls of the subservice organizations.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of Agent Production Library, Inc.'s controls are suitably designed and operating effectively, along with related controls at the service organization. The description does not extend to controls of the user entities.

We confirm, to the best of our knowledge and belief, that:

1) The description fairly presents Agent Production Library, Inc.'s information technology general control system made available to user entities of the system during some or all of the period October 1, 2023 to September 30, 2024 as it relates to controls that are likely to be relevant to user entities' internal control over financial reporting. The criteria we used in making this assertion were that the description:

    a) Presents how the system made available to user entities of the system was designed and implemented, including, if applicable:

        i) The types of services provided.

        ii) The procedures, within both automated and manual systems, by which requests for those services are provided, including, as appropriate, procedures by which services are initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports and other information prepared for user entities of the system.

        iii) How the system captures and addresses significant events and conditions.

        iv) The process used to prepare reports and other information for user entities.

        v) The specified control objectives and controls designed to achieve those objectives including, as applicable, complementary user entity controls and complementary subservice organization controls assumed in the design of the controls.

        vi) Other aspects of our control environment, risk assessment process, information and communications, control activities, and monitoring activities that are relevant to the services provided.

        vii) The services performed by a subservice organization, if any, including whether the carve-out method or the inclusive method has been used in relation to them.

    b) Includes relevant details of changes to Agent Production Library, Inc.'s information technology general control system during the period covered by the description.

    c) Does not omit or distort information relevant to the system, while acknowledging that the description is prepared to meet the common needs of a broad range of user entities and their user auditors and may

not, therefore, include every aspect of Agent Production Library, Inc.'s information technology general control system that each individual user entity of the system and its auditor may consider important in its own particular environment.

2) The controls related to the control objectives stated in the description were suitably designed and operating effectively throughout the period October 1, 2023 to September 30, 2024 to achieve those control objectives if subservice organizations and user entities applied the complementary controls assumed in the design of Agent Production Library, Inc.'s controls through the period October 1, 2023 to September 30, 2024. The criteria we used in making this assertion were that:

   a) The risks that threaten the achievement of the control objectives stated in the description have been identified by management of the service organization.

   b) The controls identified in the description would, if operating effectively, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved.

   c) The controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

Section III

Management of Agent Production Library, Inc.'s Description of Its Information Technology General Control System

Company Overview

Company Background

Agent Production Library, Inc. (“APL” or the “Company”) is a provider of business outsourcing solutions. APL offers a wide range of commission payroll software products, tax, and office administration solutions from a single source.

The origin of the core product can be traced back to 1987 when the software was created. In 1991, the copyright of the software Agent Production Library (APL) was granted by the United States Copyright Office (TX 3 083 193). The Company was incorporated in Texas under the same name on August 2, 2001.

Products and Services Overview

APL Commission Accounting Software is a web-based commission payroll accounting software designed to accommodate the need for organizations with payroll based on a tiered commission structure, such as insurance companies and agencies. The target customers are mainly insurance companies and agencies with internal payroll staff but lack of the system to accommodate the ever- changing business environments.

eAgentCenter is a web-based office management system. This product is specifically designed for insurance agencies to manage brokers and agents. This product works independently as an office management system or it works as an integrated part of the commission accounting system. It is designed to be utilized by both the insurance agencies as a team management tool and by the brokers and agents as an office tool.

Scope of the Description

This description addresses only APL’s Information Technology General Control System for the agency management and commission software as a service system provided to user entities.

The description is intended to provide information for user entities of the Information Technology General Control System for the Agency Management and Commission Software as a Service System and their independent auditors who audit and report on such user entities’ financial statement or internal control over financial reporting, to be used in obtaining an understanding of the Information Technology General Control System for the Agency Management and Commission Software as a Service System and the controls over that system that are likely to be relevant to user entities’ internal control over financial reporting. The description of the system includes certain business process controls and IT general controls that support the delivery of APL’s Information Technology General Control System for the Agency Management and Commission Software as a Service System.

APL utilizes the subservice organization, The Strickland Group (“Strickland”) for managed services including firewall, antivirus, network monitoring, infrastructure change implementation and patching, and backup configuration and monitoring. APL also utilizes the subservice organization, Amazon Web Services System (“AWS”) that is responsible for providing a web services interface that can be used to store and retrieve data. The description includes only the control objectives and related controls of APL and excludes the control objectives and related controls of the subservice organizations.

Internal Control Framework

This section provides information about the five interrelated components of internal control at APL, including the following:

- Control environment,
- Risk assessment process,
- Monitoring activities,
- Information and communications, and
- Control activities.

Control Environment

The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. The control environment has a pervasive influence on the structure of business activities, establishment of objectives, and assessment of risks. It influences control activities, information and communication systems, and monitoring procedures. The control environment is influenced by an entity's history and managerial culture. Effectively controlled entities strive to have competent personnel, instill an enterprise-wide attitude of integrity and control consciousness, and set a positive corporate direction. These entities establish appropriate controls that foster shared values and teamwork in pursuit of the organization's objectives.

Management Controls, Philosophy, and Operating Style

Management is responsible for directing and controlling operations, establishing, communicating, and monitoring control policies and procedures, as well as setting the tone for the organization. Importance is placed on accuracy and integrity, maintaining written and updated procedures, security and privacy, and establishing and maintaining sound internal controls over all functional aspects of operations.

Management's philosophy and operating style affect the way the entity is managed, including the kinds of business risks accepted. APL places a great deal of importance on working to ensure that the integrity of processing is a primary focus and that controls are maximized to mitigate risk in daily operations. Management and specific teams are structured to ensure the highest level of integrity and efficiency in customer support.

Formal job descriptions and departmental meetings and staff interactions ensure communication of organizational values, ethics, and behavior standards. Personnel operate under APL's policies and procedures, including confidentiality agreements and security policies. Annual training is conducted to communicate regulations and the importance of privacy and security. Management is committed to being aware of regulatory and economic changes that impact lines of business and monitoring the customer base for trends, changes, and anomalies.

Integrity and Ethical Values

Maintaining a climate that demands integrity and ethical values is critical to the establishment and maintenance of an effectively controlled organization. The effectiveness of internal controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. APL has programs and policies designed to promote and ensure integrity and ethical values in their environment.

Accountability

APL desires to maintain a safe, pleasant, and cooperative working environment and expects employees to have high standards of performance, integrity, productivity, and professionalism. APL has developed professional conduct practices that set forth policies of importance to all employees, relating to ethics, values, and conduct. All employees are expected to know and adhere to these standards, as well as to generally accepted norms of conduct and courtesy at all times. While managers are responsible for understanding, communicating, and enforcing Company policies, this does not override or diminish an employee's individual responsibility to be aware of and adhere to these policies. Violations of these policies or other forms of misconduct may lead to disciplinary or corrective action up to and including dismissal.

Assignment of Authority and Responsibility

The extent to which individuals recognize that they are held accountable influences the control environment. This holds true for everyone who has ultimate responsibility for activities within an entity, including the internal control system. This includes assignment of authority and responsibility for operating activities, and establishment of reporting relationships and authorization protocols. APL's management encourages individuals and teams to use initiative in addressing issues and resolving problems.

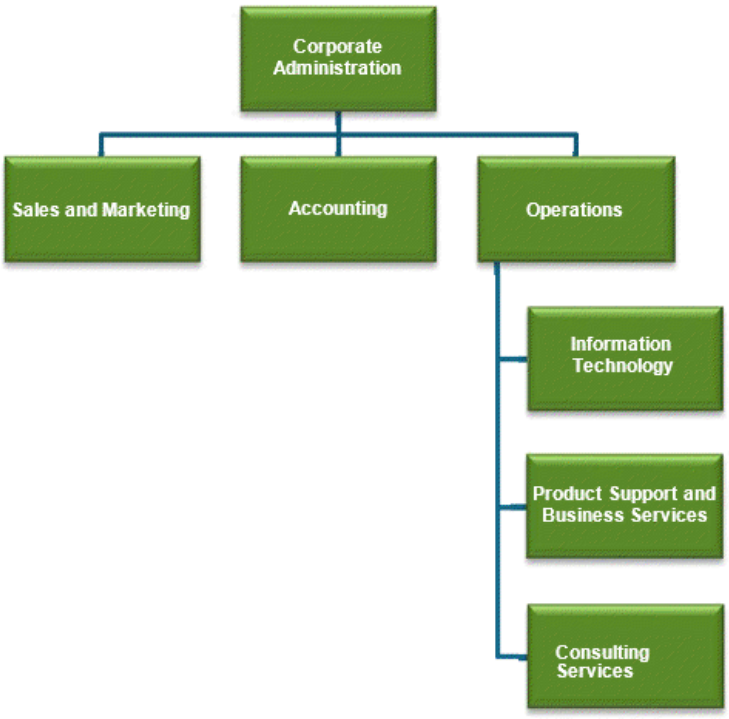
Organizational Structure and Oversight

An entity's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Significant aspects of establishing a relevant organizational structure include defining key areas of authority and responsibility and establishing appropriate lines of reporting. Significant cross training between management positions and between staff positions exists to help ensure smooth operations and maintenance of controls during staff or management absence.

APL is led by the President/Chief Executive Officer (CEO) who assigns authority and responsibility to key management personnel with the skills and experience necessary to carry out their assignments. Such assignments commonly relate to achieving corporate objectives, oversight of operating functions, and any compliance with applicable regulatory requirements. Open dialogue and individual initiative are encouraged as fundamental parts of APL's goal to deliver client service.

Roles and Responsibilities

The following organizational chart depicts the APL corporate structure.



Led by Corporate Administration, APL is organized into the following six departments: Sales and Marketing, Accounting, Operations, Information Technology, Product Support and Business Services, and Consulting Service.

Corporate Administration – Corporate Administration oversees all operations of the Company, negotiates, and engages in contracts and agreements with third parties.

Sales and Marketing – Sales and Marketing is responsible for market planning and growth strategy development and conducts all sales and marketing activities.

Accounting – Accounting is responsible for accounts receivable, accounts payable, and payroll processing.

Operations – Operations is composed of three groups: Information Technology (IT), Product Support and Business Services, and Consulting Services.

IT – This department is in charge of all technical aspects of the Company including developing new products, maintaining existing products, and hardware maintenance. IT is responsible for data backup and storage and provides all system-level support to both internal and external clients.

Product Support and Business Services – This department provides front line support to all clients. It is also the team that provides the commission accounting services.

Consulting Services – This service is fulfilled by all members of the team. APL will identify the person in the organization with the best-fit skill set to perform the job requirements.

Hiring and Termination Practices

The Human Resource (HR) department is responsible for providing a quality workforce by aiding all departments in the selection and retention of qualified employees as well as providing a safe and comfortable work environment for all company employees. HR is responsible for all personnel functions including:

- Employee benefits administration,
- Payroll auditing, reporting, and processing,
- Compliance with external and internal regulatory and policy requirements,
- All recordkeeping as it relates to HR,
- Creation and interpretation of personnel policies and procedures,
- Implementation and ongoing responsibility for employee orientation, education, and employee competency training programs,
- Maintenance of the employee performance evaluation system, and
- The recruitment process, which includes employee qualifications, testing, and selection.

Security Awareness

APL conducts security training programs for all employees. Each member of APL is made aware of the security implications that revolve around their functions and actions. Approaching security as an organization has a more profound effect than relying solely on a single group. This process begins with providing individuals with the understanding and knowledge they need to help secure them and their data within established policies. Security awareness programs include the message that individual users can have a significant impact on the overall security of an organization.

Risk Assessment

APL has a cross-functional risk assessment process that utilizes management, as well as staff, to identify risks that could affect APL's ability to meet its contractual obligations. Risk assessment efforts include analyses of threats, probabilities of occurrence, potential business impacts, and associated migration plans. Risk mitigation strategies include prevention and elimination through the implementation of internal controls and transference through commercial general and umbrella policies.

APL employs numerous methods to assess and manage risk, including policies, procedures, team structure, recurring meetings, and automated error detection controls. APL strives to identify and prevent risks at an early stage through policy and procedure adherence in addition to mitigating relevant risks as discovered through team structure, meetings, or notifications.

APL maintains security policies and communicates them to staff to ensure that all individuals utilizing Company resources understand their responsibility in reducing the risk of compromise and exercise appropriate security measures to protect systems and data.

Monitoring

APL monitors the quality of internal control performance as part of their daily activities. Monitoring is performed over a wide variety of functions at all levels of the organization and occurs through the use of both automated and manual processes. APL performs periodic assessments of the design and operation of its controls and ongoing monitoring of control effectiveness. Management performs oversight and reviews of operating performance as well as evaluates proposed modifications to controls.

APL utilizes the subservice organization, The Strickland Group ("Strickland") for managed services including firewall, anti-virus, network monitoring, infrastructure change implementation and patching, and backup configuration and monitoring. APL monitors these services primarily through activity reports.

APL also utilizes the subservice organization, Amazon Web Services System (AWS) that is responsible for providing a web services interface that can be used to store and retrieve data. AWS had a SOC 1Type II audit completed for the review period of July 1, 2023 to June 30, 2024 and has a bridge letter effective through September 1, 2024. APL monitors these services primarily through review of the annual SOC report.

Information and Communication

Information is necessary for the entity to carry out internal control responsibilities in support of achievement of its objectives. Communication occurs both internally and externally and provides the organization with the information needed to carry out day-to-day controls. Communication enables personnel to understand internal control responsibilities and their importance to the achievement of the objective.

Communication

APL uses a variety of methods for communication to ensure that significant events and issues are conveyed in a timely manner and that staff understand their role and responsibility over service and controls. These methods include the following: new hire training, ongoing training, policy and process updates, weekly departmental meetings summarizing events and changes, use of email to communicate time sensitive information, and the documentation and storage of historical data in internal repositories for business and support activities. APL maintains systems that manage the flow of information and facilitate communication with its customers.

Control Activities

APL has developed a variety of policies and procedures including related control activities to help ensure the service organization's objectives are carried out and risks are mitigated. These control activities help ensure that agency management and commission software as a service is administered in accordance with the service organization's policies and procedures.

Control activities are performed at a variety of levels throughout the organization and at various stages during the relevant business process. Controls may be preventive or detective in nature and may encompass a range of manual and automated controls, including authorizations, reconciliation, and IT controls. Duties and responsibilities, compliance, and control monitoring, are allocated among personnel to ensure that a proper segregation of duties is maintained.

A formal program is in place to review and update the service organization's policies and procedures on at least an annual basis. Any changes to the policies and procedures are reviewed and approved by management and communicated to personnel.

Information Technology General Control (ITGC) Activities

Control activities are the actions established by policies and procedures to help ensure that management directives to mitigate risks to the achievement of objectives are executed. Control activities are performed at all levels of the organization and at various stages within business processes, and over the technology environment.

ITGC include controls over computer operations, access, and systems development and maintenance. ITGC, if suitably designed and operating correctly, provide a secure and productive environment for the development and processing of applications.

APL's Operating Environment and Technical Infrastructure

At APL, security is critical to the physical network, computer operating systems and application programs. Each area offers its own set of security issues and risks. An information security policy is necessary to serve statutory goals pertaining to government organizations, healthcare organizations, and facilities. These goals include:

- Ensure continuity of operations
- Protect safety and integrity of confidential records
- Prevent unauthorized access to confidential records
- Insure proper use of communications facilities
- Assign responsibility for efficient and economical management of confidential records
- Protect corporate data

The Information Security Policy provides guidance for establishing effective security measures. The goal of the APL policy is to ensure the confidentiality of information systems, the continued availability of information systems to support critical activities, and the implementation of appropriate technologies and controls to protect information from disclosure, manipulation, modification, erasure, or copying.

Information takes many forms. It may be stored on computers, transmitted across networks, printed or written on paper, and spoken in conversations. IT systems are vital assets to all industries. These information assets are essential to the daily operation of these institutions and agencies and may impact each organization or entity that provides or relies on their services.

All employees of APL are obligated to respect and, in all cases, to protect confidential data. Customer information, employment-related records, and other intellectual property-related records are, subject to limited exceptions, confidential as a matter of law. Many other categories of records, including company and other personnel records, and records relating to APL's business and finances are, as a matter of APL policy, treated as confidential. Responsibility for guaranteeing appropriate security for data, systems, and networks is shared by the IT Department and client services personnel. IT is responsible for designing, implementing, and maintaining security protection and retains responsibility for ensuring compliance with the policy. In addition to management and the technology staff, individual users are responsible for the equipment and resources under his or her control.

Application Overview

The APL software-as-a-service solutions are internally developed applications. The applications are customizable and can be utilized to streamline the entire commission payroll accounting process.

All application-related changes are related to release upgrades and configuration changes for optimization. Procedures ensure all data is appropriately transferred when software modifications or upgrades occur.

Firewall

The Company incorporates a firewall at the perimeter of its network to protect against threats from the Internet. APL utilizes Strickland Group for firewall management. Management receives activity reports on a monthly basis to monitor the controls Strickland is responsible for.

The firewall device provides user and application policy enforcement, multi-vector attack protection, and secure connectivity services through a wide range of security and networking services in a unified threat management platform including:

- Application-aware firewall services
- Intelligent networking services
- Flexible management solutions

Administrator access to the firewall settings is restricted to authorized individuals.

Anti-Virus

APL uses an anti-virus and anti-malware protection software for production servers and workstations. The Company incorporates a centralized methodology whereby servers pull the definition updates from the vendor and pushes them to the production servers and workstations.

Administrator access to the anti-virus settings is restricted to authorized individuals.

Remote access

Remote desktop protocol is utilized to control access to the network form outside the boundaries of the system. Remote access is controlled and monitored by the President and Owner of the Company. Access is restricted to authorized individuals.

Software Development Life Cycle (SDLC)

Change requests are tracked in Issue Tracker. The Project Manager opens a ticket into Issue Tracker. Developers only work on open tickets and prioritize work according to due date. Any ticket requiring additional information from the Project Manager is changed to an updated status until resolved; then the Project Manager changes the ticket back to open. Tickets that have been completed by the developer are moved to the stage server for quality assurance testing and the ticket status is changed to stage.

Tickets are tested by the Project Manager. If there is a problem with the test, the Project Manager will change the ticket status back to open and note the problem for the developer to further review. Any tickets that pass testing are changed to a final status and are promoted to production by IT personnel. The Project Manager will verify the issue was resolved and close the issue in Issue Tracker.

Infrastructure Changes

APL has a Change Management Policy in place to control information resources that require an outage for planned upgrades, maintenance, or fine-tuning. Additionally, unplanned outages may occur that may result in upgrades, maintenance, or fine-tuning. The purpose of the Change Management Policy is to manage changes in a rational and predictable manner so that staff and clients can plan accordingly. Changes require serious forethought, careful monitoring, and follow-up evaluation to reduce negative impact to the user community and to increase the value of information resources. The APL Change Management Policy applies to all individuals that install, operate, or maintain information resources.

Patch Management

The Company takes a proactive approach to patch management. APL administrators regularly monitor various websites, message boards, and mailing lists where advanced notification of bug and related patches is often disclosed prior to a public announcement by the vendor. This allows the Company to plan ahead for upcoming patches.

Company administrators consider each patch carefully and independently to determine if it is necessary to deploy it within the production environment. In many cases, the vulnerability addressed by the patch has been mitigated through any number of other countermeasures already in place such as firewalls, the IPS, or an aspect of their hardening process. In these cases, patches may be deferred until a future service pack is made available.

Physical Security

The Company's production servers are maintained onsite in a locked server room. Access to the server room is control by physical lock and key. Only authorized individuals have keys to the server room.

Logical Access to the Network, Servers, Applications, and Databases

User accounts and access rights are managed on the domain controllers employing the Internet- standard Kerberos network authentication protocol to authenticate both the client and the network, and to protect against the possibility of unauthorized users impersonating a server to enter the network.

Access to network resources and data is granted to individuals based on their job responsibilities. Unique user IDs and passwords are assigned to each user. The system administrator sets the user's initial password. The user is required to change the password at first logon. Accounts are configured to lockout after three invalid access attempts.

APL's Commission Accounting System requires unique user IDs and passwords. User accounts for APL employees and client users are administered by APL system administrators. Passwords systematically expire every 90 days.

Backup and Recovery

APL backs up production databases and systems daily to an external hard drives. External hard drives are stored offsite in a safe deposit box. APL also utilizes the subservice organization, Amazon Web Services System ("AWS") that is responsible for providing a web services interface that can be used to store and retrieve data.

Control Objectives and Related Controls

Section IV of this report includes APL's control objectives and related control activities to eliminate the redundancy that would result from listing them here in Section III and repeating them in Section IV. Although the control objectives and related control activities are included in Section IV, they are, nevertheless, an integral part of APL's description of controls.

Complementary Subservice Organization Controls

APL's controls related to the information technology general control system cover only a portion of overall internal control for each user entity. It is not feasible for the control objectives related to the agency management and commission software as a service to be achieved solely by APL. Therefore, each user entity's internal control over management and commission reporting must be evaluated in conjunction with APL controls and related tests and results described in section IV of this report, taking into account the related complementary subservice organization controls expected to be implemented at the subservice organizations as described below:

- The Strickland Group ("Strickland") is responsible for maintaining APL's firewall, anti-virus, network monitoring, infrastructure change, and backup configuration, and monitoring. (CO 3,4,5,6)
- Strickland is responsible for maintaining logical security over the management and commission system infrastructure applications and data. (CO 3)
- Strickland is responsible for maintaining a firewall system and notifying APL of any security incidents. (CO 3)
- Strickland is responsible for maintaining anti-virus and spam filtering applications for APL mail. (CO 3)
- Strickland and AWS is responsible for backup procedures to assure backup information is properly maintained, protected and kept current. (CO 6)
- Strickland and AWS is responsible for a disaster recovery plan related to the management and commission system infrastructure applications and data. (CO 6)

Complementary User Entity Controls

This report is restricted to services provided to users of APL and, accordingly, does not extend to controls in effect at user locations. It is not feasible for all of the control objectives to be completely achieved through APL's implemented

controls. While APL fully achieves some objectives, procedures performed by user organizations contribute significantly to the overall achievement of control objectives. This section highlights procedures that should be considered by user organizations in order to fully achieve desired control objectives. Other control objectives may be defined by the users and must be achieved solely by the user.

- The client is responsible for ensuring that all information sent to APL is appropriately authorized, complete, accurate, properly secured and submitted in a timely manner. (CO 1)
- The client must notify APL of any changes (e.g., new hire, termination, transfer, etc.) to employees with access rights and relationship privileges. (CO 1)
- Any changes in communication and connectivity or related procedures that may affect the way data is secured and transmitted must be communicated to APL in a timely fashion. (CO 1)
- Issues or outages that affect the process flow must be properly communicated to APL in a timely manner. (CO 3)
- Controls must be implemented and maintained to ensure physical and logical security of systems that accumulate and transmit data to APL. These controls should encompass granting user access to information, and this access should be reviewed on a periodic basis to ensure that each user's rights are appropriate. (CO 2, 3)
- Firewalls, anti-virus and anti-spam software should be implemented, properly configured and maintained with appropriate upgrades and up-to-date definitions. (CO 3)
- Controls must be implemented to ensure that user accounts, passwords and tools provided by APL remain confidential and are used appropriately. (CO 3)
- The client is responsible for notifying APL of any security breaches that may compromise confidential data and associated systems or negatively impact data flow. (CO 3)
- The client is responsible to ensure that issues as communicated to the client by APL are completely, accurately and timely rectified. (CO 3)
- The client should review all information provided by APL on a regular basis. Discrepancies should be communicated timely. (CO 3)

Section IV

Description of APL's Control Objectives and Related Controls, and Independent Service Auditor's Description of Tests and Results

CO1.0 - Control Objective Related to Control Environment & Risk Assessment
Controls provide reasonable assurance that management identifies and assesses risks and provides oversight, standards of conduct, and a structure for carrying out internal controls.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CO1.1	An organizational structure is in place to establish and communicate key areas of authority, responsibility, and appropriate lines of reporting. The organizational structure is reviewed and updated periodically.	Inquired of management that reporting lines and levels of authority and responsibility are based on positions and that the organizational chart was up- to-date.	No exceptions noted.
		Inspected the Company's most recent organizational chart.	No exceptions noted.
CO1.2	A board of directors oversees management activities.	Inquired of management regarding the board of directors to determine that a board of directors was in place to oversee management activities.	No exceptions noted.
		Inspected the listing of the board of director members to determine that a board of directors was in place.	No exceptions noted.
		Inspected board minutes to verify that the board oversees management activities.	No exceptions noted.
CO1.3	The Company maintains established policies and procedures, which outline operating practices and business conduct for employees, contractors and interns. Policies and procedures are reviewed periodically, updated when needed and communicated to employees. The policies and procedures include the following: • New Hire Package - Confidentiality Agreements - Employee Rules of Conduct - Attendance Policy - Acceptable Use Policy • Disciplinary Policy • Hiring Practices • Employee Handbook - Standards of Conduct • Confidential Information and Invention Assignment • Information Security Manual - Acceptable Use - Anti-virus - Application security - Data Encryption - Firewalls - Password - Change/Patch Management - Restoration Procedures - Remote Access • Password Policy • Remote Access Policy	Inspected the Company's most recent versions of the identified policies and procedures and inquired with management to verify they were reviewed as needed, and up to date.	No exceptions noted.
CO1.4	Employees, contractors, and interns are required to read and acknowledge receipt of the Confidentiality Agreement, Rules of Conduct, and Acceptable Use Policy upon hire. Employees and Contractors must also read and acknowledge receipt of the Attendance Policy.	Inquired of management and reviewed the new hire query for new hires.	No exceptions noted.

CO1.0 - Control Objective Related to Control Environment & Risk Assessment
Controls provide reasonable assurance that management identifies and assesses risks and provides oversight, standards of conduct, and a structure for carrying out internal controls.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected signed acknowledgements for a sample of new employees to verify that the Confidentiality Agreement, Rules of Conduct Acknowledgement and Acceptable Use Policy were communicated.	No exceptions noted.
		Inspected signed acknowledgements for a sample of new contractors to verify that the Confidentiality Agreement, Rules of Conduct Acknowledgement and Acceptable Use Policy were communicated.	No happenings during the period.
		Inspected signed acknowledgements for a sample of new interns to verify that the Confidentiality Agreement, Rules of Conduct Acknowledgement and Acceptable Use Policy were communicated.	No happenings during the period.
CO1.5	Contractors are required to re-acknowledge the Confidentiality Agreement annually.	Inspected signed acknowledgements for a sample of contractors to verify that the Confidentiality Agreement, was re-acknowledged annually.	No exceptions noted.
CO1.6	Management performs an annual enterprise-wide Risk Assessment, whereby it identifies and evaluates business, operating, IT, compliance, and financial statement risks facing the Company, as well as mitigation plans. The risk assessment is reviewed and approved by the President.	Inquired of management that the risk assessment is performed annually.	No exceptions noted.
		Inspected the 2023/2024 Risk Assessment and approval by the President	No exceptions noted.
CO1.7	Management establishes training programs and monitors completion of training programs at least annually.	Inspected training materials to verify training courses are available to personnel.	No exceptions noted.
		Inspected attendance roster of employees to verify that management monitored training at least annually.	No exceptions noted.
		Inspected attendance roster of contractors to verify that management monitored training at least annually.	No exceptions noted.
CO1.8	Each employee's performance is monitored on an ongoing basis and communicated; remedial action is taken when appropriate.	Inquired of the management regarding employee performance monitoring and communications.	No exceptions noted.
		Inspected a sample of personnel files for evidence of performance monitoring of employees.	No exceptions noted.

CO2.0 - Control Objective Related to Physical Access and Environmental Security of Main Office
Controls provide reasonable assurance that physical access to computer and other resources is restricted to authorized personnel.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CO2.1	Access to the company's onsite server room is limited and provided to authorized employees, consultants and principals of the Company.	Inquired of management that entry to the onsite server room is limited and provided to authorized personnel. Inspected the corporate facility access list.	No exceptions noted. No exceptions noted.

CO3.0 - Control Objective Related to Logical Access and Security
Controls provide reasonable assurance that security measures are in place around sensitive data and logical access to programs, data, and computer resources is restricted to authorized and appropriate users.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CO3.1	New or modified access to the network, applications and databases is timely granted or changed after the completion of an access request form that is authorized by appropriate individuals.	Inquired of management that access to the network, applications and databases is timely granted or changed after the completion of an access request form that is authorized by appropriate individuals.	No exceptions noted.
		Inspected new employee query forms & role changes forms to see if access was timely and authorized.	No exceptions noted.
CO3.2	Administrator access to the network, application, and related databases is restricted to authorized personnel.	Inquired of management that administrator access to systems is authorized personnel.	No exceptions noted.
		Inspected the administrator access listing for the network and applications.	No exceptions noted.
		Inspected network diagram.	No exceptions noted.
CO3.3	Network, application, and database passwords conform to the requirements described in the Password Policy.	Inspected that the Internal network domain (default domain) passwords conformed to the following requirements: • Enforce password history - 24 passwords remembered • Maximum password age - 100 days • Minimum password age - 1 day • Minimum password length - 6 characters • Complexity requirement enabled	No exceptions noted.
		Inspected that the production domain passwords conformed to the following requirements: • Enforce password history - 24 passwords remembered • Maximum password age - 100 days • Minimum password age - 1 day • Minimum password length - 6 characters • Complexity requirement enabled.	No exceptions noted.
CO3.4	Management revokes network and production server connection privileges assigned to terminated employees as a component of the employee termination process.	Inspected the default domain user listing and a sample of production server user listings to determine that management revoked network access privileges assigned to terminated employees as a component of the employee termination process	No exceptions noted.
CO3.5	Human Resources management utilizes a termination checklist to ensure that specific elements of the termination process are consistently executed. The checklist is retained in the employee file.	Inspected termination checklists for terminated employees during the review period, to determine that Human Resources management utilizes a termination checklist to ensure that specific elements of the termination process are consistently executed, and that the checklists are retained in the employee files.	No exceptions noted.
CO3.6	Remote access connections are utilized over public networks.	Inspected remote access configuration to verify remote access was enabled and access is restricted to authorized individuals.	No exceptions noted.

CO3.0 - Control Objective Related to Logical Access and Security
Controls provide reasonable assurance that security measures are in place around sensitive data and logical access to programs, data, and computer resources is restricted to authorized and appropriate users.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CO3.7	APL has a secure web application for the use of clients to enter agent hierarchy and payment information.	Inspected the web application software in use to verify whether security protocol (Hypertext Transport Protocol Secure) was enabled.	No exceptions noted.
		Inspected the secure web application to verify that a username and password are required for access.	No exceptions noted.
		Inspected the certification of the web server to verify that secure communication tunnels were in place for file transfers requiring encryption to the Company's web servers through the use of SSL encryption.	No exceptions noted.
CO3.8	A secure file transfer protocol (SFTP) server is utilized for encrypted file transfers.	Inspected the SFTP configuration to verify that an SFTP server was utilized for encrypted file transfers during the audit period under review.	No exceptions noted.
CO3.9	A firewall is in place to control network traffic and prevent unauthorized traffic from passing between the internal network and external networks. Administrator access to the firewall is restricted to authorized personnel.	Inspected the firewall configuration to verify that a firewall was in place to control network traffic and prevent unauthorized traffic from passing between the internal network and external networks.	No exceptions noted.
		Inquired of management that administrator access is restricted to authorized individuals.	No exceptions noted.
		Inspected the system generated user list to verify that administrator access is restricted to authorized individuals.	No exceptions noted.
CO3.10	Anti-virus software is installed and configured on all production servers and workstations to automatically scan and update virus definitions real-time. Administrator access to the anti-virus software is restricted to authorized personnel.	Inspected the anti-virus software configuration for a sample of servers to verify that anti-virus software was configured to automatically scan and update virus definitions real-time.	No exceptions noted.
		Inspected the anti-virus software configuration for a sample of workstations to verify that anti-virus software was configured to automatically scan and update virus definitions real-time.	No exceptions noted.
CO3.11	APL management reviews the SOC report of the subservice organization and documents the results of the review of the SOC report in a memo.	Inquired of management to determine that APL management reviews the SOC report of the subservice organization annually.	No exceptions noted.
		Inspected the most recent SOC report for the subservice organization.	No exceptions noted.
		Inspected management's memo to determine that APL management documents the results of the review of the SOC report in a memo.	No exceptions noted.

CO4.0 - Control Objective Related to System Monitoring
Controls provide reasonable assurance that systems are monitored and deviations, problems, and errors are identified, tracked, and recorded in a complete, accurate, and timely manner.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CO4.1	Management contracts with a third party to provide monitoring of its production environment. Management receives monthly emails to monitor the subservice organizations. Remediation tickets are created as a result of monitoring alerts, if necessary.	Inspected monthly emails to verify critical/relevant system errors were monitored for the period.	No exceptions noted.
		Inspected a sample of tickets to determine that remediation tickets are generated as a result of monitoring alerts, if necessary.	No happenings during the period
CO4.2	APL management reviews the SOC report of the subservice organization and documents the results of the review of the SOC report in a memo.	Inquired of management to determine that APL management reviews the SOC report of the subservice organization annually.	No exceptions noted.
		Inspected the most recent SOC report for the subservice organization.	No exceptions noted.
		Inspected management's memo to determine that APL management documents the results of the review of the SOC report in a memo.	No exceptions noted.

CO5.0 - Control Objective Related to System Change Management
Controls provide reasonable assurance that changes to systems, applications, databases, and infrastructure are authorized, tested, documented, approved and implemented.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CO5.1	Management authorizes and approves the implementation of changes to existing systems, applications, and databases according to approved policies.	Inspected the ticket details for a sample of changes to existing systems, applications, and databases to verify they were authorized by management for development.	No exceptions noted.
		Inspected the ticket details for a sample of changes to existing systems, applications, and databases to verify they were approved by management for migration to production.	No exceptions noted.
CO5.2	The Company tests changes to systems, applications, and databases in a segregated environment prior to system implementation.	Inspected the ticket details for a sample of changes to existing systems, applications, and databases to verify they were tested prior to system implementation.	No exceptions noted.
		Inspected the system documentation to verify that there are segregated environments for testing, development, and production.	No exceptions noted.
CO5.3	Access to move changes to production is authorized and restricted to appropriate individuals.	Inquired of management that personnel that have access to move changes to production are authorized by management.	No exceptions noted.
		Inspected the management approved list of personnel with access to move changes to production to verify the access rights were authorized.	No exceptions noted.
		Inspected ticket details for a sample of changes to verify that changes are authorized by authorized individuals.	No exceptions noted.
CO5.4	Management authorizes and approves the implementation of new and changes to infrastructure according to approved policies.	Inquired of management that management authorizes and approves the implementation changes to infrastructure.	No exceptions noted.
		Inspected ticket details for a sample of changes to infrastructure to verify they were authorized and approved by management	No happenings during the period.
CO5.5	IT personnel periodically review availability of patches on production systems and critical patch updates are installed by IT personnel.	Inspected logs of updates and implemented patches for a sample of servers to verify that critical patch updates were installed.	No exceptions noted.
CO5.6	APL management reviews the SOC report of the subservice organization and documents the results of the review of the SOC report in a memo.	Inquired of management to determine that APL management reviews the SOC report of the subservice organization annually.	No exceptions noted.
		Inspected the most recent SOC report for the subservice organization.	No exceptions noted.
		Inspected management's memo to determine that APL management documents the results of the review of the SOC report in a memo.	No exceptions noted.

CO6.0 - Control Objective Related to Back-Up and Recovery
Controls provide reasonable assurance that critical applications and data are backed up regularly and are available for restoration in the event of processing errors or unexpected processing interruptions.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CO6.1	A backup process is in place to perform full daily data and system backups. Backup jobs are monitored daily by designated IT staff. Administrator access to the backup software is restricted to authorized personnel.	Inspected the configuration of the backup software used for a sample of servers and databases to verify that backup processes were scheduled to run to provide daily backups and has logging enabled.	No exceptions noted.
		Inspected the historical backup log for the examination period for a sample of servers and databases to verify the daily backups were performed.	No exceptions noted.
		Inspected the administrator access listing and compared to the system-generated list of backup administrators to verify their access was authorized.	No exceptions noted.
CO6.2	APL management reviews the SOC report of the subservice organization and documents the results of the review of the SOC report in a memo.	Inquired of management to determine that APL management reviews the SOC report of the subservice organization annually.	No exceptions noted.
		Inspected the most recent SOC report for the subservice organization.	No exceptions noted.
		Inspected management's memo to determine that APL management documents the results of the review of the SOC report in a memo.	No exceptions noted.

End of Report