SOC 3 – Security

Independent Practitioner's Trust Services Report for the Period of July 1, 2014 through June 30, 2015

whitleypenn

Dallas Office
8343 Douglas Avenue
Suite 400
Dallas, Texas 75225
214.393.9300 Main

whitleypenn.com

I. INDEPENDENT PRACTIONER'S TRUST SERVICES REPORT

American Data Corporation
Lafayette, Louisiana

We have examined management's assertion that during the period of July 1, 2014 through June 30, 2015, American Data Corporation (the "Company") maintained effective controls over its land management system (the "system") to provide reasonable assurance that the system was protected against unauthorized access (both physical and logical) based on the American Institute of Certified Public Accountants ("AICPA") and Canadian Institute of Chartered Accountants ("CICA") security principle and criteria set forth in TSP section 100, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Principles and Criteria)* (the "applicable trust services criteria").

The Company's management is responsible for its assertion. Our responsibility is to express an opinion based on our examination. Management's description of the aspects of the system covered by its assertion is attached. We did not examine this description, and accordingly, we do not express an opinion on it.

Our examination was conducted in accordance with attestation standards established by the AICPA and, accordingly, included (1) obtaining an understanding of the Company's relevant controls over security of the system; (2) testing and evaluating the operating effectiveness of the controls; and (3) performing such other procedures as we considered necessary during our examination. We believe that our examination provides a reasonable basis for our opinion.

Because of the nature and inherent limitations of controls, the Company's ability to meet the applicable trust services criteria and its commitments may be affected. For example, controls may not prevent or detect and correct error or fraud, unauthorized access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection of any conclusions based on our findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

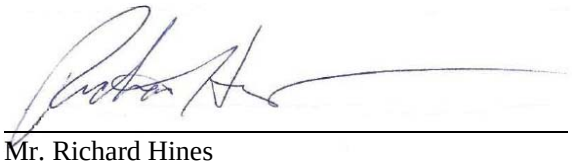
In our opinion, the Company's assertion referred to above is fairly stated, in all material respects, based on the applicable trust services criteria.

Whitley Penn LLP

Dallas, Texas
February 23, 2016

II. AMERICAN DATA CORPORATION'S ASSERTION REGARDING ITS LAND MANAGEMENT SYSTEM

American Data Corporation (the "Company") maintained effective controls over the security of its land management system (the "system") to provide reasonable assurance that the system was protected against unauthorized access (both physical and logical) for the period of July 1, 2014 to June 30, 2015, based on the AICPA and CICA security principle and criteria set forth in TSP section 100, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Principles and Criteria*).



Mr. Richard Hines
Vice President and Managing Partner

III. AMERICAN DATA CORPORATION'S DESCRIPTION OF ITS LAND MANAGEMENT SYSTEM

OVERVIEW OF OPERATIONS

Summary of Business

American Data Corporation's iLandMan Software Solution ("iLandMan" or the "Company"), based in Lafayette, Louisiana, is a specialized professional services firm offering a comprehensive land management system which is a software as a service online database for the organization, storage, and mapping of contracts for clients with thousands of oil and gas lease, rights of way, and seismic permit relationships. The Company was founded by Timothy Supple in 1980. The Company improves efficiency and delivers process improvements through three service lines: (i) information data integrity, (ii) client data review, and (iii) visual performance reviews using a mapping interface.

iLandMan provides a standardized structure for the collection of land title and ownership information. This information is used to contact surface and mineral owners, prepare oil and gas industry contracts, and provide payment instruments to these owners from either lease broker contractors or oil and gas companies. The resulting contracts and associated materials are stored on the iLandMan servers for retrieval by clients as well as reporting and mapping services for answering industry specific queries and visual representation of client information for their proprietary use.

The Company has structured its differentiated process to incorporate proprietary methodologies, analysis of all supporting ownership data/documentation, and knowledge gained from preparing and negotiating contracts with notable oil and gas companies.

iLandMan utilizes proprietary processes and software to assist clients' land departments and lease broker contractors to identify, validate, and resolve erroneous contract entry and payments. iLandMan combines data entry and importation of information, review of client data files with an emphasis on delivering analytical review accompanied by actionable operational recommendations and Geographic Information Systems ("GIS") Mapping tools to present the information in a logical and viewable mapping format.

COMPONENTS OF THE SYSTEM

Infrastructure

The internal infrastructure of American Data Corporation's iLandMan software solution must be designed and sustained in such a way to ensure that security is maintained.

The iLandMan building uses a card pass system for after-hours access. The suite uses a key system on the door locks. A barrel lock is implemented on the front door with only 12 keys issued. A separate server network closet is also maintained in the suite. The closet contains an air conditioning ("A/C") system, full rolling rack, and is protected with a key pad code lock with code access limited by only certain team members. This server network is used for the Research and Development team as well as the Consulting/Services team.

The iLandMan System employs multiple servers, both physical and virtual, in the production environment. The servers are currently on a Windows Server platform, using Structured Query Language ("SQL") Server, Internet Information Services ("IIS"), and specific languages/environments. Using a suite of other various canned and custom solutions iLandMan can provide the software as a service from its commercial production environment.

III. AMERICAN DATA CORPORATION'S DESCRIPTION OF ITS LAND MANAGEMENT SYSTEM *(continued)*

The internal network utilizes Dell switches and Cisco routers. The external network is redundant through two different internet service providers routed on different networks using LUS Fiber and Rackspace.

As of October 1, 2014, the iLandMan System resides on a separate network housed offsite at a commercial hosting facility, known as Amazon Web Services. This report includes only the controls to meet the applicable trust services criteria of American Data Corporation and excludes the controls to meet the applicable trust services criteria of the commercial hosting subservice organization.

Management has established policies and procedures around incident management for complaints and requests relating to security issues. With both a security breach and disaster recovery policy in place, users have a course of action to notify the Company of potential security threats and breaches, as well as have assurance that data can be timely restored in the event of a disaster.

Changes to system components, including those that may affect system security, require the approval of the Information Technology ("IT") Director before implementation. Discussions may be held within the IT department or with other management prior to implementation depending on the scale of the change and timeframe for its accomplishment. Management, along with Programming development and Mapping development teams, meet on a regular basis to determine how system components interact as well as affect the system security. Documentation and action items are created with workflow tickets.

Procedures are followed for design, acquisition, implementation, and maintenance of computerized information systems, and related technology that are consistent with security policies.

The IT department maintains an up-to-date listing of all system software versions and patches that have been applied using system utility software. This is dynamic and available from the administration of the server software dashboard.

Infrastructure changes are documented before being placed into the production environment. A full sandbox environment is used to test new ideas and structure. Following completion of new build coding a staging environment is used which is as close to a live production environment as possible. Testing is completed on the staging environment if all testing passes then a production build is scheduled. System maintenance releases and changes follow a structured program change methodology which includes review and approval by the IT Director.

Emergency change requests are documented and subject to formal change management procedures. iLandMan uses a priority system on a 1 to 5 scale, where 1 has the lowest priority and 5 the highest. If a priority 5 change request occurs, a hot fix is initiated immediately and is uploaded to the production build as soon as the change has been completed and tested. Documentation cannot always happen prior to implementation, but once a fix has occurred, the permanence of the fix is based on the standard procedures to determine if the emergency fix is kept or another fix is implemented once the immediate concern is mitigated.

The IT department monitors and assesses the system vulnerabilities using system utility software. Using multiple monitors allows the IT department to have the ability to view items that may cause a problem, as well as detect events as they are occurring. Operating System ("OS") and application security events are captured in an event log and monitored; the logs are reviewed in the event of a suspected security breach.

III. AMERICAN DATA CORPORATION'S DESCRIPTION OF ITS LAND MANAGEMENT SYSTEM *(continued)*

When a security related incident is detected or reported, a defined incident management process is initiated by authorized personnel; corrective actions are implemented in accordance with established incident management policies and procedures. The IT department personnel will initiate a workflow ticket for the incident and follow up with the appropriate response and results.

Critical incidents related to security are tracked by management until resolved through our internal workflow process.

Personnel and Software Components

Security policies, addressing both IT and physical security, are defined and approved by Senior Management and implemented throughout the organization. The Security Administrator is responsible for maintaining and enforcing security policy. This is done with assistance from Senior Management as necessary.

New full-time employees sign a statement signifying that they have read, understood, and will follow relevant security policies outlined in the employee handbook. The handbook is organized and updated annually and supplied to all Company employees and contractors. It is available via the Company intranet and in printed version. All new contractors' sign a statement signifying that they have read, understood, and will follow relevant security policies in the contractor handbook.

Management validates that position descriptions are established and updated regularly. These position descriptions delineate both authority and responsibility, and include definitions of skills and experience needed in the relevant positions. This is the primary tool for discerning security rights within the organization.

New personnel (full-time employee and contractors) are offered employment subject to background and reference validation. This is completed post-employment offer, as the perspective employee or contractor must consent to some of the screening. Completion of the screening process is done as soon as practical and those who do not pass are either not hired or are terminated.

Procedures prevent unauthorized access to client data by non- iLandMan personnel. By using license specific log in information, unique user identification codes ("ID"), and secure passwords the client allows only authorized users to access their information. Also, by giving full permission access to the License Administrator, iLandMan clients have full control of who has access to their data as well as specific areas of data.

Procedures

Management has developed policies and procedures that establish the organization's overall approach to security and internal control. These policies and procedures comply with overall business objectives and are aimed at minimization of risk through preventive measures, timely identification of irregularities, limitation of losses, and timely restoration. The Company's policies and procedures include the definition and assignment of responsibilities. Penalties and disciplinary actions associated with failing to comply with security and internal control policies are defined.

III. AMERICAN DATA CORPORATION'S DESCRIPTION OF ITS LAND MANAGEMENT SYSTEM *(continued)*

Physical Access

iLandMan is located in a leased office building in Lafayette, Louisiana at 315 S. College, Suite 270. The building is managed by Property One, Inc. The property manager is responsible for all infrastructure maintenance, including fire alarms and suppression, building entry, and video surveillance. iLandMan has 6 full time employees and 13 full time contractors.

The corporate office is equipped with access control devices to validate that access to facility is restricted. This includes barrel locked doors and an electronic card system at the primary entrance for after-hours use.

The server room is restricted to authorized personnel. This is done using key pad locks, and allowing only a limited number of parties to have access. A log is kept with information on entry, allowed access, day, time, and reason for entry. Procedures are defined and implemented for the proper authorization and termination of physical access to the corporate office.

Logical Access

Management has established policies and procedures for logical access, as well as computer network access and equipment responsibilities. User access is limited to the applications and related data for which they are authorized and approved. Network and application authorization policies address password parameters around frequency, complexity, and length. The levels of this are suggested by the IT staff and approved by management through email and/or discussions. User IDs are assigned to individual users. New network access is reviewed and approved by the appropriate user manager; access to client data is approved by the designated manager.

System access for a user is terminated upon termination of the user's affiliation with iLandMan. A Termination and/or Resignation letter is usually received by management from the user. A termination/resignation checklist is then enacted to document the corporate information and/or items that have been disabled and retrieved. The user access (keys and cards) are then retrieved during the exit interview/discussion. Management performs a monthly review of user accounts to ensure that user accounts are valid and assigned privileges are aligned with users' functional roles.

Employees and contractors carrying sensitive data are provided with laptops that have encryption software to ensure security of client data. Employees and contractors are advised not store any personal or client-sensitive data on their personal computers or on laptops. Management has designed a secure data storage methodology on the corporate servers for client data.

Until October 1, 2014, firewall, anti-virus protection, intrusion detection software ("IDS"), and intrusion prevention software ("IPS") were in place and managed by the Company to limit the possibility of disruptions that could compromise the security of client data. As of October 1, 2014, all servers hosting the iLandMan application were outsourced to Amazon Web Services ("AWS"). AWS manages all firewall, anti-virus, IDS, and IPS. The testing in Section IV of this report includes only the controls of American Data Corporation and excludes the controls of the commercial hosting subservice organization.

Data

Information owners are the senior management personnel, or their delegates within iLandMan, who bear responsibility for the acquisition, development, use and maintenance of the data, systems, and applications which process American Data Corporation's iLandMan Software Solution information and that of its clients and business partners.

iLandMan does not change client data, unless it is instructed to do so by the client. Clients have full access to enter and edit their own data but at times they contract the data entry and verification to the iLandMan service unit. The Service unit reviews the data that has been entered and/or given to the Company by the client and loaded into the database environment. The client is responsible for the maintenance of its project data unless it has contracted with iLandMan to provide additional services. The client is also responsible for setting up their own license users and permissions. The users can be deactivated with one selection of the active user check box.

Transmission of sensitive data between iLandMan, its clients and its business partners is encrypted. All data packets traveling to and from the servers are encrypted using Secure Sockets Layer ("SSL") certificates.

RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT, INFORMATION AND COMMUNICATION, AND MONITORING

Control Environment

Management has developed policies that establish the organization's overall approach to security and internal control. These policies comply with overall business objectives and are aimed at minimization of risk through preventive measures, timely identification of irregularities, limitation of losses, and timely restoration. The Company's policies include the definition and assignment of responsibilities. Penalties and disciplinary actions associated with failing to comply with security and internal control policies are defined.

Risk Assessment

All systems must be reviewed regularly to ensure it meets all Company needs and possible regulatory and legal requirements as mandated by outside parties. Management develops an annual business plan, which identifies business risks and establishes their key initiatives/action plans.

Management holds a leadership and member retreat at its corporate offices annually to address initiatives and action plans dealing with hardware, software, sales, training, management, operations, marketing, and other related business items. The entire corporate team participates in this multiday event either in person or over voice/video presence. An agenda is developed and distributed prior to the event, with time slots maintained to give all stakeholders a chance to express their ideas and concerns.

Management also holds regular meetings to address short and long-term business goals and make any necessary adjustments based on new risks or opportunities. These meetings include any offsite personnel or client personnel necessary to address the items or goals.

Risk assessments are conducted on a semi-annual basis unless changes require more frequent meetings. Goals and adjustments are addressed and made available to the development team as well as management.

Information and Communication

All users must be made aware of expectations and be trained on how to fulfill these expectations. Management orients and trains newly hired employees as well as distributes important materials which include detailed descriptions of roles and responsibilities.

Management provides news, memos, and important information via email sent to all employees and contractors. These updates happen any time there are significant changes to policies or procedures that impact employees and contractors.

Monitoring

The monitoring process is achieved through several ongoing activities that include: independent audits, executive management oversight, management review of operating performance, and performance improvement evaluations.