Report on Kastle System's Management Assertion Relating to the Managed Security Services System For the Period January 1, 2018 through November 30, 2018 Relevant to Security

SOC 3®

I.S. Partners
Audit + Compliance + IT Advisory Services

INDEPENDENT PRACTITIONER'S TRUST SERVICES REPORT

To the Management of Kastle Systems:

We have examined management's assertion that Kastle Systems ("Kastle") during the period January 1, 2018 through November 30, 2018, maintained effective controls to provide reasonable assurance that the managed security services system, as described in the attached system description, was: 1) protected against unauthorized access, use, or modification (both physical and logical) to meet the entity's commitments and system requirements, based on the American Institute of Certified Public Accountants' ("AICPA") Trust Services Criteria for Security set forth in TSP Section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* ("applicable trust services criteria").

Kastle's management is responsible for this assertion. Our responsibility is to express an opinion based on our examination. Management's description of the managed security services 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 American Institute of Certified Public Accountants and, accordingly, included: (1) obtaining an understanding of the controls related to the security of the managed security services system; (2) testing and evaluating the operating effectiveness of the controls; and (3) performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

Because of the nature and inherent limitations in controls, Kastle's ability to meet the aforementioned criteria 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 and requirements. Furthermore, 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, management's assertion referred to above is fairly stated, in all material respects, based on the AICPA Trust Services Criteria for Security.

IS Partners, LLC

IS Partners, LLC
Certified Public Accountants
Horsham, Pennsylvania
February 13, 2019

I.S. Partners, LLC
100 Tournament Drive
Suite 225
Horsham, PA 19044

215.675.1400 main office
866.642.2230 toll-free
215.259.7928 fax
www.ISPartnersLLC.com

Management's Assertion Regarding the Effectiveness of its Controls over Kastle Systems' Managed Security Services System Based on the AICPA Trust Services™ Criteria for Security

Kastle Systems maintained effective controls over the security of the managed security services system to provide reasonable assurance that:

- the system was protected against unauthorized access, use, or modification (both physical and logical) to meet the entity's commitments and system requirements

during the period January 1, 2018 through November 30, 2018, based on the Trust Services™ Criteria for security, established by the American Institute of Certified Public Accountants ("AICPA") set forth in TSP Section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

The attached "System Description of Kastle Systems' Managed Security Services System" identifies those aspects of the system covered by our assertion.

Kastle Systems
February 13, 2019

System Description of Kastle Systems' Managed Security Services System

Background

Kastle Systems has been a leader in the security industry for more than 45 years with new technologies and advanced security solutions. Kastle was named the 2015 Systems Integrator of the Year for outstanding innovation and customer experience by SDM, the industry's leading trade publication, Kastle operates and manages security systems for over 10,000 locations around-the-clock. Kastle's innovative outsourced security services including video, access and visitor management, significantly reduce costs and improve the critically important, 24/7 performance of security systems for building owners, developers and tenants.

Kastle creates security solutions based on an expert assessment of each client's unique environment and situation. Kastle partners with leading manufacturers in the security industry and build open, standardized systems suited to each client. Kastle implements their designs using industry best practices, with minimal business interruption. Kastle ensures that each client's system operates in peak condition because they repair, replace, and warranty their products.

Kastle's Managed Security Services includes a team of trained operators that works in the industry's most advanced centers 24×7, responding to critical signals that are reported to client administrators. Kastle takes responsibility for security procedures, database management, and reporting on trends and events, delivering the highest level of preparedness. Account managers work as the main point of contact, while tools and organization ensure that Kastle can provide assistance to clients quickly and efficiently. Kastle's services strengthen business continuity plans with redundancy in power, connectivity, support coverage, and data storage.

This system description covers Kastle's Managed Security Services.

Products and Services

The primary products and services that Kastle Systems provides to clients are as follows:

Access Control - Kastle Systems is the industry's leading provider of managed access control and is recognized by peers as best in class You can count on us, as part of your team, to complete the tasks that maintain security integrity day in and day out. Kastle's access control monitors and responds to critical security alarms at industry-best levels. With Kastle's access control, an employee is recorded only once, and every credential is associated with that person. Kastle syncs their access control system with the client's authoritative source. The result is that on-boarding and off-boarding are automatically controlled, and end users can use a single credential to access multiple offices or spaces easily.

Video Surveillance (KastleVideo) - KastleVideo allows clients to receive and view highly detailed images from cameras in client buildings. KastleVideo also allows clients to see their video cameras anywhere to monitor what's happening in real time or to review past events. Client computers, laptops, surface tablets, and smartphones can be used to access live footage from KastleVideo. Through advances in analytics, KastleVideo can set rules for multiple functions. The system can be programmed to send an alert to client management when someone is in an area they shouldn't be and various related security and monitoring functions.

Visitor Management (Kastle FrontOffice) - Kastle FrontOffice enables visitor registration directly from Microsoft Outlook or Gmail, to user-friendly barcodes that are emailed to visitors for a better check-in experience, KastleFrontOffice helps clients securely increase pre-authorized visitor rates and decrease wait times and congestion in the lobby. The system automatically sends invites, maintains tight control for visitor access timeframes, and assigns and shares a barcode for each visitor, allowing entry into the facility in a fast, efficient manner.

Fire and Life Safety - Kastle monitors critical alarms, such as fire, so that within seconds of an alarm Kastle will have already begun handling it and dispatching first responders. Kastle partners with clients to regularly test equipment and alarm functionality to ensure everything is working exactly as it should be. All of client alarms are sent to multiple monitoring centers simultaneously.

Environmental Control - Kastle critical sensor monitoring protects client systems from a variety of potential disasters caused by unexpected changes in the environment including overheating in the IT room, equipment tampering, HVAC system indicators, power outages or even rising water levels. Kastle provides immediate notification of critical environmental or system changes so you can take action before the damage is done.

24x7 Monitoring - Kastle Systems are connected to client buildings 24×7. This connection gives Kastle the ability to remotely report on everything that's happening in a client space live, in real-time. The Kastle priority queue reports everything but orders it from highest to lowest priority, allowing Kastle operators to respond to the most important events first. Any Kastle location can immediately pick up and take over for any other location, providing clients with expert service. Kastle's team of operators receive extensive training in advanced technology and innovative solutions, and they are committed to client security.

Components of the System
The system is comprised of the following five components:

- Infrastructure (facilities, equipment, and networks)
- Software (systems, applications, and utilities)
- People (developers, operators, users, and managers)
- Procedures (automated and manual)
- Data (transactions streams, files, databases, and tables)

The following sections of this description define each of these five components comprising Kastle's managed security services system.

Infrastructure

Kastle Systems is headquartered in Falls Church, Virginia. Kastle Systems also has offices in Atlanta, Los Angeles, San Francisco, Houston, Dallas, Chicago, Miami, New York, Philadelphia, and Sydney, Australia. Physical and logical security controls are uniform across all Kastle locations. Access to every office, computer machine room, and other Kastle work areas containing sensitive information is physically restricted. During non-working hours, workers in areas containing sensitive information lock-up all information. All Kastle computer and network equipment is physically secured at all times. Local area network servers and other multi-user systems are placed in locked cabinets, locked closets, or locked computer rooms. Computer and network gear may not be removed from Kastle offices unless the involved person has obtained permission from management.

- **Internal Network Connections** - All Kastle computers that store sensitive information and that are permanently or intermittently connected to internal computer networks have a password-based access control system approved by the Information Security department. Regardless of the network connections, all stand-alone computers handling sensitive information also employ an approved password-based access control system. Multi-user systems throughout Kastle employ automatic log-off systems that automatically terminate a user's session after a defined period of inactivity and require the user to re-log on to regain access.

- **External Network Connections** - All in-bound session connections to Kastle computers from external networks are protected with an approved password access control system. Users with personal computers connected to external networks are prohibited from leaving unattended modems turned-on while data communications software is enabled when using Kastle computers. Kastle workers must not establish connections with external networks including Internet service providers unless these connections have been approved by the Information Security department.

- **Electronic Mail** - All Kastle business communications sent by electronic mail are sent and received using an approved electronic mail address. A personal Internet service provider electronic mail account or any other electronic mail address cannot be used for Kastle business unless a worker obtains management approval.

- **Computer Virus Screening** - All personal computer users have the current versions of approved virus screening software enabled on their computers. Virus screening software is used to scan all software and data files coming from either third parties or other Kastle groups. This scanning takes place before new data files are opened and

before new software is executed. Workers cannot bypass or turn off the scanning processes that could prevent the transmission of computer viruses.

- **Computer Virus Eradication** - If workers suspect infection by a computer virus, they must immediately stop using the involved computer and call the Kastle help desk. The infected computer must be immediately isolated from internal networks. Users must not attempt to eradicate viruses themselves. Qualified Kastle staff or consultants must complete this task in a manner that minimizes both data destruction and system downtime.

- **Formal Change Control** - All multi user computer and communications systems used for production processing employ a documented change control process that is used to ensure that only authorized changes are made. This change control procedure must be used for all significant changes to production system software, hardware, communications links, and procedures.

Software

- **Software Sources** - Kastle computers and networks must not run software that comes from sources other than other Kastle departments, knowledgeable and trusted user groups, well-known systems security authorities, or established computer, network, or commercial software vendors. Software downloaded from electronic bulletin boards, shareware, public domain software, and other software from untrusted sources must not be used unless it has been subjected to a rigorous testing regimen approved by the Information Technology department.

- **Internet Access** - Workers are provided with Internet access to perform their job duties, but this access may be terminated at any time at the discretion of a worker's supervisor. Internet access is monitored to ensure that workers are not inappropriately visiting sites unrelated to their jobs, and also to ensure that they continue to be in compliance with security policies. Workers must take special care to ensure that they do not represent Kastle on Internet discussion groups and in other public forums, unless they have previously received top management authorization to act in this capacity. All information received from the Internet should be considered to be suspect until confirmed by reliable sources. Workers must not place Kastle material on any publicly-accessible computer system such as the Internet the Information Owner has approved the posting. The establishment of Internet pages is separately handled by an approval process involving the Director of IT. Sensitive information, including passwords and credit card numbers, must not be sent across the Internet unless the communication is secured through secure transport protocols.

Information Technology Department - The Information Technology department is the central point of contact for all information security matters at Kastle Systems. Acting as internal technical consultants, it is this department's responsibility to create workable information security compromises that take into consideration the needs of users, custodians, owners, and selected third parties. Reflecting these compromises, this department defines information security standards, procedures, policies, and other requirements applicable to the entire organization. Information Security must handle all access control administration activities, monitor the security of Kastle information systems, and provide information security training and awareness programs to Kastle workers. The department is responsible for periodically providing management with reports about the current state of information security at Kastle. While information systems contingency planning is the responsibility of information custodians, the Information Technology department must provide technical consulting assistance related to emergency response procedures and disaster recovery. The Information Technology department is also responsible for organizing a computer emergency response team to promptly respond to virus infections, hacker break-ins, system outages, and similar information security problems.

People

The following people comprise the Kastle Systems management team: The Kastle Systems Chairman and Co-Chairman, Chief Executive Officer, Chief Customer Officer, Chief Technology Officer, Chief Human Resources Officer, Chief Financial Officer, and the Regional General Managers.

Procedures

Kastle Systems has documented policies and procedures to support the operation and controls over the system. Specific examples of the relevant policies and procedures include the following:

- Configuration Management
- User Account Management
- Incident Response
- System Security
- Security Standards
- Audits and Accountability
- Data Classification
- Data Security

Data

This component of the system definition is limited to the information used and supported by the system for the services outlined in this description. The Kastle Systems data classification system is based on the concept of need-to-know. This term means that information is not disclosed to any person who does not have a legitimate and demonstrable business need to receive the information. This concept, when combined with security policies, will protect Kastle Systems information from unauthorized disclosure, use, modification, and deletion.

Kastle Systems is committed to protecting the privacy of its clients and to the confidentiality of their information. Kastle Systems expects all employees, consultants and vendors to abide by Kastle Systems' Data Classification and Information Security policies. If non-public information is to be accessed or shared with these third parties, they should be bound by contract to abide by Kastle Systems' Data Classification and Information Security policies.