Report on Kastle Systems, Inc.'s Management Assertion Relating to the Managed Security Services System

January 1, 2019 through December 31, 2019

INDEPENDENT SERVICE AUDITOR'S REPORT

To the Management of Kastle Systems, Inc.:

Scope
We have examined Kastle Systems, Inc.'s ("Kastle") accompanying assertion titled "Management Assertion of Kastle Systems, Inc." ("assertion") that the controls within Kastle's Managed Security Services System ("system") were effective throughout the period January 1, 2019 through December 31, 2019, to provide reasonable assurance that Kastle's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability and confidentiality ("applicable trust services criteria") set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Service Organization's Responsibilities
Kastle is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Kastle's service commitments and system requirements were achieved. Kastle has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Kastle is responsible for selecting, and identifying in its assertion, the applicable trust service criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities
Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that controls were not effective to achieve Kastle's service commitments and system requirements based on the applicable trust services criteria
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Kastle's service commitments and system requirements based on the applicable trust services criteria.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations
There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion
In our opinion, management's assertion that the controls within Kastle's Managed Security Services system were effective throughout the period January 1, 2019 through December 31, 2019, to provide reasonable assurance that Kastle's service commitments and system requirements were achieved based on the applicable trust services criteria, is fairly stated, in all material respects.

IS Partners, LLC

IS Partners, LLC
Horsham, Pennsylvania
June 30, 2020

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 Assertion of Kastle Systems, Inc.

We are responsible for designing, implementing, operating, and maintaining effective controls within Kastle's Managed Security Services System ("system") throughout the period January 1, 2019 through December 31, 2019, to provide reasonable assurance that Kastle's service commitments and system requirements relevant to security, availability, and confidentiality were achieved. Our description of the boundaries of the system is presented in this report and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period January 1, 2019 through December 31, 2019, to provide reasonable assurance that Kastle's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality ("applicable trust services criteria") set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*). Kastle's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period January 1, 2019 through December 31, 2019, to provide reasonable assurance that Kastle's service commitments and system requirements were achieved based on the applicable trust services criteria.

Kastle Systems, Inc.
June 30, 2020

Kastle Systems, Inc.'s Description of the Boundaries of the Managed Security Services System

Background

Kastle Systems has been a leader in the security industry for more than 45 years with new 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 system 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.

Products and Services

Some of 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 onboarding and offboarding 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, Kastle FrontOffice 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.

24/7 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.

Principal Service Commitments and System Requirements

Kastle Systems designs its processes and procedures related to their managed security services system to meet ongoing objectives for the solutions and services offered to customers. Kastle Systems takes commercially reasonable steps and measures in accordance with prevailing practices in the industry to maintain and enforce physical and logical security with respect to customer's data hosted by Kastle Systems, but Kastle Systems makes no guarantee that the customer data will be secure from all threats.

Kastle Systems will report to customers any confirmed security breach or unauthorized access affecting customer data of which Kastle Systems detects or becomes aware. Kastle Systems uses diligent efforts to remedy any breach of security or unauthorized access to customer data. Kastle Systems establishes that, in the course of providing services to customers, Kastle Systems may become aware of or come into possession of certain confidential or proprietary information and documents of customers. Kastle Systems shall not copy any such information without customers' permission, shall not disclose the information to any other person, shall not use the information for any purpose other than performing agreed upon services and shall return all copies of such information when all agreed upon services have been performed.

Kastle Systems establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Kastle Systems' policies and procedures, which were created and established with relevant customer services and systems previously identified. Internal controls are developed with system requirements outlined by management, relevant third-party assessments, and contracts with customers.

Kastle Systems policies define strict guidance governing security practices and commitments. Related subservice organization assessments of internal controls and system vulnerabilities and incidents help maintain Kastle Systems' commitments and requirements to its customers.

This description covers Kastle's managed security services system.

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 the boundaries of 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 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:

Mark Ein – Kastle Systems Chairman - Mark D. Ein is an investor, entrepreneur and philanthropist, who has created, acquired, invested in and built a series of growth companies across a diverse set of industries over the course of his 25-year career. During this time, Mr. Ein has been involved in the founding or early stages of six companies that have been worth over one billion dollars and has led over $1.5 billion of private equity, venture capital and public company investments.

Piyush Sodha – Co-Chairman - Piyush Sodha is the Co-Chairman of Kastle Systems International. In addition, Mr. Sodha has also been a part owner of Kastle Systems International since 2008. Over the last 20 years, Mr. Sodha has been the Chief Executive Officer and Chairman of several world leading technology and telecommunication companies. Prior to joining Kastle, 2004-2008, he has served as the Chairman and Chief Executive Officer of Cibernet Corporation, which merged into MACH in April 2007. Cibernet was the world's largest Financial Settlement House for Wireless operators and settled annually in excess of $10 Billion of transactions. The company served in excess of 400 Wireless Operators in 120+ countries.

Haniel J. Lynn – Chief Executive Officer - Haniel J. Lynn is the Chief Executive Officer of Kastle Systems International (KSI), the industry leader in managed security solutions and services consisting of a family of five security brands including Kastle Systems, Mutual Security Services, Stat Land Security Services, CheckVideo and Urban Alarm. Mr. Lynn joined Kastle in 2018, bringing more than 25 years of global operating and executive management experience growing and scaling enterprises from startup to $1 billion. Mr. Lynn has distinctive strengths in strategy, leadership, and operations and possesses a unique ability to oscillate between high-level vision and tactical execution while inspiring a culture of teamwork.

Tom Radigan – Chief Customer Officer – Tom Radigan is Kastle Systems' Chief Customer Officer and is responsible for the alignment of company processes, resources and attitude to ensure that the customer experience is more efficient, more effective and less intrusive every day. Tom began his Kastle career more than 25 years ago in the Houston office as a part-time alarm monitor while still in college. He has served in a variety of roles, including Director of Call Center Operations, Operations Manager and General Manager for the Southern Region.

Tom received a B.A. in English Literature from The University of Houston and an M.B.A. from Rice University.

Mohammad Soleimani – Chief Technology Officer - Mohammad Soleimani is Kastle Systems' Chief Technology Officer and is responsible for all aspects of Kastle Systems' development and IT efforts. Most recently, Mohammad served as Chairman of the Board for SoleNet, Inc., an engineering services company focused on developing state of the art communications equipment. From 2006 to 2007, Mohammad served as Vice President Engineering for RFID at Motorola, Inc. His responsibilities included advanced development and architectural design of radio-frequency identification (RFID) equipment. While in this position, he led a team of about 40 SW and HW engineers. From 2004 to 2006, Mohammad served as Vice President of Engineering at Matrics, Inc/Symbol , where he was responsible for SW and HW development of RFID readers. Before joining Matrics, Inc/Symbol , Mohammad founded Sole Net, Inc. in 2001 and co-founded BitCom, Inc. in 1998. Mohammad also spent fifteen years as Senior Director for Hughes Network Systems (HNS), where he obtained tremendous leadership experience. He first served as Co-lead System Engineer for Thuraya, a mobile satellite voice and data communication system based in the UAE. He later became the Lead Systems Engineer for ICO, a Medium Earth Orbit (MEO) mobile satellite system for voice and data communication. He also became Lead Engineer for the first phase of DirecTV receivers. Mohammad obtained his Bachelor of Science in Electrical Engineering at Rochester Institute of Technology and Master of Science in Electrical Engineering with honors from George Washington University.

Brook Carlon – Chief Human Resources Officer

Ralph Masino – Chief Financial Officer - Ralph Masino is Kastle Systems' Chief Financial Officer and is responsible for managing overall financial strategy including financing, acquisition analysis, capital usage, risk management and business profitability. Ralph brings more than 25 years of extensive financial knowledge and executive leadership experience from his work with publicly traded, private equity and venture capital backed businesses. Ralph was most recently the Chief Financial Officer of ASG Security through its sale to Apollo Global Management in 2015. During his tenure at ASG, Masino helped to grow the regional security company into one of the top 10 largest security companies in the U.S. through a combination of organic growth and strategic acquisitions. Prior to ASG, Masino held executive positions with Baan Company N.V., a global ERP provider, and World Airways, an international provider of passenger and cargo airline services. Masino began his career in the audit practice of Arthur Andersen after graduating from The American University with a bachelor's degree in Accounting.

Mike Slauson – General Manager – Southern Region - Mike Slauson, based in Houston, Texas, is responsible for sales, operations and development for Kastle's Central Region. Offices in the Central Region include the Midwestern office in Chicago and the Southern office

serving Houston and Dallas. Mike obtained his BA in Management Information Systems from Texas Tech University and his MBA from West Texas A&M University.

Andrea Kuhn – General Manager – Midwestern Region - Andrea M. Kuhn is the General Manager of Kastle Systems' Midwestern Region. Andrea is responsible for the new business development as well as the operational success of Kastle's Chicago-based office. Andrea received her education from Bradley University in Peoria, Illinois.

Harry Choi – General Manager – Enterprise Accounts - Harry Choi is Kastle Systems' General Manager of Enterprise Accounts, a business unit dedicated to serving national enterprise clients as a single service provider from sales to support. Harry has over 15 years of domestic and international sales, operation and support experience in IT, cloud and security managed services field. Harry is a graduate of the George Washington University's Elliott School of International Affairs and University of California, San Diego.

David Fisher – General Manager – Remote Video Monitoring - Dave Fisher is the General Manager for Kastle Systems' Remote Video Monitoring division. Dave is responsible for growing Kastle's position as the leading national provider of intelligent video solutions, designed specifically for outdoor environments. Dave received his education from the University of Maryland in Mechanical Engineering and The University of Chicago's Graduate School of Business.

John Gellel – General Manger – Australia - John Gellel is the General Manager of Kastle's Australian operations. With over 20 years' experience in electronic security, John has extensive knowledge in delivering integrated security solutions across a range of corporate, government, and private industries, and regularly spends time with organizations to understand market trends and challenges. John takes an active role in the Australian security industry regulations, codes, and standards, holding a Board of Director role for Australia's peak security industry association, Australian Security Industry Association Limited (ASIAL) from 2014 to 2016, and has served as ASIAL's Vice-President since 2017.

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:

- Acceptable Use
- Access Control
- Information Technology
- Information Security
- Configuration Management
- Compliance

- User Account Management
- Incident Response
- System Security
- Security Standards
- Business Continuity
- Human Resources
- 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.