Report on Kastle Systems International LLC's Management Assertion Relating to the Managed Security Services System January 1, 2023 through December 31, 2023

INDEPENDENT SERVICE AUDITOR'S REPORT

To the Management of Kastle Systems International LLC:

Scope

We have examined Kastle Systems International LLC's ("Kastle Systems", "Kastle", or the "Company") accompanying assertion titled "Assertion of Kastle Systems International LLC's Management" ("assertion") that the controls within Kastle's Managed Security Services System ("system") were effective throughout the period January 1, 2023 through December 31, 2023, 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.

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

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, 2023 through December 31, 2023, 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
Dresher, Pennsylvania
March 14, 2024

Assertion of Kastle Systems, LLC's Management

We are responsible for designing, implementing, operating, and maintaining effective controls within Kastle's Managed Security Services System ("system") throughout the period January 1, 2023 through December 31, 2023, 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, 2023 through December 31, 2023, 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, 2023 through December 31, 2023, to provide reasonable assurance that Kastle's service commitments and system requirements were achieved based on the applicable trust services criteria.

Kastle Systems, LLC
March 14, 2024

Kastle Systems, LLC's Description of the Boundaries of its Managed Security Services System

Background

Kastle Systems has been a leader in the security industry for more than 50 years with new and advanced security solutions. 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 assessment of each client's unique environment and situation. Kastle partners with manufacturers in the security industry and build open, standardized systems suited to each client.

Kastle's Managed security services system includes a team of operators that work in the centers 24/7, responding to signals that are reported to client administrators. Kastle takes responsibility for security procedures, database management, and reporting on trends and events. Account managers work as the main point of contact, while tools and organization ensure that Kastle can provide assistance to clients. 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'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 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. 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 allows clients to 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.

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 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. Kastle's team of operators receive extensive training in advanced technology and innovative solutions.

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 third-party 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 each of these five components comprising Kastle's Managed security services system and other relevant aspects of Kastle's control environment, risk assessment process, information and communication systems, and monitoring controls.

Infrastructure

Kastle Systems is headquartered in Falls Church, Virginia. Kastle Systems also has offices throughout the United States and 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. Kastle Systems has services hosted in AWS and Microsoft Azure East with disaster recovery in AWS and Microsoft Azure West.

Software
The following web-based applications are provided to customers:

- MyKastle
- Kastle Multifamily
- Essence

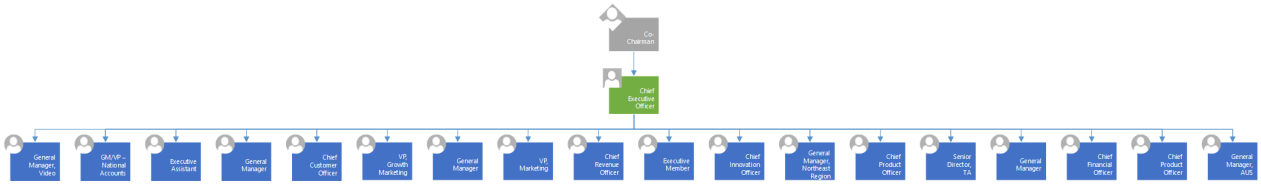
The coding languages used by customer-facing web applications is C#, JavaScript, and SQL for the data layer. The code is hosted in our private bitbucket cloud repository.

There are number other applications used day-to-day by internal Kastle employees that fall under the following general categories:

- Internal business processes (Microsoft Dynamics CRM, Dynamics AX, Microsoft Office)
- Operational administration core business functions (Kastle Direct, NED, KastleTree, Class/type/priority, CAP, epmonitor)
- Operations Center (CATS, Platypus, Superscreen, disregarder)

People

The following organizational chart provides a high-level overview of the internal structure at Kastle:



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 30-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 $3 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 30 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.

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.

Todd Burner - Chief Product Officer Todd Burner is the Chief Product Officer for Kastle Systems International and is responsible for ensuring short- and long-term revenue growth by setting product strategy, pricing, and go-to-market strategy for new and existing offerings.

Mark Rosenthal – Chief Revenue Officer – Mark Rosenthal is the Chief Revenue Officer of Kastle. He leads the nationwide sales organization with responsibility for driving sales growth and maximizing revenue for the family of brands. Mark has a track record of strong leadership with more than 20 years of success in technology and digital media sales for some of the most successful companies in the industry.

Mohammad Soleimani – Chief Innovation Officer - Mohammad Soleimani is Kastle's Chief Innovation Officer, recently advancing to this role after fourteen years serving as Kastle's Chief Technology Officer. As CTO, Mohammad was responsible for all aspects of Kastle's development and IT efforts that transformed the business to become the leading cloud-based smart access security technology provider nationally. This new role enables Mohammad to focus on leading Kastle's efforts to develop the next generation access control platform, building on his leadership roles in industry governing groups such as Physical Security Interoperability Alliance (PSIA) and Connectivity Standards Alliance (CSA) to ensure access credentials can be used seamlessly across disparate buildings and tenant spaces.

Ameet Amin – General Manager – Northeastern Region – Ameet Amin is the General Manager of Kastle Systems Northeast and is responsible for growth, leadership, operational excellence, and customer success across the Kastle Systems, Mutual Security Services, and Stat Land Security Services brands. Ameet brings over 20 years of real estate experience growing real estate technology startups, commercial real estate investment management startups, and investment banking businesses.

Bob Cutting – General Manager – West Region – Bob Cutting is General Manager of Kastle's West region responsible for growth, leadership, operational excellence, and customer success. Bob initially joined Kastle Systems' product management team in 2016 to lead multiple mobile platform initiatives, and eventually moved into leadership roles as VP of Operations. He is an experienced operations and product strategy leader, working the past 20 years with several computer vision and other technology companies bringing innovation to market, primarily in the security, business intelligence, IoT, and smart building spaces.

Adam Joseph – General Manager – Southern Regions – Adam Joseph is the General Manager of Kastle Systems Mid-Atlantic and South-East. He joined the organization in 2019 and is responsible for growth, leadership, operational excellence, and customer success across the Kastle Systems and Urban Alarm brands. He has extensive operating experience as a senior executive and advisor in both private-equity and public market companies and an innovator in developing managed technology services for various business to business enterprises. Previously, Mr. Joseph established a reputation for delivering service and technology excellence at scale across multiple industries.

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. A native of the Chicago area. Andrea began her career with Kastle in 2005. After directing the National Accounts program, Andrea was promoted to run the Chicago operations, and more recently, to assume the responsibility for the region's growth.

Allan Preziosi - General Manager – Philadelphia – Allan Preziosi is responsible for regional sales, operations and development for Kastle's Philadelphia office. In addition to Pennsylvania, the Philadelphia office serves the southern half of New Jersey and the northern half of Delaware. Allan joined Kastle in 2013 as the Client Care Manager responsible for client retention but quickly assumed oversight of the Operations Center and EPL departments. He played a major role in introducing Kastle's multifamily products to the Philadelphia office and acted as the project executive for major installations. He has degrees from the American University in D.C. (BA) and the University of Miami (JD).

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.

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 from 2017-2021 and is the current ASIAL President.

Nik Gagvani – General Manager – Video Services – Nik Gagvani, Ph.D. is responsible for the launch and continued growth of Kastle's managed video services since 2013. As part of his role, he runs the Outside Video and CheckVideo business units. Nik also leads development of Kastle's video products and supports video initiatives across other business units and verticals. Nik has played a founding or leading role at multiple companies seamlessly bridging business development, technology and operations.

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

Kastle receives some personal identifiable information (first name, last name, email address) as part of its service offerings.

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.