REPORT ON EVERBRIDGE, INC.'S CRITICAL EVENT MANAGEMENT PLATFORM RELEVANT TO SECURITY, AVAILABILITY AND CONFIDENTIALITY FOR THE PERIOD OCTOBER 1, 2017 TO SEPTEMBER 30, 2018

SOC 3® - SOC for Service Organizations: Trust Services Criteria for General Use Report

TABLE OF CONTENTS

SECTION 1

Independent Service Auditor's Report....................3

SECTION 2

Assertion of Everbridge, Inc. Management....................6

SECTION 3

Everbridge, Inc.’s Description of the Boundaries of Its Critical Event Management Platform....................8

SECTION 1

INDEPENDENT SERVICE AUDITOR’S REPORT

INDEPENDENT SERVICE AUDITOR’S REPORT

To: Everbridge, Inc. (“Everbridge”)

Scope

We have examined Everbridge’s accompanying assertion titled “Assertion of Everbridge, Inc. Management” (assertion) that the controls within Everbridge’s Critical Event Management Platform (system) were effective throughout the period October 1, 2017 to September 30, 2018, to provide reasonable assurance that Everbridge’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 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (2016).

Service Organization’s Responsibilities

Everbridge 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 Everbridge’s service commitments and system requirements were achieved. Everbridge has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Everbridge 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 Everbridge’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 Everbridge’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 Everbridge's Critical Event Management Platform were effective throughout the period October 1, 2017 to September 30, 2018, to provide reasonable assurance that Everbridge's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Coalfire Controls LLC

Westminster, Colorado
December 11, 2018

SECTION 2

ASSERTION OF EVERBRIDGE, INC. MANAGEMENT

Assertion of Everbridge, Inc. Management

We are responsible for designing, implementing, operating, and maintaining effective controls within Everbridge, Inc.'s (Everbridge's) Critical Event Management Platform (system) throughout the period October 1, 2017 to September 30, 2018, to provide reasonable assurance that Everbridge'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 Section 3 of 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 October 1, 2017 to September 30, 2018, to provide reasonable assurance that Everbridge'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 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (2016)*. Everbridge'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. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Section 3 of this report.

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 October 1, 2017 to September 30, 2018, to provide reasonable assurance that Everbridge's service commitments and system requirements were achieved based on the applicable trust services criteria.

Everbridge, Inc.

SECTION 3

EVERBRIDGE, INC.'S DESCRIPTION OF THE BOUNDARIES OF ITS CRITICAL EVENT MANAGEMENT PLATFORM

COMPANY BACKGROUND

Everbridge, Inc. (“Everbridge”, “the Company”) (NASDAQ: EVBG) is a global software company that provides enterprise software applications that automate and accelerate organizations’ operational response to critical events in order to keep people safe and businesses running. During public safety threats such as active shooter situations, terrorist attacks, or severe weather conditions, as well as critical business events including IT outages, cyber-attacks or other incidents such as product recalls or supply-chain interruptions, over 4,200 global customers rely on the company’s Critical Event Management Platform to quickly and reliably aggregate and assess threat data, locate people at risk and responders able to assist, automate the execution of pre-defined communications processes through the secure delivery to over 100 different communication devices, and track progress on executing response plans. The company’s platform sent over 2 billion messages in 2017 and offers the ability to reach over 500 million people in more than 200 countries and territories, including the entire mobile populations on a country-wide scale in Sweden, the Netherlands, the Bahamas, Singapore, Greece, Cambodia, and a number of the largest states in India. The company’s critical communications and enterprise safety applications include Mass Notification, Incident Management, Safety Connection™, IT Alerting, Visual Command Center®, Community Engagement™ and Secure Messaging. Everbridge serves 9 of the 10 largest U.S. cities, 9 of the 10 largest U.S.-based investment banks, all 25 of the 25 busiest North American airports, six of the 10 largest global consulting firms, six of the 10 largest global auto makers, all four of the largest global accounting firms, four of the 10 largest U.S.-based health care providers and four of the 10 largest U.S.-based health insurers. Everbridge is based in Boston and Los Angeles with additional offices in Lansing, San Francisco, Beijing, Bangalore, Kolkata, London, Munich, Oslo, Stockholm and Tilburg.

OVERVIEW OF SERVICE PROVIDED

Since inception, the Software-as-a-Service (SaaS)-based Everbridge Critical Event Management (CEM) Platform (“the Platform”) was architected on a single code base to deliver multi-tenant capability and the speed, scale, and resilience necessary to communicate globally when a critical event occurs. The CEM platform is designed to address both the emergency and operational components of a critical event and communications program. The CEM platform is capable of providing event collaboration and orchestration along with two-way communications and verified delivery in accordance with customers' escalation policies. The CEM platform has multi-modal communications reach, including redundant global SMS and voice delivery capabilities, and is designed to comply with local, technical, and regulatory requirements.

THE COMPONENTS OF THE SYSTEM USED TO PROVIDE THE SERVICES

THE BOUNDARIES OF THE SYSTEM

This report includes the Everbridge CEM platform SaaS solution. Any other Everbridge services are not included within the scope of this report.

The boundaries of the system are the specific aspects of the Company’s infrastructure, software, people, procedures, and data necessary to provide its services and that directly support the services provided to customers. Any infrastructure, software, people, procedures and data that indirectly support the services provided to customers are not included within the boundaries of the system.

INFRASTRUCTURE

To provide scalable and global solutions, Everbridge employs redundant and diverse production implementations and has built the CEM platform infrastructure in multiple SSAE 18 SOC 2/ISAE 3402 compliant data center facilities in North America and Europe. Within each data center, Everbridge utilizes a virtual private cloud architecture that allows the Company to enable "on-demand" capacity and performance. Everbridge's virtual private cloud architecture enables its customers to select the location in which to store their contact data, allowing for compliance with local and international data privacy laws. The architecture also enables the CEM platform to dynamically determine the best location from which to deliver critical event and communication management on behalf of customers and solves many international communications delivery challenges by utilizing in-country or in-region telephony, messaging, and data communication providers. The Everbridge CEM platform infrastructure is continuously maintained and monitored by dedicated engineers based in fully redundant Global Operations Centers located in Los Angeles, CA and Boston, MA, United States.

SOFTWARE

Everbridge's CEM platform delivers reliable enterprise-ready applications that support the visualization, orchestration, communication, and collaboration capabilities required to ensure operational resiliency to keep people safe and business running.

The CEM platform applications include:

- **Mass Notification** — a secure, scalable, and reliable mass notification platform application which enables enterprises and governmental entities to send contextually aware notifications to individuals or groups to keep them informed before, during, and after critical events. This application provides analytics, map-based targeting, flexible group management, distributed contact data, language localization, multiple options for contact data management, and a globally-optimized approach to voice and SMS routing.
- **Incident Management** — an incident management platform application that enables organizations to automate workflows and make their communications contextually relevant using drag and drop business rules to determine who should be contacted, how they should be contacted, and what information is required. This application also supports cross-account collaboration and situational intelligence sharing during crises for corporations and communities.
- **IT Alerting** — an IT alerting application which enables IT professionals to alert and communicate with key members of their teams during an IT incident or outage, including during a cyber security breach. The application integrates with IT service management platforms and uses automatic escalation of alerts, on-call scheduling, and mobile alerting to automate manual tasks and keep IT teams collaborating during an incident. This application also provides shift calendars with integrated on-call notifications to help users better manage employee resources in order to get the right message to the right person at the right time through automated staffing.
- **Safety Connection** — with an increasingly mobile workforce, distributed teams and large campuses, this platform application helps businesses and organizations quickly locate and communicate with their people. Safety Connection aggregates geo-location data from multiple systems so that you can reach out to those who are potentially at risk (employees, contractors, visitors).
- **Visual Command Center** — this visualization and orchestration application of the platform helps organizations aggregate risk data and drive a coordinated response. The application serves as the backbone for the command centers of some of the largest organizations in the world,

dynamically displaying threat intelligence and data related to business operations, continuity, security, and the supply chain.

- **Care Converge (Secure Messaging)** — a comprehensive clinical communications platform application that helps healthcare organizations coordinate with clinical staff in seconds for all-hands clinical emergencies, as well as day-to-day communications such as shift coverage and patient transitions.
- **Community Engagement** — a community engagement application which integrates emergency management and community outreach by providing local governments with a unified solution to connect residents to both their public safety department, public information resources, and neighbors via social media and mobile applications. This platform application improves the communication reach for emergency personnel, while providing residents with real-time emergency and community information, and allows residents to anonymously opt-in and provide tips.

PEOPLE

Everbridge's operational functions are organized into the following departments:

- **The SaaS Operations team** includes site and database reliability engineers, service quality analysts, and security engineers which collectively are responsible for maintaining the availability, confidentiality, and integrity of all information systems within the Platform.
- **The Network Operations Center (NOC) team** includes systems engineers which monitor the Everbridge solutions for availability and performance on a 24x7x365 basis from fully redundant NOCs located in Boston and Los Angeles.
- **The Customer Technical Support (TS) team** interfaces directly with customers during the onboarding and training process. The TS team is responsible for promptly addressing customer issues.
- **The Software Development team** creates quality solutions that meet the business needs, maintain existing software components, support IT operations, and commit to continuous improvements.
- **Quality Assurance** utilizes several methodologies of testing to ensure the highest quality product is being delivered.
- **The Product Management team** is responsible for determining the strategy for the Product Portfolio based on the Everbridge organization's business goals, and for collecting and prioritizing system enhancements and discovered defects and defining requirements for approved projects.
- **The Information Security team** is responsible for ensuring integrity, availability, and confidentiality of customer data are protected at every stage in product lifecycle and across all company processes.

PROCEDURES

Everbridge's operational service procedures are based on the Information Technology Infrastructure Library (ITIL). These ITIL based procedures for service management are divided into procedures for the management of problems, incidents, service levels, availability, capacity, supplier, change/configuration, asset, and deployment.

DATA

Everbridge’s customers can use the Everbridge CEM platform to visualize, orchestrate events, and send notifications to recipients where the content of the notification or message is completely determined by the customer. For message recipients, the Everbridge CEM platform stores and processes the contact data for each recipient. The recipient contact data may be classified as Personally Identifiable Information (PII). This information may include: first name, last name, address, phone numbers (home, work, mobile, etc.), email addresses, fax, and pager numbers as well as contact attributes associated with communication preferences, language spoken, technical certifications, on-call status, etc.

The Company has deployed secure methods and protocols for transmission of confidential and/or sensitive information over public networks. Databases housing sensitive customer data are encrypted at rest.

COMMITMENTS AND SYSTEM REQUIREMENTS

COMMITMENTS

Commitments are declarations made by management to customers regarding the performance of the CEM Platform. Standardized commitments are communicated to every customer and are included in the Company’s Master Services Agreement, which includes the following commitments to:

- Implement appropriate technical and organizational measures to protect client data from accidental or unlawful destruction, and loss, alteration, unauthorized disclosure of, or access to the data (a “Security Incident”). Such measures shall include the encryption of personal data, the ability to ensure the ongoing confidentiality and availability of services, etc.
- 99.99% Platform availability
- 24x7x365 technical support availability
- Not disclose any confidential information to any person or entity other than the representatives of the Company who have a need to know such information in the course of the performance of their duties.

The Company provides an external-facing support system and contact information to allow users to report system information on failures, incidents, concerns, and other complaints to appropriate personnel. The Company notifies customers of critical changes that may affect their processing.

SYSTEM REQUIREMENTS

System requirements are specifications regarding how the CEM platform should function to meet the Company’s commitments to customers. Requirements are specified in the Company’s policies and procedures, which are available to all employees. The Company’s system requirements include the following:

- Employee provisioning and deprovisioning standards
- Logical access controls such as use of user IDs and passwords to access systems
- Risk assessment standards
- Change management controls
- Monitoring controls

AVAILABILITY

The availability principle refers to the accessibility of the system or services as committed by the Company's master service agreement. The availability of Everbridge's CEM platform is dependent on many aspects of the Company's operations. The risks that would prevent the Company from meeting its availability commitments and requirements are diverse. Availability includes consideration of risks during normal business operations, during routine failure of elements of the system, as well as risks related to the continuity of business operations during a natural or man-made disaster.

The Company has designed its controls to address the following availability risks:

- Insufficient processing capacity
- Insufficient Internet response time
- Loss of processing capability due to a power outage
- Loss of communication with user entities due to a break in telecommunication services
- Loss of key processing equipment, facilities, or personnel due to a natural disaster

Availability risks are addressed through the use and testing of various monitoring tools, replication setup, and backup and disaster recovery plans and procedures.

In evaluating the suitability of the design of availability controls, the Company considers the likely causes of data loss, the commitments and requirements related to availability, the timeliness of back-up procedures, the reliability of the back-up process, and the ability to restore backed-up data. In evaluating the design of data availability controls, the Company considers that most data loss does not result from disasters but, rather, from routine processing errors and failures of system elements.

CONFIDENTIALITY

The confidentiality principle refers to the protection of customer information as committed by the Company's master service agreement. The confidentiality of Everbridge's CEM platform is dependent on many aspects of the Company's operations. The risks that would prevent the Company from meeting its confidentiality commitments and requirements are diverse. The Company has designed its controls to address both internal and external confidentiality risks specifically related to protection from improper use and disclosure (including monitoring of vendor services), as well as the proper retention and disposal of confidential customer information.

Confidentiality risks are addressed through policies/procedures related to the use, retention, and disposal of confidential data, data classification policies/procedures, network segmentation, information sharing agreements, remote access and transmission restrictions, and vendor risk assessments.

In evaluating the suitability of the design of confidentiality controls, the Company considers the likely causes of improper disclosure or handling of confidential information, and the commitments and requirements related to confidentiality.