REPORT ON EVERBRIDGE, INC.'S CRITICAL EVENT MANAGEMENT PLATFORM RELEVANT TO SECURITY, AVAILABILITY AND CONFIDENTIALITY THROUGHOUT THE PERIOD APRIL 1, 2019 TO MARCH 31, 2020

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

COALFIRE CONTROLS

TABLE OF CONTENTS

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 April 1, 2019 to March 31, 2020, 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 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

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 April 1, 2019 to March 31, 2020, 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.

RESTRICTED USE

Certain complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Everbridge, to achieve Everbridge's service commitments and system requirements based on the applicable trust services criteria. Users of this report should have sufficient knowledge and understanding of complementary user entity controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.

Certain complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Everbridge, to achieve Everbridge's service commitments and system requirements based on the applicable trust services criteria. Users of this report should have sufficient knowledge and understanding of complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements. Everbridge uses Amazon Web Services (AWS) as an infrastructure-as-a-service (IaaS) provider. Users of this report should obtain the relevant AWS SOC 2 or SOC 3 reports.

Coalfire Controls LLC

Westminster, Colorado
June 3, 2020

SECTION 2

ASSERTION OF EVERBRIDGE, INC. MANAGEMENT

Assertion of Everbridge, Inc. ("Everbridge") Management

We are responsible for designing, implementing, operating and maintaining effective controls within Everbridge's Critical Event Management Platform (system) throughout the period April 1, 2019 to March 31, 2020, 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 attachment A 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 April 1, 2019 to March 31, 2020, 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 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*). 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 attachment B.

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 April 1, 2019 to March 31, 2020, to provide reasonable assurance that Everbridge's service commitments and system requirements were achieved based on the applicable trust services criteria.

Everbridge, Inc.

ATTACHMENT A

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

TYPE OF SERVICES PROVIDED

Everbridge, Inc. (“the Company”) 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 Information Technology (IT) outages, cyber-attacks or other incidents, such as product recalls or supply-chain interruptions, over 5,200 global customers rely on Everbridge’s Critical Event Management (CEM) Platform (“the CEM 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 critical communications and enterprise safety applications include Mass Notification, Incident Management, Safety Connection™, IT Alerting, Visual Command Center®, Risk Center, Care Converge, Public Warning, Crisis Management, and Community Engagement™.

Since inception, the software-as-a-service (SaaS)-based CEM Platform was architected 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 short message service (SMS) and voice delivery capabilities, and is designed to comply with local, technical, and regulatory requirements.

The boundaries of the system in this section of the report details the Everbridge CEM Platform, deployed independently both in North America and in Europe. Any other Company services are not within the scope of this report.

THE BOUNDARIES OF THE SYSTEM USED TO PROVIDE THE SERVICES

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.

The components that directly support the services provided to customers are as follows:

INFRASTRUCTURE

To provide scalable and global solutions, the Company employs redundant and diverse production implementations and has built the CEM Platform infrastructure in multiple infrastructure-as-a-service (IaaS) provider facilities in North America and Europe. Within each facility, the Company utilizes a virtual private cloud architecture that allows the Company to enable on-demand capacity and performance. The Company'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 CEM Platform infrastructure is continuously maintained and monitored by dedicated engineers based in fully redundant Global Operations Centers (GOCs) located in Los Angeles, CA and Boston, MA.

SOFTWARE

The Company'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 businesses running.

The CEM Platform applications include:

- **Mass Notification** — a secure, scalable, and reliable mass notification platform application that 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.
- **Crisis Management** — optimizes customers' critical event response by orchestrating all crisis activities, teams, resources, and communications in one application. With all stakeholders – from responders in the field to executives in the boardroom – working from a common operating picture, customers can be assured that their plans are executed.
- **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 that enables IT professionals to alert and communicate with key members of their teams during an IT incident or outage, including during a cybersecurity 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 organizations can reach out to those who are potentially at risk (employees, contractors, visitors).
- **Visual Command Center** — this visualization and orchestration application of the CEM 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.
- **Risk Center** — this risk intelligence and situational awareness application of the Platform combines thousands of the most trustworthy data sources with an experienced team of analysts to empower organizations to proactively monitor and mitigate risk. Built on the Visual Command Center platform, the solution leverages powerful visualization tools and hyper-local risk intelligence from the Risk Intelligence Monitoring Center (RIMC) to provide situational awareness and help organizational functions such as security, business continuity, supply chain, and operations mitigate or eliminate the impact of risk.

- **Care Converge** — 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 that 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.
- **Mobile Applications** — two separate mobile applications – one for residents and employees, and one for critical event managers – enables customers to ensure they can initiate critical communications while mobile, and their recipients can also be reached no matter their location.

The following tools are used to support the CEM platform:

- Infrastructure Monitoring Tools
- Configuration Management Tools
- Log Monitoring Tools
- Governance, Risk and Compliance (GRC) Management Solution
- Antivirus Tools
- Backup/Replication Software
- File Integrity Monitoring Tools
- Vulnerability Scanning Tools
- Intrusion Detection Tools

PEOPLE

The Company develops, manages, and secures the CEM Platform via separate departments. The responsibilities of these departments are defined below:

- **The SaaS Operations team** includes site and database reliability engineers, service quality analysts, and security engineers, who collectively are responsible for maintaining the availability, confidentiality, and integrity of all information systems within the CEM Platform.
- **The Global Network Operations Center (GOC) team** includes systems engineers who monitor the Company's solutions for availability and performance on a 24x7x365 basis from fully redundant GOCs located in Boston, MA, and Los Angeles, CA.
- **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, maintains existing software components, supports IT operations, and commits to continuous improvements.
- **Quality Assurance** utilizes several methodologies of testing to ensure the highest quality product is being delivered.
- **The Product Management team** determines the strategy for the Product Portfolio based on the Company's business goals and is responsible for collecting and prioritizing system enhancements and discovered defects and defining requirements for approved projects.

- **The Information Security team** ensures integrity, availability, and confidentiality of customer data are protected at every stage in the product lifecycle and across all Company processes.

PROCEDURES

The Company'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

The Company's customers can use the 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 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 or sensitive information over public networks. Databases housing sensitive customer data are encrypted at rest.

ATTACHMENT B

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Commitments are declarations made by management to customers regarding the performance of the CEM Platform. Commitments are communicated in the Company's Master Service Agreement.

System requirements are specifications regarding how the CEM Platform should function to meet the Company's principal commitments to user entities. System requirements are specified in the Company's policies and procedures, which are available to all employees.

The Company's principal service commitments and system requirements include the following:

Trust Services Category	Service Commitments	System Requirements
Security	• Implementing appropriate technical and organizational measures to protect client data from accidental or unlawful destruction, 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. • Implement measures to remedy or mitigate effects of a security incident and keep client informed of all developments of such an event.	• 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.
Availability	• 99.99% platform availability. • 24x7x365 technical support availability. • Implement measures to remedy or mitigate effects of an availability incident and keep client informed of all developments of such an event.	• Monitoring controls • Backup and recovery standards
Confidentiality	• Not disclosing 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. • Upon any termination of services, Everbridge shall continue to maintain the confidentiality of the Disclosing Party's Confidential Information and, upon request and to the extent practicable, destroy all materials containing such Confidential Information. • Notify customer if Everbridge becomes aware of a breach of confidentiality.	• Data classification • Retention and destruction standards