Report on Everbridge, Inc.'s Critical Event Management Platform Relevant to Security, Availability, and Confidentiality Throughout the Period April 1, 2021 to March 31, 2022

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

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, 2021 to March 31, 2022, 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*).

The description of the boundaries of the system indicates that 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. The description of the boundaries of the system presents the complementary user entity controls assumed in the design of Everbridge's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Everbridge uses a subservice organization to provide Infrastructure-as-a-Service services. The description of the boundaries of the system indicates that 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. The description of the boundaries of the system presents the types of complementary subservice organization controls assumed in the design of Everbridge's controls. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

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.

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 Everbridge's Critical Event Management Platform were effective throughout the period April 1, 2021 to March 31, 2022, to provide reasonable assurance that Everbridge's service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls and complementary user entity controls assumed in the design of Everbridge's controls operated effectively throughout that period is fairly stated, in all material respects.

Coalfire Controls LLC

Westminster, Colorado
June 9, 2022

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, 2021 to March 31, 2022, 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.

The description of the boundaries of the system indicates that 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. The description of the boundaries of the system presents the complementary user entity controls assumed in the design of Everbridge’s controls.

Everbridge uses a subservice organization for Infrastructure-as-a-Service services. The description of the boundaries of the system indicates that 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. The description of the boundaries of the system presents the types of complementary subservice organization controls assumed in the design of Everbridge’s controls. The description of the boundaries of the system does not disclose the actual controls at the subservice organization.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period April 1, 2021 to March 31, 2022, 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*) if complementary subservice organization controls and complementary user entity controls assumed in the design of Everbridge’s controls operated effectively throughout that period. 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, 2021 to March 31, 2022, to provide reasonable assurance that Everbridge’s service commitments and system requirements were achieved based on the applicable trust services criteria.

Everbridge, Inc.

Elliot Mark
Senior Vice President

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 (e.g., 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 (e.g., product recalls or supply-chain interruptions), over 5,200 global customers rely on the Company’s Critical Event Management (CEM) Platform (“the CEM Platform”). The CEM Platform allows customers to quickly and reliably aggregate and assess threat data, locate both 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 CEM Platform’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.

The software-as-a-service (SaaS)-based CEM Platform delivers 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 description in this section details the CEM Platform, deployed independently 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 CEM Platform 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 CEM Platform.

The components that directly support the services provided to customers are described in the subsections below.

Infrastructure

To provide global, scalable 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 (VPC) architecture that enables on-demand capacity and performance. The Company's VPC 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.

The in-scope hosted infrastructure also consists of multiple supporting tools, as shown in the table below:

Infrastructure			
Production Tool	**Business Function**	**Operating System**	**Hosted Location**
Databases	Customer data storage	Amazon Elastic Block Store (EBS), MongoDB	Amazon Web Services (AWS)

Software

The CEM Platform delivers reliable, enterprise-ready applications that support the visualization, orchestration, communication, and collaboration capabilities required to ensure the 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**: A crisis management platform that optimizes customers' critical event response by orchestrating all crisis activities, teams, resources, and communications in one place. This application enables all stakeholders – from responders in the field to executives in the boardroom – to work from a common operating picture, allowing customers to ensure that their plans are executed.
- **Incident Management**: An incident management platform 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, and visitors).
- **Visual Command Center**: This visualization and orchestration application helps organizations aggregate risk data and drive a coordinated response. This application dynamically displays threat intelligence and data related to business operations, continuity, security, and the supply chain.
- **Risk Center**: This risk intelligence and situational awareness application 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 that helps healthcare organizations coordinate with clinical staff in seconds for all-hands clinical emergencies, as well as for 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 their public safety department, public information resources, and neighbors via social media and mobile applications. This application improves the communication reach for emergency personnel, provides 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 – enable customers to initiate critical communications while mobile and ensure their recipients can also be reached no matter their location.

Software consists of the programs and software that support the CEM Platform (operating systems [OSs], middleware, and utilities). The list of software and ancillary software used to build, support, secure, maintain, and monitor the CEM Platform includes the following applications:

Software	
Production Application	**Business Function**
Qualys, Veracode	Vulnerability scanning
MongoDB, Amazon Simple Storage Service (S3)	Backup and replication
Sumo Logic	Security information and event management (SIEM), logging system
Datadog, AlertSite,	Infrastructure monitoring
StandardFusion	Governance, Risk, and Compliance (GRC) management
Qualys	File integrity monitoring

Software	
Production Application	**Business Function**
Sophos	Antivirus
Amazon GuardDuty	Intrusion detection
SaltStack	Configuration management

People

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

People	
Group/Role Name	**Function**
SaaS Operations	Responsible for maintaining the availability, confidentiality, and integrity of all information systems within the CEM Platform.
GOC	Responsible for monitoring the Company's solutions for availability and performance on a 24/7/365 basis from fully redundant GOCs located in Boston, MA, and Los Angeles, CA.
Customer Technical Support (TS)	Responsible for promptly addressing customer issues.
Software Development	Responsible for creating quality solutions that meet business needs, maintaining existing software components, supporting IT operations, and committing to continuous improvements.
Quality Assurance	Responsible for utilizing several methodologies of testing to ensure the highest quality product is being delivered.
Product Management	Responsible for collecting and prioritizing system enhancements and discovered defects and defining requirements for approved projects.
Information Security	Responsible for ensuring that the integrity, availability, and confidentiality of customer data are protected at every stage in the product life cycle 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.

Procedures	
Procedure	**Description**
Logical Access	How the Company restricts logical access, provides and removes that access, and prevents unauthorized access.
System Operations	How the Company manages the operation of the system and detects and mitigates processing deviations, including logical security deviations.
Change Management	How the Company identifies the need for changes, makes the changes using a controlled change management process, and prevents unauthorized changes from being made.
Risk Mitigation	How the Company identifies, selects, and develops risk mitigation activities arising from potential business disruptions and the use of vendors and business partners.

Data

The Company's customers can use the CEM Platform to visualize data, 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's contact data may be classified as personally identifiable information (PII). This information may include first name, last name, address, phone numbers (e.g., home, work, mobile), email addresses, and fax and pager numbers, as well as contact attributes associated with communication preferences, language spoken, technical certifications, and on-call status.

The Company has deployed secure methods and protocols for transmission of confidential or sensitive information over public networks. Encryption is enabled for data stores housing sensitive customer data.

Complementary User Entity Controls (CUECs)

The Company's controls related to the CEM Platform cover only a portion of overall internal control for each user entity of the CEM Platform. It is not feasible for the service commitments, system requirements, and applicable criteria related to the system to be achieved solely by the Company. Therefore, each user entity's internal control should be evaluated in conjunction with the Company's controls taking into account the related CUECs identified for the specific criterion. In order for user entities to rely on the controls reported herein, each user entity must evaluate its own internal control to determine whether the identified CUECs have been implemented and are operating effectively.

The CUECs presented should not be regarded as a comprehensive list of all controls that should be employed by user entities. Management of user entities is responsible for the following:

Criteria	Complementary User Entity Controls
CC2.1	• User entities have policies and procedures to report any material changes to their overall control environment that may adversely affect services being performed by the Company according to contractually specified time frames. • Controls to provide reasonable assurance that the Company is notified of changes in: – User entity vendor security requirements – The authorized users list

Criteria	Complementary User Entity Controls
CC2.3	• It is the responsibility of the user entity to have policies and procedures to: – Inform their employees and users that their information or data is being used and stored by the Company. – Determine how to file inquiries, complaints, and disputes to be passed on to the Company.
CC6.1	• User entities grant access to the Company's system to authorized and trained personnel. • Controls to provide reasonable assurance that policies and procedures are deployed over user IDs and passwords that are used to access services provided by the Company.
CC6.4 CC7.2 A1.2	• User entities deploy physical security and environmental controls for all devices and access points residing at their operational facilities, including remote employees or at home agents for which the user entity allows connectivity.
C1.2	• Upon termination of their contract with the Company, user entities mark their confidential data as "Deleted," allowing the automated Company processes to purge the data after 30 days of contract termination. • It is the responsibility of the user entity to delete or purge their own information or data that is being used or stored by the Company.

Subservice Organization and Complementary Subservice Organization Controls (CSOCs)

The Company uses AWS as a subservice organization and as an IaaS provider. The Company's controls related to the CEM Platform cover only a portion of the overall internal control for each user entity of the CEM Platform. The description does not extend to the colocation services for IT infrastructure provided by the subservice organization.

Although the subservice organization has been carved out for the purposes of this report, certain service commitments, system requirements, and applicable criteria are intended to be met by controls at the subservice organization. CSOCs are expected to be in place at AWS related to physical security and environmental protection, as well as backup, recovery, and redundancy controls related to availability. AWS' physical security controls mitigate the risk of unauthorized access to the hosting facilities. AWS' environmental protection controls mitigate the risk of fires, power loss, climate, and temperature variabilities.

Company management receives and reviews the AWS SOC 2 report annually. In addition, through its operational activities, Company management monitors the services performed by AWS to determine whether operations and controls expected to be implemented are functioning effectively. Management also has communication with the subservice organization to monitor compliance with the service agreement, stay informed of changes planned at the hosting facility, and relay any issues or concerns to AWS management.

It is not feasible for the service commitments, system requirements, and applicable criteria related to the CEM Platform to be achieved solely by the Company. Therefore, each user entity's internal control must be evaluated in conjunction with the Company's controls taking into account the related CSOCs expected to be implemented at AWS as described below.

Criteria	Complementary Subservice Organization Controls
CC6.1	• AWS is responsible for ensuring data stores are encrypted at rest.
CC6.4	• AWS is responsible for restricting data center access to authorized personnel. • AWS is responsible for the 24/7 monitoring of data centers by closed circuit cameras and security personnel.
CC6.5 CC6.7	• AWS is responsible for securely decommissioning and physically destroying production assets in its control.
CC7.2 A1.2	• AWS is responsible for the installation of fire suppression and detection and environmental monitoring systems at the data centers. • AWS is responsible for protecting data centers against a disruption in power supply to the processing environment by an uninterruptible power supply (UPS). • AWS is responsible for overseeing the regular maintenance of environmental protections at data centers.

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 (MSA).

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.

The Company's principal service commitments and system requirements related to the CEM Platform include the following:

Trust Services Category	Service Commitments	System Requirements
Security	• The Company will implement 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"). • The Company will implement measures to remedy or mitigate the effects of a security incident and to keep the 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 • Encryption standards
Availability	• The Company will ensure 24/7/365 technical support availability. • The Company will implement measures to remedy or mitigate the effects of an availability incident and to keep the client informed of all developments of such an event.	• Monitoring controls • Backup and recovery standards
Confidentiality	• The Company will 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. • Upon any termination of services, the Company will continue to maintain the confidentiality of the customer's confidential information and, upon request and to the extent practicable, destroy all materials containing such confidential information. • The Company will notify the customer if the Company becomes aware of a breach of confidentiality. • The Company will protect the customer's confidential information in the same manner that it protects its own confidential information, but in no event using less than reasonable care.	• Data classification • Retention and destruction standards