everbridge®

REPORT ON EVERBRIDGE, INC.'S CRITICAL EVENT MANAGEMENT PLATFORM RELEVANT TO SECURITY, AVAILABILITY, AND CONFIDENTIALITY THROUGHOUT THE PERIOD APRIL 1, 2020 TO MARCH 31, 2021

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

COALFIRE®
CONTROLS

TABLE OF CONTENTS

SECTION 1

SECTION 2

ATTACHMENT A

ATTACHMENT B

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 the Critical Event Management Platform (system) were effective throughout the period April 1, 2020 to March 31, 2021, 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.

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 the Critical Event Management Platform were effective throughout the period April 1, 2020 to March 31, 2021, 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 2, 2021

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 the Critical Event Management Platform (system) throughout the period April 1, 2020 to March 31, 2021, 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, 2020 to March 31, 2021, 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, 2020 to March 31, 2021, to provide reasonable assurance that Everbridge’s service commitments and system requirements were achieved based on the applicable trust services criteria.

Everbridge, Inc.

DocuSigned by:

Sonia E Arista

3BF4335FD233402...

Sonia E Arista

VP / Chief Information Security Officer and Compliance

ATTACHMENT A

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

TYPE OF SERVICES PROVIDED

Everbridge, Inc. (“Everbridge” or “the Company”) is a global software company that provides enterprise software applications that automate and accelerate organizations’ operational response to critical events to Keep People Safe and Businesses Running™. During public safety threats (e.g., active shooter situations, terrorist attacks, or severe weather conditions) or critical business events (e.g., information technology [IT] outages, cyberattacks, or other incidents such as product recalls or supply chain interruptions), over 5,600 global customers rely on the Company’s Critical Event Management Platform (“CEM Platform”). The CEM Platform quickly and reliably aggregates and assesses threat data, locates people at risk and responders able to assist, automates the execution of pre-defined communications processes through secure delivery to over 100 communication modalities, and tracks progress on executing response plans. Everbridge is based in Boston, MA, USA with additional offices in 20 cities around the globe.

The Company’s critical communications and enterprise safety applications include Mass Notification, Incident Management, Safety Connection™, IT Alerting, Visual Command Center®, Risk Center, CareConverge, Control Center, 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 provides 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 description of 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 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 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 network operations centers (GNOCs) 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 CEM 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 Everbridge's Risk Intelligence Monitoring Center (RIMC) to provide situational awareness and help organizational functions such as security, business continuity, supply chain, and operations to mitigate or eliminate the impact of risk.
- *CareConverge*: 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 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, provides residents with real-time emergency and community information, and allows residents to anonymously opt-in and provide tips.
- *Mobile Applications*: Two mobile applications—one for residents and employees, and one for critical event managers—enable customers to ensure that they can initiate critical communications while mobile and that their recipients can also be reached no matter their location.
- *Control Center*: This security integration platform correlates events from disparate safety and security systems into a common operating picture, to focus people's attention on the relevant physical security management issues at hand. The platform provides users with actionable alerts, next step actions, and automated reporting to better manage risks, ensure compliance with operating procedures, and support business continuity.

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:

- *Infrastructure Monitoring*: The Company uses Datadog and AlertSite to monitor IT infrastructure availability and performance.
- *Configuration Management*: The Company utilizes SaltStack for configuration management.
- *Log Monitoring*: The Company utilizes Sumo Logic for log monitoring.
- *Governance, Risk and Compliance (GRC) Management Solution*: The Company utilizes ZenGRC for GRC management.
- *Antivirus*: The Company utilizes Sophos for antivirus purposes.
- *Backup/Replication Software*: The Company uses automatic MongoDB scripts to back up data and stores the data in Amazon Simple Storage Service (Amazon S3) buckets.
- *File Integrity Monitoring*: The Company utilizes Qualys for file integrity monitoring.
- *Vulnerability Scanning*: The Company utilizes Qualys, AWS ECR, and Veracode for vulnerability scanning.
- *Intrusion Detection*: The Company utilizes Amazon GuardDuty for intrusion detection.

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 **GNOC team** includes systems engineers who monitor the Company's solutions for availability and performance on a 24/7/365 basis, from fully redundant GNOCs 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 Customer TS team is responsible for promptly addressing customer issues.
- The **Software Development team** creates quality solutions that meet business needs, maintains existing software components, supports IT operations, and commits to continuous improvements.
- The **Quality Assurance team** 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, collects and prioritizes system enhancements and discovered defects, and defines requirements for approved projects.
- The **Information Security and Compliance team** is responsible for **e**nsuring 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 IT Infrastructure Library (ITIL). These ITIL-based procedures for service management are divided into procedures for the management of problems, incidents, service levels, availability, capacity, suppliers, change/configuration, assets, and deployment.

DATA

The Company's customers can use the CEM Platform to visualize and orchestrate events and send notifications or messages whose content is completely determined by the customer. The CEM Platform stores and processes each recipient's contact data, which 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, 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 on databases 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
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 CC6.4 CC7.2 A1.2	• User entities grant access to the Company's system to authorized and trained personnel. • 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.
CC6.6	• 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.
C1.2	• User entities have policies and procedures that specify that upon termination of their contract with the Company, user entities mark their confidential data as "Deleted" in the customer portal. This allows the automated Company processes to purge the data 30 days after 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 Amazon Web Services (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.

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 keep clients informed of all developments of such an event.	• Employee provisioning and deprovisioning standards • Logical access controls, such as the use of user IDs and passwords to access systems • Risk assessment standards • Change management controls
Availability	• 24/7/365 technical support availability. • The Company will implement measures to ensure the availability of information following interruption to, or failure of, critical business processes. • The Company will have the ability to restore the availability of and access to customer data in a timely manner in the event of a physical or technical incident.	• Monitoring controls • Backup and recovery standards

Trust Services Category	Service Commitments	System Requirements
Confidentiality	• The Company shall not disclose or use any confidential information of customers, for any purpose other than performance or enforcement of the Master Services Agreement, without the customers' prior consent. • Upon any termination of services, the Company 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. • The Company will notify customers if the Company becomes aware of a breach of confidentiality.	• Data classification • Retention and destruction standards