GoTo

SOC 3®
Reporting on System and Organization Controls

A SOC 3® Type 2 Independent Service Auditor's Report on GoTo's Description of its **Unified Communications and Collaboration (UCC) System** and on the Suitability of the Design and Operating Effectiveness of its Controls Based on the Trust Services Criteria Relevant to **Security, Availability, and Confidentiality**.

Throughout the period September 1, 2022 to May 31, 2023

SOC 3 FOR SERVICE ORGANIZATIONS REPORT

September 1, 2022 to May 31, 2023

Table of Contents

SECTION 1

ASSERTION OF GOTO TECHNOLOGIES USA, INC. MANAGEMENT

ASSERTION OF GOTO TECHNOLOGIES USA, INC. MANAGEMENT

June 10, 2023

We are responsible for designing, implementing, operating, and maintaining effective controls within GoTo Technologies USA, Inc.'s ('GoTo' or 'the Company') Unified Communications and Collaboration (UCC) System throughout the period September 1, 2022 to May 31, 2023, to provide reasonable assurance that GoTo'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*, in AICPA, *Trust Services Criteria*. Our description of the boundaries of the system is presented below in "GoTo Technologies USA, Inc.'s Description of Its Unified Communications and Collaboration (UCC) System throughout the period September 1, 2022 to May 31, 2023" 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 September 1, 2022 to May 31, 2023, to provide reasonable assurance that GoTo's service commitments and system requirements were achieved based on the trust services criteria. GoTo'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 "GoTo Technologies USA, Inc.'s Description of Its Unified Communications and Collaboration (UCC) System throughout the period September 1, 2022 to May 31, 2023".

GoTo uses Amazon Web Services ('AWS' or 'subservice organization') to provide cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at GoTo, to achieve GoTo's service commitments and system requirements based on the applicable trust services criteria. The description presents GoTo's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of GoTo's controls. The description does not disclose the actual controls at the subservice organization.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary to achieve GoTo's service commitments and system requirements based on the applicable trust services criteria. The description presents the applicable trust services criteria and the complementary user entity controls assumed in the design of GoTo's controls.

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 September 1, 2022 to May 31, 2023 to provide reasonable assurance that GoTo'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 GoTo's controls operated effectively throughout that period.

Attila Torok

Attila Torok
CISO
GoTo Technologies USA, Inc.

SECTION 2

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To GoTo Technologies USA, Inc.:

Scope

We have examined GoTo Technologies USA, Inc.'s ('GoTo' or 'the Company') accompanying assertion titled "Assertion of GoTo Technologies USA, Inc. Management" (assertion) that the controls within GoTo's Unified Communications and Collaboration (UCC) System were effective throughout the period September 1, 2022 to May 31, 2023, to provide reasonable assurance that GoTo'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*, in AICPA *Trust Services Criteria*.

GoTo uses AWS to provide cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at GoTo, to achieve GoTo's service commitments and system requirements based on the applicable trust services criteria. The description presents GoTo's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of GoTo's controls. The description does not disclose the actual controls at the subservice organization. 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.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at GoTo, to achieve GoTo's service commitments and system requirements based on the applicable trust services criteria. The description presents GoTo's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of GoTo'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.

Service Organization's Responsibilities

GoTo 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 GoTo's service commitments and system requirements were achieved. GoTo has also provided the accompanying assertion (GoTo assertion) about the effectiveness of controls within the system. When preparing its assertion, GoTo is responsible for selecting, and identifying in its assertion, the applicable trust services 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 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 AICPA. 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 the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its 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.

Independence and Ethical Responsibilities

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 are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating 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 GoTo's Unified Communications and Collaboration (UCC) System were suitably designed and operating effectively throughout the period September 1, 2022 to May 31, 2023, to provide reasonable assurance that GoTo's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects, if complementary subservice organization controls and complementary user entity controls assumed in the design of GoTo's controls operated effectively throughout that period.

The SOC logo for Service Organizations on GoTo's website constitutes a symbolic representation of the contents of this report and is not intended, nor should it be construed, to provide any additional assurance.

Restricted Use

This report, is intended solely for the information and use of GoTo, user entities of GoTo's Unified Communications and Collaboration (UCC) System during some or all of the period September 1, 2022 to May 31, 2023, business partners of GoTo subject to risks arising from interactions with the Unified Communications and Collaboration (UCC) System, and those who have sufficient knowledge and understanding of the complementary subservice organization controls and 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.

This report is not intended to be, and should not be, used by anyone other than these specified parties.

A-LIGN ASSURANCE

Tampa, Florida
June 10, 2023

SECTION 3

GOTO TECHNOLOGIES USA, INC.'S DESCRIPTION OF ITS UNIFIED COMMUNICATIONS AND COLLABORATION (UCC) SYSTEM THROUGHOUT THE PERIOD SEPTEMBER 1, 2022 TO MARCH 31, 2023

OVERVIEW OF OPERATIONS

Company Background

GoTo is a provider of cloud services for the work-from-anywhere economy. GoTo's portfolio of products, such as GoTo Resolve, GoTo Connect, GoTo Meeting, Rescue and more, allow its users to work remotely, collaborate with other users, and support and manage remote computers and other Internet-enabled devices. GoTo is a global Software as a Service (SaaS) company with tens of millions of active users, more than 3,500 global employees, and approximately 2 million customers worldwide who use the Company's software as an essential part of their daily lives.

GoTo is headquartered in Boston, Massachusetts with additional locations in North America, South America, Europe, Asia, Australia, and thousands of home offices around the globe.

On August 31, 2020, GoTo, Inc. was acquired by affiliates of Francisco Partners and Evergreen Coast Capital Corp. in a take-private transaction. In February 2022, LogMeIn, Inc. rebranded to GoTo.

Description of Services Provided

The Unified Communications and Collaboration (UCC) System is designed to deliver a way for people to meet, market, and train. The in-scope products that make up the UCC System are known as GoTo Connect, which includes GoTo's Phone, Meeting and Messaging solution (collectively referred to as GoTo Connect), GoTo Meeting, GoTo Training, GoTo Webinar, GoTo Contact Center, GoTo Customer Engagement, join.me, and OpenVoice:

GoTo Connect	**GoTo Connect** is GoTo's cloud-based unified communication and collaboration solution which combines cloud VoIP phone systems, GoTo Meeting's web, audio and video conferencing and business messaging through team messaging, SMS or MMS into one simple, reliable and flexible solution. Users can meet, talk, chat, text and collaborate via a single application, accessible by web, desktop, mobile device, and by a set of Open API's. GoTo Contact Center delivers a broad set of contact center features and real-time reports to enable better management of call queues and incoming customer calls. GoTo Customer Engagement provides a centralized solution for customer conversations with outbound SMS campaigns, multi-channel team inbox and customizable surveys.
GoTo Meeting	**GoTo Meeting** is GoTo's online meeting and collaboration solution which gives users the ability to host or participate in online meetings from the GoTo Meeting website, mobile apps or executable customer software. GoTo Meeting comes equipped with integrated conference dial-in numbers, VoIP and HDFaces high-definition video conferencing. It features a secure communication architecture that uses industry-standard Transport Layer Security, or TLS, end-to-end encryption.

GoTo Training	**GoTo Training** is a secure online training product that enables individuals and enterprises to provide interactive training sessions to customers and employees in any location. GoTo Training users can create curriculums for their students from a Mac, PC, or mobile device without the need for significant training or IT support; attendees can join from a Mac, PC, iOS, or Android device. GoTo Training includes features such as full-service registration with real-time reports, materials, automated e-mail templates, polling, and survey capabilities as well as testing and high-definition webcam sharing for up to six participants and VoIP and toll-based phone options.
GoTo Webinar	**GoTo Webinar** is a do-it-yourself webinar product, allowing organizations to present online to geographically dispersed audiences. GoTo Webinar users can host, attend, or participate in a webinar session from a Mac, PC, or mobile device without the need for significant training or IT support; attendees can join from a Mac, PC, iOS, or Android device. GoTo Webinar includes features such as full-service registration with real-time reports, customized branding, automated e-mail templates, polling and survey capabilities, a webinar dashboard for monitoring attendance and participation, easy presenter controls for changing presenters and high-definition webcam sharing for up to six organizers and panelists and VoIP and toll-based phone options.
join.me	**join.me** is GoTo's lightweight online meeting and screen sharing solution which gives users the ability to host ad hoc and scheduled online meetings with other people.
OpenVoice	**OpenVoice** is a reservation-less audio-conferencing service, providing robust account tools that allows user provisioning and audio meeting controls for users to manage small and large audio conferences without operator assistance. Since OpenVoice is a reservation-less conferencing platform, as a meeting organizer you can hold meetings on your telephone without having to plan ahead.

Principal Service Commitments and System Requirements

GoTo designs its processes and procedures to meet the objectives for GoTo's UCC System. Those objectives are based on the service commitments that GoTo makes to user entities and the financial, operational, and compliance requirements that GoTo has established for the services:

- Security: GoTo documents service-specific information about GoTo's products' technical and organizational security measures (e.g., as located in the "Technical and Organizational Measures" (TOMs) documentation found at GoTo's Trust and Privacy Center at https://www.goto.com/company/trust).
- Confidentiality: GoTo maintains a global privacy and security program designed to protect Customer Content and any associated personal data that GoTo may collect and/or process.
- Availability: GoTo maintains redundancy and backup and recovery processes designed to ensure service availability.

Security, availability, and confidentiality commitments to customers (user entities) are documented in customer agreements and communicated on GoTo's websites (including, https://www.goto.com/company/legal/terms-and-conditions and https://www.goto.com/company/trust) as well as in the description of services provided online. For more information, please see an excerpt from GoTo's online Terms and Conditions:

> **4.2 Your Privacy and Security.** We maintain a global privacy and security program designed to protect your Content and any associated personal data we may collect and/or process on your behalf. You can visit our Trust & Privacy Center (https://www.goto.com/company/trust) to review applicable data processing locations and Sub-Processor Disclosures, as well as Service-specific information about our technical and organizational security measures (located in the Technical and Organizational Measures or "TOMs" documentation). When providing our Services, we act as a data processor, service provider, or the equivalent construct. To review and execute our Data Processing Addendum ("**DPA**"), please visit https://www.goto.com/company/legal.

GoTo establishes operational requirements that support the achievement of security, availability, and confidentiality commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in GoTo's system policies and procedures, system design documentation, and customer contracts. GoTo's corporate policies define an organization-wide approach to how systems and data are protected, how information and systems are maintained and made available for operation, and how GoTo meets its objectives.

This documentation includes policies around how GoTo's UCC System are designed and developed, how the system operates, how the internal business systems and networks are managed, and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the services.

Components of the System

Infrastructure

GoTo's UCC System infrastructure redundancy design includes server and database clustering, Internet Protocol (IP) and Domain Name System (DNS) load balancing, containerized services, and utilization of telecommunications carriers and Internet Service Providers (ISPs).

The UCC System are built on an infrastructure with measures and controls designed to provide high availability and, as applicable, are hosted by data center and cloud service providers.

GoTo's data center and cloud service providers either maintain ISO 27001 compliance or have current SOC 1 or SOC 2 reports which indicate compliance with the AICPA's Trust Services Criteria. They may otherwise undergo on-site assessments by GoTo, which are reviewed by the GoTo Governance, Risk, and Compliance (GRC) Team in order to ensure consistency with GoTo's vendor risk management requirements/policies.

GoTo's service architecture is designed to perform replication in near-real-time to geo-diverse locations.

GoTo's DevOps and Infrastructure Services (DOIS) group manages production servers, monitors systems, performs backups, upgrades operating systems, and manages production firewalls and system updates. The GoTo Security and Information Technology (IT) teams manage the configuration of corporate firewalls, network system security, and endpoint devices (desktops, laptops and mobile devices).

Software

The UCC System are developed by the GoTo software development staff and run on shared multi-tier architectures with network segmentation and server role assignments. The hardware and software components of the infrastructure supporting the UCC System include:

Primary Software	
Component	**Description**
Server Hardware	Virtualized cloud hardware, Infrastructure as a Service (IaaS), and GoTo-owned physical servers
Operating systems	GoTo uses macOS, Windows, and Linux
Databases	A variety of databases and database tools are used to store user account information, summary data, logs, etc.
Monitoring systems	There are multiple monitoring systems in use, including but not limited to: • Security Incident and Event Management (SIEM) • Amazon and Azure platform monitoring for each respective cloud provider • System and performance monitoring • System server logs, error logs, and security audit trails • Advanced Endpoint Protection (AEP) technology • Threat intelligence monitoring
Network infrastructure	The network infrastructure uses a common set of redundant network components: • Load balancers • Advanced Firewalls • Gateways (Network Address Translation (NAT), Internet) • Virtual Private Clouds (VPCs), subnets, routing tables • Network Access Control Lists (NACLs) and whitelisting • Network intrusion prevention system
Key Supporting Tools, Processes, and Applications	The other significant application programs and IT system software that support application programs include: • Secure Development Lifecycle, including automated application security assessment tools and composition analysis • Change Management through ticketing and workflow management • Vulnerability management • Identity and Access Management Tools - Microsoft Azure AD and SailPoint IdentityNow • Backup tools • Physical security and safety controls • Database security controls, including access control, encryption, and logging • Personnel security measures • 24/7 Security Incident Monitoring and Response • Security and privacy awareness training • Offensive security testing and remediation • Governance and risk management

People

Corporate Leadership

Management of GoTo is the responsibility of the President and Chief Executive Officer (CEO). The Executive Leadership Team responsible for daily operations includes the following:

- Chief Financial Officer (CFO)
- Chief Revenue Officer (CRO)
- Chief Technology Officer (CTO)
- Chief People Officer
- Chief Marketing Officer
- Chief Legal Counsel
- Chief Customer Officer

Information Security

The following roles are directly involved in the management, coordination, and support of information security programs and security awareness initiatives:

Chief Technology Officer (CTO). The CTO reports directly to the CEO and is responsible for evaluating and prioritizing Product, Engineering, and Security initiatives relative to overall business objectives. The Product and Technology Group (PTG) has responsibility for managing product, security and technology activities and keeping the Executive Leadership Team informed about the overall program. Departments reporting up to the CTO include: Product Operations, Product Management, Platform and Data Strategy, Security, User Experience, Product Engineering, DevOps, Identity Management, and Global Infrastructure Services.

Chief Information Security Officer (CISO). The CISO is responsible for defining the governance, risk, security, technical privacy, and compliance strategy for the organization. The CISO coordinates the alignment of the Security Program across the Company. The CISO reports directly to the CTO and manages the Security Team which consists of the following major functions:

- Security Assurance consists of Application Security and Infrastructure Security professionals. The Application Security Team is responsible for discovering, remediating, and preventing security vulnerabilities that may be introduced at various stages of the application lifecycle. This team consists of security professionals (software development engineers and architects) who promote and manage secure software development practices through ongoing training and reward programs such as the Security Champions program, which rewards members of other teams for their efforts to improve security. The Infrastructure Engineering Security Team reviews, provides guidance for, and develops pre-production prototypes for technology that implements security controls for GoTo's production infrastructure.
- Security Operations includes personnel across the globe in order to ensure coverage twenty-four (24) hours a day and seven (7) days a week. Working as a centralized team, Security Operations manages cyber security issues, such as threats to the environments and applications, escalated security issues, and critical access to systems including Corporate IT Security, the product infrastructure, and the corporate IT environment. Members of this team also provide threat intelligence based on recent vulnerabilities, indicators of compromise using different attacker methodologies, and support for the prioritization of associated remediation activities.
- Offensive Security acts as an internal security testing team to assess and validate the security of all products, infrastructure, websites, and applications. The team simulates adversary techniques and tactics and leverages full adversarial ("red team") and collaborative ("purple team") approaches. These exercises are performed in collaboration with other stakeholders across the Company in order to test and simulate specific TTPs (Tactics, Techniques and Procedures). The team also helps remediate vulnerabilities and works with other teams to improve GoTo security posture through an offensive approach.

- Governance, Risk, & Compliance (GRC) is responsible for the security policy framework, governance, supplier reviews, control design, risk assessment, and maintenance of GoTo's compliance programs. The team is composed of certified professionals with a focus on audit, risk, and technology compliance.
- Security Engagement is responsible for building and administering a comprehensive security communications and awareness program at GoTo. Core responsibilities of this function include administering annual security and privacy training, conducting awareness campaigns and events, creating security and privacy communications and collateral, providing security and privacy support to the Sales and Customer Care organizations, and coordinating a critical communications process for security and privacy.

Chief Legal Officer. The Chief Legal Officer and Legal Team manage various entity roles, including privacy, ethics, corporate governance, contract negotiation, and corporate and regulatory legal risk management, as well as legal support for mergers and acquisitions, intellectual property management, real estate and facilities.

Chief People Officer. The Chief People Officer and the Human Resources (HR) Department play an integral role in ensuring that qualified people are hired and retained to not only contribute to the enterprise's overall growth and success but also to uphold behavioral expectations that help protect GoTo, its customers, and their end users' information and intellectual property. The HR Department is responsible for employee recruiting which includes managing and facilitating background checks (as permitted by applicable law), performance management, compensation and benefits administration, and employee relations. Performance is evaluated by management semi-annually and tracked centrally by HR.

Other Functional and Operational Responsibilities. GoTo has multiple product groups that manage all of GoTo's product-specific functions which include: Product Development, Product Management, Marketing, User Experience and Business Operations. Functional and operational teams, such as Customer Care, Sales, and other groups, provide support as needed.

Key functional responsibilities include:

- Product Development. The Product Development function consists of teams that are part of a distinct product group, as well as shared teams that are part of GoTo's CTO Team. These teams are responsible for the assessment, development, testing, and implementation of product requirements. The leadership of the Product Development and Engineering Teams reports to the CTO.
- DOIS. The DOIS group is responsible for the planning, building, and managing of the infrastructure supporting the products and their associated platforms and services. DOIS teams manage Data Center Infrastructure, parts of Cloud Infrastructure, Voice Operations, and Operational Services including the Network Operations Center (NOC). DOIS leadership reports to the CTO.
- Product Management (PM) and User Experience (UX). The PM and UX functions are responsible for defining GoTo's product strategy, product roadmap and the end-to-end user experience (e.g., user interactions/usability, visual design, etc.) for GoTo products. PM and UX Teams define and prioritize specific requirements and collaborate with Product Development Teams for implementation. The PM and the UX functions report up to the CTO.
- Customer Care. The Customer Care function includes horizontal customer support functions and customer success teams. This function is responsible for managing customer issues, satisfaction, and efforts to support retention and growth. Customer Care leadership reports to the Chief Customer Officer.
- Finance. The Finance Department maintains the finances of the business through functions such as accounting, purchasing, planning, and analysis. Finance leadership reports directly to the CFO.

Data

Data Classification and Handling

GoTo's services, as outlined in this report, include the handling of electronic information submitted by or otherwise maintained on behalf of its customers within the applicable GoTo service environment. Specifically, this electronic information, defined as Content in the GoTo Terms of Service (ToS), includes any files, documents, recordings, chat logs, transcripts, and similar data that GoTo maintains on behalf of its customers and their end-users, as well as any other information a GoTo customer may upload to their service account in connection with the GoTo services (referred to as Customer Content herein). Such information is encrypted in transit and, depending upon the product, may employ additional technical measures, such as encryption at rest.

Product or suite-specific technical specifications, including applicable encryption standards and methods, may be found either on the applicable product-specific resource web pages and/or the TOMs documentation located on the GoTo Trust and Privacy Center web pages under Product Resources. This information is subject to the confidentiality controls in this report. Specifically, Customer Content shall be safeguarded through the implementation and use of administrative, technical, and physical measures designed to ensure its security, integrity, and availability. Customer Content shall be returned or deleted in accordance with the Retention, Archiving, and Disposal sections below.

Additionally, GoTo's Information Classification scheme describes pre-defined controls necessary to safeguard data in accordance with a sensitivity classification. Customer Content is considered confidential data (GoTo Confidential) and is protected according to relevant data protection controls, policies, and/or procedures.

Furthermore, connections to production applications and networks over the Internet or other public networks are encrypted. Appropriate network application safeguards are implemented to secure connections internally between production data centers. To the extent reasonable, Data Loss Prevention (DLP) software is used on corporate systems in order to reduce the likelihood that sensitive data is transported outside of the corporate network.

Retention, Archiving, and Disposal

GoTo reviews data retention and disposal policies and procedures on an ongoing basis to ensure compliance with applicable requirements. GoTo retains Customer Content in accordance with its internal policies and procedures, applicable legal and regulatory requirements, and any contractual agreements with its customers. To the extent applicable, automated retention periods for Customer Content are disclosed via the applicable TOMs located in the Product Resources section of the GoTo Trust and Privacy Center. When disposing of electronic data storage devices, GoTo evaluates against industry standard practices and internal controls to determine the appropriate approach to ensure that data destruction is irreversible. When hard drives holding Customer Content are retired, they are wiped using appropriate software and/or discs are rendered unreadable and destroyed based on industry standard practices and internal controls. Secure shred bins are located in every office to enable appropriate and secure disposal of data that is determined to be of a sensitive nature (e.g., pertaining to GoTo customers).

Processes, Policies and Procedures

GoTo maintains policies and procedures to assist in guiding business operations. The procedures include control activities designed to help ensure that operations are carried out properly, consistently, and efficiently. GoTo uses a risk management approach to select and develop these control activities. After relevant risks are identified and evaluated, in each case controls are established, implemented, monitored, reviewed, and improved when determined necessary to meet the overall objectives of the organization.

Documented information security policies, standards, and procedures are in place to guide IT and operations personnel in information security administration processes, including but not limited to, in the following key security lifecycle areas:

- Information Security Policy
- Acceptable Use Policy
- Security Standard (categories include):
    - Information Security Management:
        - Information Security Policy Management
        - Management and Ownership of Information Assets
        - Information Asset Inventory
        - Information Protection and Control
        - Information Security Awareness and Training
        - Information Disposal
        - Information Security Incident Management
        - Information Security Issue Management
    - Access Control:
        - User Access Control
        - Joiners, Movers, and Leavers
        - User Access Recertification
        - System Accounts and Privileged Accounts
        - Customer Access Control
        - Remote Access
        - Multi-Factor Authentication (MFA)
        - Supplier Access to GoTo Systems
    - Supplier Security:
        - Supplier Selection and Service Implementation
        - Supplier Contracts
        - Supplier Management
        - Supplier Contract Expiry
        - Supplier Cloud Computing Services
    - System Development Lifecycle (SDLC) Security:
        - Security Requirements for Software and Hardware Acquisition
        - Security Requirements for System Development and Maintenance
        - Security Requirements for System Design and Build
        - Security Requirements for System Testing
        - Security Requirements for System Implementation
        - Security Requirements for System Implementation for product-based systems
        - Security Requirements for Technology End of Life (EOL)
    - Application Security:
        - General Security Requirements for Applications
        - Additional Security Requirements for Payment Systems
        - Additional Security Requirements for Web-based Applications
        - Additional Security Requirements for eCommerce Applications
        - Additional Security Requirements for Mobile Applications
    - Infrastructure Security:
        - Physical and Environmental Security
        - Secure Infrastructure Build and Installation
        - Cryptography
        - Electronic Communications
        - Virtual Systems
        - Office Systems
        - Mobile Devices
        - Internet Access

        - Removable Media
    - Network Security:
        - Network Management and Design
        - External Network Connections
        - Wireless Access
        - Perimeter Defense
        - Intrusion Prevention Systems
        - Network Security Monitoring
        - Telecommunications for Corporate and Production VoIP
    - Operational Security:
        - Operational Procedures
        - Capacity Management
        - System Maintenance
        - Patch Management
        - Malware Management
        - Technical Vulnerability Management
        - GoTo System Component Disposal
        - Backup
        - Change Management
        - Information Security Investigations and Forensic Analysis
        - Security Logging and Monitoring
        - System Resilience
        - Secure Transportation

Other Governance Documentation:

- Business Continuity Management Policy
- Data Retention, Archiving, and Deletion Statement
- Privacy by Design Policy
- Risk Management Policy
- Third-party Risk Management Policy
- Security Logging Standard
- Cloud Security Standard
- Technical Privacy Standard
- Core Security Development Lifecycle (CSDL) Program Documentation
- Security Incident Response Plan
- Security Operations - Standard Operating Procedures
- Clean Desk Guidelines
- Data Classification Guidelines
- Security and Privacy Awareness Training Guidelines

Applicable policies are reviewed by management on no less than an annual basis to ensure that, where determined necessary, relevant procedures and standards are updated in accordance with contractual and legal commitments, as well as Company requirements and standards. Additionally, applicable policies, when determined necessary, are reviewed upon material changes or revisions to the relevant environment. Management posts policy updates as needed to GoTo's Intranet site and notifies employees when specified policies need to be acknowledged.

Implementation of Policies

In general, operational and functional departments are responsible for implementing policies and defining appropriate procedures. Where applicable, the Security Team supports and provides guidance to respective teams regarding the design of their procedures.

Physical Security

GoTo inherits physical security for underlying physical infrastructure via AWS, Equinix, Azure, Switch, Oracle, CoreSite, Turbobridge, and Google. Please see the "Subservice Organizations" section for controls maintained by AWS, Equinix, Azure, Switch, Oracle, CoreSite, Turbobridge, and Google.

GoTo has a physical security program in place which is designed to provide access control to global locations. The entrances to GoTo premises with network connections are secured using a transponder/badge system managed by the Facilities Team. Facilities and HR personnel manage the assignment and collection of access badges to each facility. New hires are granted access to applicable buildings as necessary for their role. Visitors at GoTo's offices worldwide are required to check in at a reception desk, sign into a visitor management system, and be escorted by GoTo personnel. Where applicable, security guards are located on-site in multi-tenant buildings.

Environmental protections have been implemented in the data centers that house production servers (GoTo production data centers) and include the following control systems, as appropriate for the relevant system:

- Heating, ventilation, and air conditioning temperature control
- Fire suppression
- Uninterruptible power supply
- Smoke detectors
- Raised floors or comprehensive cable management

GoTo contracts with subservice organizations, such as co-location data center facilities, to provide physical security and environmental controls for the GoTo production data centers. DOIS management regularly reviews access reports and logs for authorized and unauthorized access and failed access attempts. GoTo additionally has the ability to run access reports, on an ongoing and as-needed basis, through select data center portals.

Access to production data centers is limited to authorized GoTo personnel. Operations management reviews access logs for third-party hosting facilities, on no less than a quarterly basis, to verify that access was limited to only authorized individuals. A formal request process is designed to authorize and monitor access to physical data centers and are approved by DOIS.

Access to any third-party hosting facilities requires submission of a request through a ticketing system and are approved by the management of Corporate IT and/or DOIS. Access to on-premise server rooms is granted, if deemed appropriate, based on an individual's role. If an individual needs subsequent access, a ticket or e-mail are submitted to the Facilities Team with appropriate management approval and justification.

Upon termination, an automated process is executed between the HR resource management system and Corporate Active Directory (Corp AD) to terminate Corp AD access automatically in accordance with the termination date and time specified by HR. Additionally, a termination notification is automatically generated through a distribution list and is sent to system administrators for further processing and verification of access to subsequent systems. The corporate facilities security management system integrates with Corp AD and the terminated individual's badge is automatically disabled at office locations and on-premise server rooms. Access to subservice hosting provider locations is disabled by the DOIS Team, upon notice.

Logical Access

Logical access control procedures are in place and designed to prevent or mitigate the threats of unauthorized application access and data loss in corporate and production environments. Employees' access to GoTo systems, applications, networks, and devices, is subject to relevant restrictions based upon specific job function. Access to customer production data is restricted to authorized personnel and is granted solely on a "need-to-know" basis. Minimum permissible password requirements follow industry standard best practices.

GoTo employs internal tools and controls designed to manage and limit access to corporate applications containing or accessing sensitive or critical data sources. Authorized access to the corporate, application, and production environments is controlled using multi-tier authorizations, which are maintained in a central ticketing system for approval and tracking. Employee access to specified resources requires direct manager or HR approval and, in specific cases, application/data source owner approval. Employee application and data source access lists are reviewed, on at least a quarterly basis, in order to verify that current access levels for employees are authorized and appropriate for their position and that access is revoked promptly upon termination.

Logical access control policies and/or procedures, including the Information Security Policy and the Security Standard, are designed to prevent or mitigate unauthorized application access and data loss. IT, DOIS and software development management follow a set of policies and/or procedures to ensure that access to technical infrastructure is properly restricted to authorized personnel. Remote access to the Virtual Private Network (VPN) uses two-factor authentication. Two-factor authentication is also used when providing access to systems that are federated with Active Directory (AD), either internally or externally.

UCC Service production servers are maintained in a separate environment from the Corporate IT environment. Product engineering, DOIS, and engineering support functions review logical access to the production environment, on no less than a quarterly basis, to ensure that no unauthorized accounts have been added. When employee terminations are entered into the HR system, revocation of logical access to the corporate environment is processed through an automated job that disables access based on a specified date and time corresponding to the conclusion of employment. For applications dependent upon Corp AD, termination of the Corp AD account will effectively disable authentication for the application account.

Employee terminations are processed through a formal off-boarding process in which equipment, facility access cards, and logical access to critical systems are disabled by the termination date. Once an employee termination has been processed by HR, a termination ticket is created, and an automated termination notification is sent to the applicable departments to remove systems/physical access. This occurs through both automated and/or manual processes, contingent upon the level and type of access.

Data Communications

Intrusion Prevention

Intrusion Prevention Systems (IPS) are used in the Corporate IT network and specific GoTo production environments using multiple industry-standard tools. Corporate IT, DOIS, and product engineering are automatically notified of discovered intrusion attempts against the network and issues are addressed and resolved in accordance with criticality and risk. Suspicious server login activity is monitored by the Security Operations Center (SOC), and relevant identified issues are researched, documented, and resolved.

Firewalls are deployed on the Corporate IT network and production environments, and access to modify firewall settings is restricted to authorized IT and DOIS personnel. On no less than an annual basis, firewall configuration reviews are performed.

Vulnerability Management

GoTo incorporates vulnerability management programs into its production and Corporate IT environments, which include both internal and external network system scanning, dynamic code analysis, and application-level penetration testing that is performed internally, as well as externally, by qualified third-parties. Significant or critical issues discovered through such programs are reported to leadership and stakeholders for appropriate prioritization. Events and vulnerabilities may be identified through staff and customer reports, security notification channels (public or private bug bounty programs), monthly internal and external vulnerability scanning, application vulnerability testing, and penetration testing activities for targeted environments. External and internal vulnerability scans are performed on the network and the production environment at least monthly. These scanning results are reported into network monitoring tools.

Corporate IT and production environment security is monitored using multiple industry-standard technologies, and relevant incidents are reported to the SOC. Once alerts or reports are analyzed, the SOC collaborates with relevant stakeholders to resolve identified issues-reporting and analysis are tracked and documented for management review. Resolutions are tracked through a ticketing system.

Boundaries of the System

This description of GoTo's UCC System includes the design of the Company's controls relevant to security, availability, and confidentiality. This description does not include other Company or third-party service offerings which may complement, support, or access GoTo's UCC System operation(s). Compliance with laws and regulations for privacy, export or similar requirements are not included in the scope of this description.

Changes to the System Since the Last Review

There were no changes occurred to GoTo and the applicable UCC System used to provide services during the period of September 1, 2022 to May 31, 2023.

Incidents Since the Last Review

There were no identified material system incidents that were: (a) the result of controls that were not suitably designed or operating effectively; or (b) otherwise resulted in a significant failure in the achievement of one or more of GoTo's service commitments and system requirements during the reporting period September 1, 2022 to May 31, 2023, however, GoTo did disclose a security event that occurred before the audit period on November 30, 2022, which is now contained and remediated, and encourages its readers to visit its blog at https://www.goto.com/blog and GoTo's Trust and Privacy Center at https://www.goto.com/company/trust.

Criteria Not Applicable to the System

All Common Security, Availability, and Confidentiality criteria were applicable to GoTo's UCC System.

Subservice Organizations

As part of GoTo's third-party due diligence process, vendor evaluations may be performed by multiple teams, as determined necessary. The Security Team will evaluate vendors that provide information security-based services and that have access to, process, store, or transmit GoTo Information, including third-party hosting facilities. The Legal and Procurement Departments will evaluate or execute agreements, as determined necessary, such as non-disclosure agreements, data processing agreements, service contracts, etc. Where available, Service Organization Control reports (SOC 1 or SOC 2) or other compliance reports may be obtained and evaluated, to ensure that an adequately functioning control environment is in place and that any necessary user consideration controls are addressed. Third-parties hosting or otherwise granted access to the application production data are required to sign a written contract, which will include appropriate confidentiality (or equivalent) obligations.

For critical vendors that provide information security-based services, ongoing due diligence of relevant vendors occurs at least annually, in order to ensure that the security posture of identified vendors has not materially deteriorated to unacceptable levels and that the scope of the product or service has not materially changed, such as through significantly expanded or materially differing use of GoTo Information that a vendor may access, process, store, or transmit on behalf of GoTo:

Functions Performed	Subservice Organizations
Data Center and Cloud Service Providers	• Amazon Web Services (AWS) • Equinix, Inc. (Equinix) • Microsoft Azure (Azure) • Switch, Ltd. (Switch) • CoreSite Realty Corporation (CoreSite) • Oracle America, Inc. • Turbobridge, Inc. • Google Cloud
Voice-to-text transcription	• Google Cloud • GoTo VoiceAI
Call Routing	• Syniverse Technologies LLC
Call Answering	• Ruby Receptionist • Aflalo Communications, Inc.
Product Analytics	• MixPanel • Amplitude Analytics (Amplitude) • AudienceProject (UserReport)
DDoS Protection	• Akamai Technologies, Inc.
Identity and Access Management	• Microsoft Azure (Azure)
Content Delivery Network (CDN)	• Akamai Technologies, Inc. • AWS CloudFront
Logging and Monitoring	• Splunk, Inc. • Sentry.io
Payment service provider	• Stripe Inc. • PayPal • Visa (Authorize.net, CyberSource)
File upload service provider	• Filestack, Inc.
Communication Platform	• SendGrid, Inc. • Pendo.io, Inc. • Genesys DX • PubNub Inc. • DocuSign, Inc. • Twilio • Slack • Microsoft Teams • Apple (APNS) • Google (Firebase)
RTC Server Hosting	• Amazon Web Services (AWS) • Oracle America, Inc.

Functions Performed	Subservice Organizations
Call Connection	• Qunifi
Voice Carrier Network for voice traffic of VoIP and PSTN calls	• Telecommunications providers not listed on sub-processor disclosures for confidentiality
Address Validation	• SmartyStreets

Complementary Subservice Organization Controls

The following subservice organization controls have been implemented by the subservice organizations and are not included in this report to provide additional assurance that the Trust Services Criteria are met:

Controls Expected to be Implemented at the Subservice Organizations		
Category	**Criteria**	**Control**
Common Criteria / Security	CC6.1, CC6.2, CC6.3,	Policies and other relevant system documentation communicate descriptions of responsibilities and expected behavior with regard to system usage.
		Account creation and modifications are authorized by management and documented in a ticketing system.
		Production network, database server, and application server user access is revoked in a timely manner upon termination.
		Industry standard encryption algorithms are used to remotely manage production infrastructure.
		Appropriate identification and authentication are required to perform actions on the production infrastructure.
		Production network and server user accounts are reviewed by management on a quarterly basis. Suspicious accounts are investigated and resolved.
		Physical access to server rooms and secured areas within production data centers is revoked upon termination.
		Physical access to server rooms and secured areas within production data centers is reviewed by management on a quarterly basis.
		Relevant identified issues are investigated and resolved.
	CC6.4	Physical access to server rooms and secured areas within production data centers is granted based on management authorization.
		Physical access to server rooms and secured areas within production data centers is revoked upon termination.
		Physical access to server rooms and secured areas within production data centers is reviewed by management on a quarterly basis.
		Relevant identified issues are investigated and resolved.
	CC6.6, CC6.7	Industry standard encryption algorithms are used to remotely manage production infrastructure.

Controls Expected to be Implemented at the Subservice Organizations		
Category	**Criteria**	**Control**
		Remote access to the corporate network is restricted through managed VPN concentrators.
		Approved networking ports and protocols are implemented in accordance with documented production network standards.
	CC8.1	Application changes are documented and tracked in an internal ticketing system.
		Application releases into production do not occur until appropriate signoffs are obtained and documented.
		Changes to infrastructure components are subject to peer review and/or approval by management.
Availability	A1.2	Environmental protections have been implemented for GoTo designated spaces, including, as appropriate: • Fire suppression • Smoke detectors • Raised floors • CCTV monitoring • Locked entrances
Confidentiality	C1.1	The entity has processes and tools designed to ensure that confidential information will not be transmitted beyond the boundaries of the system unless otherwise authorized or provided to unauthorized user entity personnel.
		The entity establishes written policies related to retention periods for relevant confidential information it maintains. The entity, as applicable: has automated system processes in place to delete confidential information in accordance with specific retention requirements.
		The entity deletes backup information in accordance with a defined schedule.
		The entity requires approval for access to confidential information.
		The entity classifies information to be retained beyond its retention period and specifically marks such information for retention.
	C1.2	The entity reviews information marked for retention annually.
		The entity locates and removes or redacts specified confidential information as required.
		The entity regularly and systematically destroys, erases, or makes anonymous specified confidential information that is no longer required for the purposes identified in its confidentiality commitments or system requirements.
		The entity erases or destroys specified records in accordance with applicable retention policies, regardless of the method of storage (for example, electronic, optical media, or paper based).

Controls Expected to be Implemented at the Subservice Organizations		
Category	**Criteria**	**Control**
		The entity disposes of original, archived, backup, and ad hoc or personal copies of records in accordance with applicable destruction policies documents the disposal of confidential information.

GoTo management, along with the subservice organizations, define the scope and responsibility of the controls necessary to meet all the relevant Trust Services Criteria through written contracts, such as service level agreements. In addition, GoTo performs monitoring of the subservice organization controls, including the following procedures:

- Reviewing completed attestation reports over services provided by vendors and subservice organizations
- Monitoring external communications, such as customer complaints relevant to the services provided by the subservice organizations

COMPLEMENTARY USER ENTITY CONTROLS

GoTo's system was designed with the assumption that certain controls will be implemented by user entities. In certain situations, the application of specified internal controls at user organizations is necessary to achieve certain Security, Availability, and Confidentiality Trust Services Criteria included in this report.

The user entity controls subsequently presented should not be regarded as a comprehensive list of all controls that should be employed by user entities:

- The security, availability, and confidentiality obligations pertaining to Customer Content are shared between customers, who manage their own policies, user permissions, and login information, and GoTo, who manages the transfer process through its UCC System.

Customer obligations may be described in relevant customer agreements (e.g., non-disclosure agreements, data processing addendum, subscription agreements, etc.), the ToS, and/or related legal policies, which are available on GoTo's website, as applicable.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls:

Controls Expected to be Implemented at User Entity Organizations	Complemented Criteria Ref. Number
Customers are responsible for notifying GoTo of product issues, problems, or actual or suspected incidents detected in their environments for resolution.	CC2.2, CC2.3
Customers are responsible for notifying GoTo of any specific security, availability, or confidentiality related requirements.	CC2.2, CC2.3
Customers are responsible for ensuring that their employees comply with customer-related policies and procedures when using workstations or terminals that may be used to access GoTo products.	CC6
Customers are responsible for notifying GoTo of application unavailability or inaccessibility from their customer environment and whether any downtime affects the terms of use.	CC2.3, A1.2

Controls Expected to be Implemented at User Entity Organizations	Complemented Criteria Ref. Number
Customers are responsible for using GoTo products based on their intended purpose, as specified in the relevant terms of service (or agreement for GoTo services) and in compliance with applicable laws, regulations, and policies.	CC1.3, CC2.2
Customers are responsible for periodically checking GoTo managed customer support channels, forums, articles, community pages, and/or knowledgebases for release and upgrade information.	CC2.2
Customers are responsible for implementing physical access security controls over their own environments and any workstations that the customer may use to access GoTo products.	CC6.4
Customers are responsible for configuring application password settings in accordance with their own policies and procedures as each system permits.	CC6.1, CC6.2
Customers are responsible for implementing secure user authentication credentials, including individual user IDs and passwords, when setting up and managing account access to in-scope systems.	CC6.1, CC6.2
GoTo customers are required to securely store authentication credentials. These include but are not limited to: User Account IDs, Passwords, or other access control, encryption, and security measures. GoTo will provide a means for resetting passwords.	CC6.1, CC6.2
GoTo customers are responsible for ensuring that user (employee) data is kept private, secured adequately, and maintained appropriately for accuracy and completeness, including the timely removal of user accounts as/if required.	CC6.3, C1.1, C1.2
GoTo customers are responsible for communicating user (employee) responsibilities regarding the use of the system.	CC2.2