HUBSPOT, INC.

INDEPENDENT SERVICE AUDITOR'S SOC 3 REPORT

FOR THE HUBSPOT PLATFORM SYSTEM

FOR THE PERIOD OF MAY 1, 2021, TO APRIL 30, 2022

Attestation and Compliance Services

INDEPENDENT SERVICE AUDITOR'S REPORT

To HubSpot, Inc.:

Scope

We have examined HubSpot, Inc.'s ("HubSpot") accompanying assertion titled "Assertion of HubSpot, Inc. Service Organization Management" ("assertion") that the controls within HubSpot's Platform system ("system") were effective throughout the period May 1, 2021, to April 30, 2022, to provide reasonable assurance that HubSpot'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, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*.

HubSpot uses various subservice organizations for cloud hosting and computing and data center hosting 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 HubSpot, to achieve HubSpot's service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Service Organization's Responsibilities

HubSpot 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 HubSpot's service commitments and system requirements were achieved. HubSpot has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, HubSpot 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 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 systems 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 HubSpot's service commitments and system requirements based on the applicable trust services criteria; and
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve HubSpot'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 HubSpot'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 HubSpot's Platform system were effective throughout the period May 1, 2021, through April 30, 2022, to provide reasonable assurance that HubSpot's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Schellman & Company, LLC

Atlanta, Georgia
June 3, 2022

ASSERTION OF HUBSPOT SERVICE ORGANIZATION MANAGEMENT

We are responsible for designing, implementing, operating, and maintaining effective controls within HubSpot, Inc.'s ("HubSpot") Platform system ("system") throughout the period May 1, 2021, to April 30, 2022, to provide reasonable assurance that HubSpot's service commitments and system requirements relevant to security, availability, and confidentiality were achieved. Our description of the boundaries of the system is presented below 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 May 1, 2021, to April 30, 2022, to provide reasonable assurance that HubSpot'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, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*. HubSpot's objectives for the system in applying the applying the applicable trust services criteria are embodied in its service commitments and systems requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented below.

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 May 1, 2021, to April 30, 2022, to provide reasonable assurance that HubSpot's service commitments and systems requirements were achieved based on the applicable trust services criteria.

DESCRIPTION OF THE BOUNDARIES OF THE HUBSPOT SYSTEM

Company Background

HubSpot, Inc. (”HubSpot”) provides software and support through a cloud-based customer relationship management (CRM) platform to help businesses grow better. The HubSpot’s CRM platform includes marketing, sales, service, and website management products. HubSpot’s products contain features, tools, and integrations that enable businesses to attract, engage, and delight customers throughout the customer lifecycle. Over 143,000 total customers in more than 120 countries use HubSpot’s software, services, and support to transform the way they attract, engage, and delight customers.

HubSpot was founded in 2005 and is based in Cambridge, Massachusetts.

Description of Services Provided

HubSpot’s CRM Platform consists of several integrated products that are bundled into integrated software packages:

- HubSpot CRM
- Marketing Hub
- Sales Hub
- Service Hub
- Content Management System (CMS) Hub

HubSpot CRM

The core of HubSpot’s Platform, the HubSpot CRM, is a single database of lead and customer information that allows businesses to track their interactions with contacts and customers, manage their sales activities, and report on their pipeline and sales. This allows a complete view of lead and customer interactions across HubSpot’s integrated applications, giving the CRM substantial power. This integration makes it possible to personalize every aspect of the customer interaction across web content, social media engagement, and e-mail messages across devices, including mobile. The integrated applications on the CRM have a common user interface, are accessed through a single login, and are based on the CRM database. HubSpot CRM is a free product that can be used standalone, or with any combination of Marketing Hub, Sales Hub, and/or Service Hub.

Marketing Hub

Marketing Hub is an all-in-one toolset for marketers to attract, engage, and nurture new leads towards sales readiness over the entire customer lifecycle. Marketing Hub is available in both free and paid tiers, and can be used standalone, with HubSpot CRM, and/or any version of Sales Hub or Service Hub. Features include marketing automation and e-mail, social media, search engine optimization (SEO), CRM Sync, and reporting and analytics.

Sales Hub

Sales Hub was introduced to enhance the productivity and effectiveness of sales representatives. Businesses can empower their teams with tools that deliver a personalized experience for prospects with less work for sales representatives. Sales Hub is available in both free and paid tiers, and can be used with HubSpot CRM, a third-party CRM, and/or any version of Marketing Hub or Service Hub. Features include: email templates and tracking, conversations and live chat, meeting and call scheduling, lead and website visit alerts, sales automation, and lead scoring.

Service Hub

Service Hub is our customer service software that is designed to help businesses manage and connect with customers. Service Hub is available in free and paid tiers, and can be used standalone, with HubSpot CRM Free, and/or any version of Marketing Hub or Sales Hub. Features include: conversations and live chat functionality,

conversational bots, tickets and help desk, automation and routing, knowledge base, team emails, feedback and reporting tools, and customer goals.

CMS Hub

CMS Hub combines the power of customer relationship management and a content management system into one integrated platform. HubSpot content tools enable businesses to create new and edit existing web content while also personalizing their websites for different visitors and optimizing their websites to convert more visitors into leads and customers. HubSpot CMS can be purchased as a standalone product and/or with any version of Marketing Hub, Sales Hub, or Service Hub. Features include: website pages, business blogging, smart content, landing pages and forms, SEO tools, forms and lead flow, web analytics reporting, calls-to-action, and file manager.

System Boundaries

A system is designed, implemented, and operated to achieve specific business objectives in accordance with management-specified requirements. The purpose of the system description is to delineate the boundaries of the system, which includes the services outlined above and the five components described below: infrastructure, software, people, procedures, and data.

Excluded from the scope of this report are security controls under the purview of the third-party data center colocation facilities. Currently, beta systems, as well as HubSpotVideo as of September 30, 2021, are excluded from the scope of this report. HubSpot has issued a separate SOC 2 Type II report covering systems dedicated to solely supporting the new Operations Hub offering (i.e. services formerly managed by PieSync) launched on April 21, 2021, for the period of Nov 1, 2021, through April 30, 2022.

Principal Service Commitments and System Requirements

HubSpot designs its processes and procedures related to the HubSpot Platform to meet its objectives for its HubSpot Platform services. Those objectives are based on the service commitments that HubSpot makes to user entities, the laws and regulations that govern the provision of the HubSpot Platform services, and the financial, operational, and compliance requirements that HubSpot has established for the services. The HubSpot Platform services are subject to the relevant regulatory and industry information and data security requirements in which HubSpot operates.

Security, availability, and confidentiality commitments to user entities are documented and communicated in customer agreements and in the Data Processing Agreement, which is published online. The principal security, availability, and confidentiality commitments are standardized, and include, but are not limited to, the following:

Security:

- Maintain administrative and logical safeguards to protect the security and integrity of the HubSpot Platform and customer data in accordance with HubSpot's security requirements.
- Use formal access management processes for the request, review, approval, and provisioning of HubSpot personnel with access to production systems.
- Use formal HR processes including: security awareness training, security and acceptable use policy, and a formal code of conduct.
- Use commercial industry standard secure encryption methods to protect customer data at rest and in transit.
- Maintain secure software development processes to ensure consistent quality that goes across policy, people, processes, and technology.
- Employ a dedicated product security incident response team that follows industry best practices in managing and responding to security vulnerabilities to minimize customers' risk of exposure.
- Maintain anti-virus protection, perform vulnerability scanning, and conduct periodic penetration testing to detect and prevent security vulnerabilities from being introduced into production systems.

- Use Web Application Firewall (WAF) solutions to protect hosted customer websites and other internet-accessible applications.

Availability:

- Employ infrastructure providers who use commercially reasonable efforts to ensure a minimum of 99.95% uptime. The providers maintain a minimum of N+1 redundancy to power, network, and heating, ventilation, and air conditioning (HVAC) services.
- Use backup and replication strategies that are designed to ensure redundancy and fail-over protections during a significant processing failure.
- Maintain and regularly test disaster recovery plans to help ensure availability of information following interruption to, or failure of, critical business processes.

Confidentiality:

- Maintain customer data as confidential and not disclose information to any unauthorized parties without written consent and notify customers should there be a breach of their data.
- Delete or return customer data upon contract termination or expiration in accordance to specified timeframes set out in the customer agreements.
- Delete customer data outside of scheduled data disposal periods upon request.

HubSpot establishes operational requirements that support the achievement of the principal service commitments, relevant laws and regulations, and other system requirements.

Such requirements are communicated in HubSpot's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These policies include ones around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired, trained, and managed. 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 HubSpot Platform.

In accordance with the Company's assertion and the description criteria, the aforementioned service commitments and requirements are those principal service commitments and requirements common to the broad base of users of the system and may therefore not fully address the specific service commitments and requirements made to system users individually.

Infrastructure and Software

HubSpot uses cloud storage and compute services from Amazon Web Services (AWS) and Google Cloud Platform (GCP), and data center hosting services from TierPoint, LLC. HubSpot does not own or maintain hardware located in the AWS and GCP data centers and operates under a shared security responsibility model, where AWS and GCP are responsible for the security of the underlying cloud infrastructure (i.e. physical infrastructure, geographical regions, availability zones, edge locations, operating, managing and controlling the components from the host operating system, virtualization layer and storage) and HubSpot is responsible for securing the application platform deployed in AWS and GCP (i.e. applications, identity access management, operating system and network virtual security groups configuration, network traffic, server-side encryption). HubSpot also does not own or maintain hardware located in the TierPoint data center and does not own any of the underlying infrastructure. Production servers and client-facing applications are logically and physically secured from HubSpot's internal corporate information systems.

A combination of internally-developed, externally-supported, and wholly-purchased applications support the HubSpot application platform, and is summarized as follows:

- The production infrastructure is centralized in AWS and GCP cloud hosting facilities and is managed by the HubSpot engineering team.

- The application platform utilizes containerized applications in a clustered environment for many services for security and reliability.
- Infrastructure Automation services are used to deploy and manage the lifecycle of public cloud instances with appropriate configuration and to prevent configuration drift.
- The job scheduler platform manages data feeds that run continuously, on-demand, or on a configured schedule.
- Automated segregation of duties (SoD) tools utilize branch protections in GitHub to enforce independent peer review and sign-off on high risk changes as well as to perform evaluation tasks to detect potential security changes in a pull request before it is eligible for deployment to production.
- HubSpot's compliance system hosts, aggregates, and reports on access, change, and employee events.
- Multiple security zones are utilized to segment and administer the production environment.

HubSpot's core infrastructure is spread across multiple availability zones in the United States (US) East region. HubSpot's Infrastructure team monitors the performance of infrastructure resources and provisions additional resources as capacity requires.

HubSpot has selected several vendors to provide important aspects of the application hosting framework used to support a robust cloud infrastructure for HubSpot applications. The production stack leverages the following third-party providers during the audit period:

- AWS: Core cloud hosting infrastructure based on AWS;
- GCP: Supplemental cloud hosting infrastructure based on GCP;
- Single Sign-On (SSO); and
- Cloud based data warehousing: Customer reporting across data sets.

These vendors help provide the platform with secure and reliable access to users, manageability by system administrators, and seamless upgradeability.

People

The following groups contribute to the management and oversight of our internal control environment:

- Board of Directors – responsible for overseeing the business on behalf of shareholders.
- Executive Leadership – responsible for overseeing company-wide activities, establishing and accomplishing goals, and overseeing objectives.
- Enterprise Risk — responsible for identifying risks to the business and developing mitigation strategies throughout the growth and evolution of the company.
- Systems and Network Operations – responsible for managing and supporting HubSpot's corporate network and infrastructure.
- Compliance Assurance — responsible for identifying and monitoring technology risks, managing the assessment and mitigation of said risks and enforcing compliance of security issues and incidents throughout the service delivery infrastructure.
- Legal — responsible for overseeing all legal matters affecting HubSpot, developing team strategy, and advising senior leadership.
- PeopleOps — responsible for developing and implementing HR policies, practices, and processes with a focus on key HR department delivery areas (e.g. talent acquisitions, employee retention, compensation, employee benefits, performance management, employee relations and training, and development).
- Engineering (Product) – responsible for developing applications and services that compose the HubSpot Platform.

- Engineering (Platform Infrastructure) – responsible for managing and supporting tooling to build, deploy, run and monitor the microservices and frontends that make up the HubSpot Platform.
- Engineering (Infrastructure Security) – responsible for managing and supporting tooling around the authentication, authorization and provisioning for both internal use as well as for third party cloud providers. Responsible for identifying, detecting, assessing, responding and remediating security risks and incidents.
- Engineering (Data Infrastructure) – responsible for managing and supporting HubSpot's unified data platform.
- Corporate Security – responsible for identifying, detecting, assessing, responding, and remediating security risks and incidents.
- Customer Services – responsible for supporting and onboarding customers.
- Customer Support – responsible for providing technical support for customers to assist with the proper use of the HubSpot platform.

Procedures

Authentication and Authorization

Access to HubSpot internal systems is protected by multiple authentication layers. A valid unique username and password is required to access the HubSpot corporate network. To access key in-scope systems from outside the office, HubSpot personnel are required to first connect via encrypted remote access tools or an Identity Aware Proxy (IAP) system using a username and password with multi-factor authentication (MFA). The corporate platform is managed through Active Directory (AD) and many key systems are integrated with AD. HubSpot employees are able to access the integrated systems through SSO. The engineering environment is logically segregated from the corporate environment and provides HubSpot personnel access to product infrastructure. Authentication to the product infrastructure is managed through an Identity Access Management (IDAM) system. Authentication to the IDAM follows the same process of authenticating through a unique username and password as when in the HubSpot Office. When accessing the IDAM remotely, an encrypted Virtual Private Network (VPN) connection is also needed, which requires MFA. Once authenticated, HubSpot personnel can access production systems. The authentication of each integrated system to the IDAM can vary, where certain systems are configured with a lightweight directory access protocol (LDAP) binding to the IDAM, while others use a privileged access management tool requiring an active IDAM account with specific group memberships. AWS requires a separate username and password paired with MFA. Tokens for application access to the secrets management system are distributed via the Infrastructure Automation system.

Management has restricted administrative access privileges within the production environment to authorized personnel. Administrative access to each in-scope system may be derived from assignment to privileged groups in AD or the IDAM; however, certain systems are restricted from having continuous administrative access. For these systems, a Just-In-Time Access (JITA) process is in place to request temporary administrative access for the purpose of performing job duties. Each JITA request is documented, tracked, and reviewed. Access is temporarily allowed and activity is logged for high risk actions performed during the session. After the configured session limit, access to the account expires and is automatically revoked.

Password managers are in place to manage certain administrative account passwords and access to the password manager is managed through individual groups or through the JITA process.

Access Requests and Access Revocation

A process has been established by HubSpot to manage user access requests, modifications, and deletions. The process varies based on the type of access needed and whether the system is related to corporate or product infrastructure. Administrative and high-risk access is either pre-authorized based on the employee's functional role in the company or authorized through an in-workflow approval prior to provisioning. Users requesting a modification for additional access will follow the same process.

New access is detected automatically by the compliance system and, if appropriate, routed to the appropriate personnel for retroactive approval as well. Additionally, user access and permissions to the key in-scope systems

are reviewed semi-annually to help ensure that only authorized individuals have access to key in-scope systems and that the access granted to these users is necessary for their job function. The same access review and re-approval process is automatically triggered when employees transfer to new roles, as reported in the HubSpot Human Resources Management System (HRMS).

Logical and physical access removal to the in-scope systems upon employee termination is also triggered automatically based on the integration with the HubSpot HRMS. If automated access removal is not technically possible, an automated notification is sent to the team responsible for access management requesting access removal.

Network and Data Security

Multiple access control lists (ACLs) are in place to protect the production network and are utilized to restrict access and filter unauthorized traffic. Rules are put in place for certain traffic to pass through the firewall to communicate with the production servers. Each firewall is configured to deny connections that are not explicitly authorized by the security groups ruleset. In addition, the firewall rulesets are reviewed on an annual basis to ensure that only necessary connections are configured. The reviews certify that the implemented firewall policies and rules function as intended. A WAF solution is also in place to protect hosted customer websites and other internet-accessible applications. The WAF is designed to identify and prevent attacks against publicly available network services.

To further protect the network, an endpoint detection and response solution is installed on the company-owned laptops and corporate network Windows/Linux servers. The endpoint detection and response is configured to detect and prevent malicious activity on registered endpoints. Encryption is also utilized on web servers for web communication sessions.

To protect customer data, HubSpot stores data on encrypted disks where access to the cryptographic keys is restricted to authorized personnel. AWS utilizes Elastic Block Store (EBS) encryption to protect data, while data residing within GCP is encrypted at rest.

Media Handling and Disposal of Data

Asset disposal procedures are in place to guide personnel in disposing of technology equipment when they reach the end of their life. HubSpot relies on disk encryption and the established AWS and GCP secure media disposal processes to ensure safe decommissioning.

HubSpot maintains a data subject request form for requests from customers and prospects regarding data deletion, portability, and general inquiries. The HubSpot Legal/Privacy team monitors and tracks the requests through completion.

Change Management

The HubSpot system development process is a formalized, process-driven approach intended to maintain the stability of production systems. This process dictates how changes to HubSpot-developed systems are documented, tested, reviewed, approved, and deployed. Program change documents and security best practices are documented on the HubSpot intranet and within the Engineering documentation repository.

HubSpot follows a standard GitHub Pull Request development process for internally-developed high-risk system changes wherein engineers create feature branches, work on them until a change is ready to be released, and then create a pull request. The pull request is used as a mechanism to seek feedback from other engineers, acquire approvals for high-risk changes, and discuss any changes before the code is merged back into the master branch of the code repository. HubSpot uses a combination of GitHub features such as status checks and protected branches to automatically enforce a series of checks that must be completed before a pull request is eligible to be merged into the master branch. Checks include code review, testing (where applicable), and merge approval from an engineer who did not author the change or commit the code. To automate the deploy process, continuous integration and deploy tools are used, including building, testing, tagging, versioning and releasing deployable artifacts to production. Access to implement changes into the production environment is restricted to authorized personnel and segregated from the development environment. For internally-developed changes, only signed deployables are implemented into the production environment.

Emergency changes follow a similar process to standard development with the exception that approvals do not need to be provided in advance of a production deployment. In an emergency scenario, engineers have the ability to "self-sign" their code which will trigger the creation of an incident in HubSpot's compliance system. Each such incident requires retroactive review and approval by Engineering management.

HubSpot utilizes a configuration management tool to ensure baseline configurations are consistently applied. In the event that a production server deviates from the baseline configuration, it will be overwritten with the baseline configuration within 30 minutes.

Manual/third-party system configuration changes are authorized, designed, developed, and managed through change ticket approval workflows or compliance system review workflows.

Data Backup and Disaster Recovery

Key systems are backed up on a regular basis with established schedules and frequencies. Backups are monitored for successful execution, and alerts are generated in the event of an unsuccessful execution. Failure alerts are escalated, investigated, and resolved.

Data is backed up daily to AWS in order to permit the resumption of operations in the event of a disaster. Monitoring is in place and alerts automatically inform the responsible team if the job fails so teams can triage. Additionally, backups are copied periodically to another AWS region to ensure recovery in the event of a complete regional outage.

HubSpot has a disaster recovery plan that details how the company sustains internal corporate and product infrastructure in the event of a disaster. The disaster recovery plan is documented, updated, and tested annually. Each system has mapped-out recovery test steps and is tested against a predefined Recovery Time Objective (RTO) and Recovery Point Objective (RPO). Disaster recovery testing methods include:

- Desk check - stakeholders review the content of a disaster recovery plan;
- Automated Backup Testing - a scheduled job is developed to automate the restoration of a recent backup as a test of the recovery process;
- Table-top exercise - members of the disaster recovery team gather and roleplay a disaster scenario; and
- Simulation test - support personnel meet while a disaster is simulated.

Incident Response

Data breach response and incident (CritSit) response policies and procedures are in place to manage unexpected incidents impacting the business and are provided to internal users to aid in identifying and reporting failures, incidents, concerns and other complaints. These procedures are reviewed on an annual basis to ensure they are effectively meeting business objectives.

The identification of and response to a CritSit follows multiple steps. When an event is first reported, the event is triaged and classified. For events that are classified as incidents, personnel utilize a CritSit repository to document the incident and subsequent steps. Individuals are involved as necessary for containment, eradication, recovery and corrective action to restore services and mitigate risks. For each CritSit, a postmortem is run to identify actions that can be taken to prevent future outages. Corrective measures or changes that occur because of CritSits and identified deficiencies follow the standard change control process.

CritSits are classified by severity. CritSits range from SEV-1 to SEV-5, and additionally include a SEV-NA category. A classification of SEV-1 is critical while SEV-5 is minor customer impact; SEV-NA indicates no customer impact. Triage and tactical members, including members of the Legal - Privacy, Security & Risk, Corporate Security, Trust & Safety and/or Infrastructure Security teams are notified when CritSits are further escalated as the result of potential or confirmed unauthorized access to HubSpot Product or Corporate infrastructure. Potential and confirmed personal data breaches are managed through closure in a separate system that facilitates both legal and security responses and the documentation of any such breach.

System Monitoring

HubSpot utilizes monitoring software to help detect potential anomalous activity related to security, such as product abuse, malicious activity, and login/user anomalies, as well as availability-related issues. Anomalous events are flagged within the software and organized by severity, time of appearance, and the search that detected them. Each event is reviewed by the impacted system's owning team and is tracked through closure. If an event indicates significant Customer impact, a CritSit may be opened. Anomalous activity has also been defined to include policy/configuration changes and anomalies in critical systems impacting the availability of the HubSpot product.

Additional system monitoring includes internal vulnerability scans over AWS and GCP, as well as penetration testing for HubSpot products and infrastructure. Vulnerability scans are configured to scan for exploitable vulnerabilities on a daily basis. Remediation tickets are automatically created from the vulnerability scans. Findings from the vulnerability scans are triaged for false positives, and tickets are created for true vulnerabilities and monitored through resolution. Remediation tickets are created from the penetration testing report findings and are triaged and monitored through resolution.

Data

The following table describes the information used and supported by the system.

Data Used and Supported by the System		
Data Description	**Data Reporting**	**Classification**
Customer contract information Disaggregated / identified Customer contact data Customer Intellectual Property or business data Customer communications (chat transcripts, email bodies, email attachments, etc.)	Private Customer and Company Data	Restricted
Customer "Deal Data" App usage data – Identified Customer support requests Online identifiers (IP addresses, cookie info, etc.) for HubSpot users Aggregated / de-identified customer data Metadata about customer communications (time, to/from, etc.)	Contact Insights and Browsing Information	Confidential
Customer names Aggregated / de-identified HubSpot usage data	Anonymized Data	Internal Only
Company names Other general information	Public Data	Public

Subservice Organizations

The HubSpot Platform services provided by AWS, GCP, and TierPoint were not included within the scope of this examination.

The following table presents the applicable Trust Services criteria that are intended to be met by controls at AWS, GCP, and TierPoint, alone or in combination with controls at HubSpot, and the types of controls expected to be implemented at AWS, GCP, and TierPoint to achieve HubSpot's service commitments and system requirements based on the applicable trust services criteria.

Control Activity Expected to be Implemented by AWS, GCP, and TierPoint	Applicable Trust Services Criteria
AWS and GCP are responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where HubSpot applications reside.	CC6.1 – CC6.2, CC6.5
AWS, GCP, and TierPoint are responsible for restricting physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers.	CC6.4 – CC6.5
AWS and GCP are responsible for implementing controls for the transmission, movement, and removal of the underlying storage devices for its cloud hosting services where HubSpot systems reside.	CC6.7
AWS and GCP are responsible for monitoring anomalies that are indicative of natural disasters within the data centers as well as physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers.	CC7.2
AWS, GCP, and TierPoint are responsible for ensuring the data center facility is equipped with environmental security safeguards and utilizing an environmental monitoring application to monitor for environmental events.	A1.2

Trust Services Criteria Not Applicable to the In-Scope System

All criteria within the security, availability, and confidentiality categories are applicable to the HubSpot Platform system.