BROADCOM®

System and Organization Controls (SOC) 3

Report on the Symantec SES Enterprise Platform System

Relevant to Security

For the Period
January 1, 2020 to June 30, 2020

Table of Contents

I.   **INDEPENDENT SERVICE AUDITORS' REPORT**

INDEPENDENT SERVICE AUDITORS' REPORT

To the Management of Broadcom, Inc.
San Jose, California

Scope

We have examined management's assertion, contained within the accompanying "Assertion of Broadcom Inc. Management" (assertion) that Broadcom's controls over the Symantec SES Enterprise Platform System (system) were effective throughout the period January 1, 2020 to June 30, 2020, to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the criteria relevant to security (applicable trust services criteria) set forth in the AICPA's TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

Service Organization's Responsibilities

Broadcom 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 Broadcom's service commitments and system requirements were achieved. In Section II of this report, Broadcom has provided the accompanying assertion titled "Assertion of Broadcom Inc. Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. Broadcom is responsible for preparing the description and assertion; including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditors' Responsibilities

Our responsibility is to express an opinion on the assertion, based on our examination. 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. An examination involves performing procedures to obtain evidence about management's assertion, which includes: (1) obtaining an understanding of Broadcom's relevant security policies, processes and controls, (2) testing and evaluating the operating effectiveness of the controls, and (3) performing such other procedures as we considered necessary in the circumstances. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence obtained during our examination is sufficient to provide a reasonable basis for our opinion.

Inherent Limitations

There are inherent limitations in 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 Broadcom'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 or 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, Broadcom's controls over the system were effective throughout the period January 1, 2020 to June 30, 2020, to provide reasonable assurance that its principle service commitments and system requirements were achieved based on the applicable trust services criteria.

JohansonGroup LLP

Colorado Springs, Colorado
September 1, 2020

BROADCOM®

II.   ASSERTION OF BROADCOM, INC. MANAGEMENT

BROADCOM®

Assertion of Broadcom, Inc. Management

We are responsible for designing, implementing, operating, and maintaining effective controls within Broadcom's Symantec SES Enterprise Platform System (system) throughout the period January 1, 2020 to June 30, 2020, to provide reasonable assurance that Broadcom's service commitments and system requirements relevant to security were achieved. Our description of the boundaries of the system is presented in the section of this report titled, "Broadcom, Inc. Description of the System," (description) 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 January 1, 2020 to June 30, 2020, to provide reasonable assurance that Broadcom's service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Broadcom'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 the accompanying system description.

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 January 1, 2020 to June 30, 2020, to provide reasonable assurance that Broadcom's service commitments and system requirements were achieved based on the applicable trust services criteria.

Broadcom, Inc. Management
September 1, 2020

BROADCOM

III.   BROADCOM, INC. DESCRIPTION OF THE SYSTEM

TYPES OF SERVICES PROVIDED

Symantec SES Enterprise Platform System provides enterprise services to supported applications via managing, operating, and maintaining data centers, infrastructure, systems and related functions that support activities, such as network, production, security, change management, hardware and environmental control activities.

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Commitments are declarations made by management to customers regarding the performance of SES Enterprise. Commitments are communicated in written individualized agreements and standardized contracts.

System requirements are specifications regarding how the Symantec SES Enterprise Platform System should function to meet Symantec's principal commitments to user entities. System requirements are specified in Symantec SES Enterprise Platform System's Service Agreement and its end user documentation, both of which are available internally to all employees and externally to all SES Enterprise customers.

Trust Services Category	Service Commitments	System Requirements
Security	• Protection of data at rest and in transit. • Regular System updates. • Protection and security of the information system from unauthorized access, use, modification, disclosure, destruction, threats, or hazards.	• Logical and physical access standards • Access provisioning and deprovisioning standards • Access reviews • Encryption standards • Intrusion detection and prevention standards • Risk and vulnerability management standards • Configuration management • Incident response standards • Change management standards • Vendor management standards • System access is granted to authorized personnel only • Regular security assessments • Identification and remediation of security incidents • Perform risk assessments for both internal and external threats to the system and its information

THE COMPONENTS OF THE SYSTEM USED TO PROVIDE THE SERVICE

The boundaries of the system are the specific aspects of Broadcom's infrastructure, software, people, procedures, and data necessary to provide its services and that directly support the services provided to customers. Any infrastructure, software, people, procedures and data that indirectly support the services provided to customers are not included within the boundaries of the system.

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

Infrastructure

Broadcom has entered into an agreement with AWS to provide global IaaS at its North Virginia site. AWS provides the physical and environmental security services in these two regions. However,

Broadcom is responsible for designing and configuring the Symantec SES Enterprise Platform System's architecture within AWS to ensure SES's security and confidentiality requirements are met.

Software

Software includes supporting operating systems and databases (AWS DynamoDB and AWS RDS) and Okta software for two-factor authentication. Broadcom uses AWS CloudWatch and CloudTrail to monitor system logs and service levels. Broadcom uses Amazon GuardDuty and Qualys to perform security monitoring and periodic security scans. Grafana is used for monitoring data. On a monthly basis, Key Performance Indicator (KPI) data is updated into a spreadsheet and reviewed by relevant management (based on service line).

People

Broadcom develops, manages, and secures the Symantec SES Enterprise Platform System via separate departments. The responsibilities of these departments are defined in the following table:

People	
Group/Role Name	**Function**
Executive Management	Responsible for overseeing company-wide activities, establishing and accomplishing goals, and overseeing objectives.
Global Security Office (GSO)	Responsible for delivering cyber security and physical security services to Broadcom.
Engineering and Operations	Responsible for the development, testing, deployment, daily operation, and maintenance of new code for the Symantec SES Enterprise Platform System.
Info Sec	Manages security measures including access controls and security of the development and production environment for Symantec Enterprise SES Platform System.

Product Management	Responsible for the product lifecycle including adding additional product functionality.
Human Resources (HR)	Manages the processes that support the employee lifecycle, to include: partnering with management on defining new roles/positions; performing background screening, onboarding new personnel, and facilitating the employee termination process.

Procedures

Procedures include the automated and manual procedures involved in the operation of the Symantec SES Enterprise Platform System. Procedures are developed and documented by the respective teams for a variety of processes, including those relating to product management, engineering, technical operations, security, IT, human resources, etc. These procedures are drafted in alignment with the overall Information Security Policies and are updated and approved as necessary for changes in the business, no less than annually.

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

Data

Data refers to transaction streams, files, data stores, tables, and output used or processed by the Symantec SES Enterprise Platform System. Via the platform, the customer/end-users define and control the data they load and store in the Symantec SES Enterprise Platform System's production network. This data is loaded into the environment and accessed remotely from customer systems via the internet.

Customer data is managed, processed, and stored in accordance with relevant data protection and other regulations and with specific requirements formally established in client contracts.

SYSTEM INCIDENTS

There were no identified significant system incidents that (a) were the result of controls that were not suitably designed or operating effectively to achieve one or more of the service commitments and system requirements or that (b) otherwise resulted in a significant failure in the achievement of one or more of those service commitments and system requirements as of period end date of this report.

THE APPLICABLE TRUST SERVICES CRITERIA AND RELATED CONTROLS APPLICABLE TRUST SERVICES CRITERIA

The Trust Services Categories that are in scope for purposes of this report are as follows:

- *Security*: Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the security of information or systems and affect the entity's ability to meet its objectives.

The common criteria are organized as follows:
1. *Control environment:* The criteria relevant to how the organization is structured and the processes the organization has implemented to manage and support people within its operating units. This includes criteria addressing accountability, integrity, ethical values, and qualifications of personnel, and the environment in which they function.

2. *Communication and information:* The criteria relevant to how the organization communicates its policies, processes, procedures, commitments, and requirements to authorized users and other parties of the system, and the obligations of those parties and users to the effective operation of the system.

3. *Risk assessment:* The criteria relevant to how the entity (i) identifies potential risks that would affect the entity's ability to achieve its objectives, (ii) analyzes those risks, (iii) develops responses to those risks, including the design and implementation of controls and other risk mitigating actions, and (iv) conducts ongoing monitoring of risks and the risk management process.

4. *Monitoring activities:* The criteria relevant to how the entity monitors the system, including the suitability, and design and operating effectiveness of the controls, and acts to address deficiencies identified.

5. *Control activities:* The criteria relevant to the actions established through policies and procedures that help ensure that management's directives to mitigate risks to the achievement of objectives are carried out.
6. *Logical and physical access controls:* The criteria relevant to how an entity restricts logical and physical access, provides and removes that access, and prevents unauthorized access.

7. *System operations:* The criteria relevant to how an entity manages the operation of system(s) and detects and mitigates processing deviations, including logical and physical security deviations.

8. *Change management:* The criteria relevant to how an entity identifies the need for changes, makes the changes using a controlled change management process, and prevents unauthorized changes from being made.

9. *Risk mitigation:* The criteria relevant to how the entity identifies, selects, and develops risk mitigation activities arising from potential business disruptions and the use of vendors and business partners.

This report is focused solely on the security category and Broadcom has elected to exclude the availability, confidentiality, processing integrity and privacy categories.

CONTROLS RELATED TO THE APPLICABLE CRITERIA

Broadcom's applicable controls supporting the security and confidentiality categories and related criteria are included in Section 4 of this report. Although the applicable criteria and related controls are included in Section 4, they are, nevertheless, an integral part of the organization's description of its system.

The five interrelated components of internal control at Broadcom include:

1. Control Environment – sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure.

2. Communication and Information – are systems, both automated and manual, that support the identification, capture, and exchange of information in a form and time frame that enable people to carry out their responsibilities.

3. Risk Assessment – is the entity's identification and analysis of relevant risks to the achievement of its objectives, forming a basis for determining how the risks can be managed.

4. Monitoring – is a process that assesses the quality of internal control performance over time.

5. Control Activities – are the policies and procedures that help make sure that management's directives are carried out.

The Symantec SES Enterprise Platform System's internal control components include controls that may have a pervasive effect on the organization, an effect on specific processes, account balances, disclosures, classes of transactions or applications, or both. Some of the components of internal control include controls that have more of an effect at the entity level, while other components include controls that are primarily related to specific processes or applications. When assessing internal control, the Symantec SES Enterprise Platform System considers the interrelationships among the five components.

CONTROL ENVIRONMENT

Integrity and Ethical Values

Broadcom has developed a Code of Conduct that addresses acceptable business practices, conflicts of interest, and expected standards of ethical and moral behavior. Broadcom has also developed employee

Confidentiality Agreements that prohibit inappropriate use and disclosure of customer or Broadcom information. These documents are provided to all new employees. All employees and contractors are required to sign a Confidentially Agreement as well as acknowledge and agree to follow the Code of Conduct.

Broadcom management performs annual performance evaluations of personnel to maintain compliance with Broadcom policies and codes of conduct. Employees and contractors who violate the code of conduct are subject to disciplinary actions.

Board of Directors

The Broadcom Board of Directors or a designated committee oversees and advises Broadcom's corporate governance, strategy, and risk oversight. The Board of Directors, composed of internal and external business executives, meets regularly to discuss matters pertinent to Broadcom business operations, financial results, and strategic planning.

Organizational Structure

Broadcom has established lines of reporting which facilitate the flow of information to personnel. Broadcom's HR system has a built-in organization chart that sets forth Broadcom's lines of reporting and which is updated automatically as organizational changes occur. The Executive Management Team empowers business functions to implement and manage functional policies, procedures, methods, and organization structure for increasing operational effectiveness and service delivery excellence. The Symantec SES Enterprise Platform System's organization is structured to oversee the implementation and compliance of all required financial, business, and security controls. Roles and responsibilities are segregated based on functional requirements.

Management's Philosophy and Operating Style

Broadcom's senior management takes a "hands on" approach to running the business. Senior Management is heavily involved in all phases of the business operations. Management uses a top-down approach to establish or update specific business objectives for business units and functions, including information technology, within the organization. This process includes budgeting resources and establishing metrics for the achievement of the objectives.

Authority and Responsibility

Management and employees are assigned levels of authority and responsibility to facilitate effective internal control. The Chief Security Officer (CSO) is responsible for overseeing the control environment. The duties, responsibilities, and hierarchy of employees on the information security team are defined in a role matrix and form the foundation of Broadcom's control environment. The CSO reports administratively to the EVP, General Counsel, with an escalation point to the CEO. As part of the development of specific business objectives, the Executive Vice President for the Symantec SES Platform System's business unit is responsible for executing Broadcom's strategy and other decisions agreed upon by Broadcom executive management and the Board of Directors.

HUMAN RESOURCES

Broadcom maintains formal hiring and termination policies and procedures. Applicants with a role in the delivery of services are hired based on their ability to satisfy the job duties and responsibilities of the position and fulfill the goals and expectations of Broadcom. They are evaluated on their level of education, the merits of their experience, and their knowledge of relevant security controls and processes. All applicants must undergo a background check in accordance with local law; employment is contingent upon satisfactory results. Broadcom has a process to assign key processes and technology to authorized personnel.

Upon hiring and annually thereafter, all employees must successfully complete training courses covering Broadcom's code of conduct, data protection/privacy, and basic information security practices. The training courses are designed to assist employees in identifying and responding to social engineering attacks and in avoiding inappropriate security practices.

Contractors are required to follow the same onboarding process as employees and are contractually obligated to perform the same background checks and security awareness training requirements as employees. Employees' and contractors' compliance with security awareness training requirements is monitored on an annual basis by Digital Trust & Safety.

All employees go through an annual performance review cycle. At the beginning of each review period, employees and their immediate supervisors establish goals and expectations for their job performance over the upcoming year based on the job duties, priorities, and responsibilities described. Employees receive an annual performance review from their supervisors that assesses the employees' performance against the agreed-upon goals and expectations. Employees whose performance is not in alignment with established goals and expectations for job performance, or who are not fulfilling their job responsibilities, may be referred to human resources by their supervisor to develop a performance improvement plan.

If an employee violates any Broadcom policies, or otherwise acts in a manner deemed contrary to the mission and objectives of Broadcom or in violation of the code of conduct, whether purposefully or not, the employee is subject to sanctions up to and including termination of employment.

COMMUNICATION AND INFORMATION

Broadcom has implemented information and communication mechanisms to make information available regarding its business practices.

The Global Security Office has a documented Information Security Policy and a suite of supporting Standards. These documents are updated at least annually and are made available to all employees. The internal communication of cybersecurity information for employees is according to their role in the organization. Training on the Information Security Policy is described on the Security Awareness Program site, which is available to all employees on the Broadcom intranet site.

Broadcom has reporting mechanisms for employees to communicate potential security issues or concerns they have been involved in or witnessed (such as phishing attacks, malware, lost or stolen devices, and inappropriate information disclosure). One mechanism employees can use includes the anonymous EthicsLine, available 24/7 via phone, email, or website. Broadcom also has established processes to accept

and address reports of software vulnerabilities, including providing a means for external entities to contact the information security group.

Broadcom obtains or generates and uses relevant information to support the functioning of internal control through the following:

- Control monitoring through periodic management review meetings, internal audits, and external audits

- Vulnerability scans

- Log management tools

Broadcom limits communication of matters related to the functioning of internal systems to only those stakeholders and business partners who have a need to know such information. This information is communicated via mediums appropriate to the nature of the information and the urgency of the situation, and may include conference calls, electronic mail, memoranda, or in-person meetings. In the rare instance when public disclosure of such matters would be necessary or appropriate, Broadcom's legal counsel and

Corporate Communications team are responsible for jointly distributing and communicating such disclosure.

Broadcom provides customers with multiple channels to report and manage service issues. Dedicated support resources are responsible for keeping these Service Requests up to date and use available escalation and communication methods to keep customers informed about their requests.

RISK ASSESSMENT AND MITIGATION

The Corporate Risk Assurance (CRA) team oversees Broadcom's global risk assessment process to identify and manage risks that could affect Broadcom's ability to provide reliable services to its clients. This process requires management to identify significant risks in their areas of responsibility and to implement measures to address those risks. In designing its controls, Broadcom has considered the risks that could prevent it from effectively addressing the criteria under the security and confidentiality trust services categories.

Broadcom maintains a risk management framework designed to ensure risks are evaluated and that controls are reasonably designed, implemented, and operated to address all areas, as appropriate, to detect, respond to, mitigate, and recover from security events based on the assessed risks. Areas for consideration include compliance objectives, external laws and regulations, and risk appetite. Areas for evaluation include systems development, computer operations, program changes, and access to programs and data. Implemented controls include preventive and detective controls, such as manual, automated, or IT-dependent controls based on the environment in which the entity operates, the nature and scope of the entity's operations, and its specific characteristics. Broadcom identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed. Broadcom's risk assessment process includes an analysis of possible threats and vulnerabilities relative to each of the objectives. The risk identification process includes consideration of both internal and external factors and their impact on the achievement of the objectives.

Broadcom considers the potential for fraud in assessing risks to the achievement of objectives. The assessment of fraud risk considers fraudulent reporting, possible loss of assets, or data and corruption resulting from the various ways that fraud and misconduct can occur. It also considers opportunities for unauthorized acquisition, use or disposal of assets, altering of the entity's reporting records, or committing other inappropriate acts and how management and other personnel might engage in or justify inappropriate actions.

Broadcom identifies and assesses changes that could significantly impact the system of internal control. The risk identification process considers changes to the regulatory, economic, and physical environment in which Broadcom operates. Broadcom considers the potential impacts of new business lines, dramatically altered compositions of existing business lines, acquired or divested business operations, rapid growth, and new technologies on the system of internal control.

Identified risks are analyzed through a process that includes estimating the potential significance of the risk. Broadcom's risk assessment process includes considering how the risk should be managed and whether to accept, avoid, mitigate, or share the risk. Broadcom determines mitigation strategies for the risks that have been identified and designs, develops, and implements controls, including policies and procedures, to implement its risk mitigation strategy.

Security risks related to external parties (such as contractors and vendors) are identified and addressed based on Broadcom's procurement process. Designated responsibilities are defined in reviewing risks associated with external parties and establishing relevant agreements. Purchase orders to engage a third-party require a vendor agreement and signed NDA to be established.

Sensitive information is disclosed to a vendor or business partner only on an as-needed basis, and only if the vendor or business partner has enacted appropriate information security and privacy controls. All vendors and business partners with access to sensitive information are subject to confidentiality and privacy agreements and other contractual confidentiality provisions, which must be signed and acknowledged before access to Broadcom's systems and data is granted.

Broadcom's Supplier Security Assurance program manages supply chain security risk throughout the lifecycle of the relationship and provides assurance that third parties who handle and process information and facilities on Broadcom's behalf do so in accordance with legal, regulatory, and contractual requirements for security.

Adoption of a supplier's services has inherent information security risks, which are managed by adopting the following approach:

- Categorize: Third parties are categorized according to the nature, criticality, and likelihood of risk commensurate with the adoption of their services
- Assess: Third parties are security reviewed in accordance with their assigned risk category
- Respond: The Supplier Assurance team conducts risk assessments based upon information provided in completed questionnaires and audit findings
- Monitor: All risk remediation actions identified from risk assessments are tracked through to closure. Third parties are periodically re-assessed, according to their risk categorization

MONITORING

Broadcom selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning. Internal personnel conduct periodic assessments and tests of internal controls that include (a) working with process owners and IT support personnel to identify specific security threats and vulnerabilities and how the associated risk is being addressed and (b) tests of the design, implementation, and operating effectiveness of internal controls that address risks. Members of the internal assessment team have the requisite knowledge of and experience with cybersecurity risks and controls. They also subscribe to industry standard bulletins and email alerts on security, delivered through Broadcom's Vulnerability Management Team, Broadcom's SecurityFocus Bugtraq mailing list (BID alerts), as well as its DeepSight Intelligence for Vulnerability Management mailing list.

Broadcom also uses external parties to independently evaluate the state of the control environment. Quarterly vulnerability assessments and annual penetration tests are performed by an external service provider to identify specific technical threats and vulnerabilities and to benchmark the environment against leading cybersecurity practices. Every year, Broadcom engages a service provider to perform an independent assessment of the system program to evaluate alignment with leading industry practices and consistency with company policies to identify gaps and potential opportunities for improvement.

Both internal and external evaluations are made using a risk-based approach that may vary in the nature, timing, and extent of testing. The criteria for such evaluations, including the nature and frequency of such evaluations, are reviewed during the annual risk assessment and modified as needed, with consideration for changes to Broadcom's operational processes, including changes to the size, scope, and operational nature of the business, recent security threats or incidents, new or emerging risks, and changes in industry standards.

The results of all monitoring activities, regardless of source, are entered into a vulnerability tracking system for evaluation and identification of remediation activities that may be needed. Identified vulnerabilities are assessed regarding the likelihood and magnitude of exploitation. All vulnerabilities evaluated are identified for remediation or additional monitoring. Responsibilities for corrective action plans are assigned and completion dates determined. The Information Security team reviews the list of open vulnerabilities monthly to monitor progress toward resolution and to identify trends and responses.

CONTROL ACTIVITIES

Broadcom's control activities are defined through its established policies and procedures. Policies are dictated through management or board member statements of what should be done to effect control. Such statements may be documented, explicitly stated in communications, or implied through actions and decisions. Policies serve as the basis for procedures. Control activities are deployed through policies that establish what is expected, and procedures that put policies into action. A list of policies and procedures is documented in the above Procedures section.

LOGICAL AND PHYSICAL ACCESS

Broadcom's Identity and Access Management Standard establishes the access control requirements for requesting and provisioning user access for the system. The policy requires that access be denied by default, following a least privilege principle, and be granted only upon business need. Broadcom uses centralized authentication and authorization to restrict access to the systems and services within the environment. Each user account is unique and is identifiable to an individual user. Segregation of duties is established on critical functions within the environment to minimize the risk of unauthorized changes to production systems.

Domain-account management requests are routed to the designated asset owner or associated employee according to established account provisioning and de-provisioning processes for approval. Typically, access is controlled through addition of individual user accounts to established domain security groups within the Active Directory (AD). Based on the configuration of a security group, any access requests require explicit approval from the assigned security group owner. Requests are automatically forwarded to the security group owner for approval in the system.

Employee status data is used to facilitate the provisioning and removal of user accounts in the system. Account management processes prevent the creation of an account for individuals that do not have valid HR records. Select users can request removal of user accounts from the system. In addition, system owners can directly remove users from Security Groups. Upon termination, employees are required to return their badges and workstations to Broadcom. Terminated employees are removed from the AD and thus all access is terminated.

Automated mechanisms have been implemented to manage the appropriateness of access granted to information systems. Manual periodic reviews of individual accounts and security group memberships on assets are performed by authorized individuals, as appropriate, to evaluate whether access is still required. Remediation action is taken, as necessary, based on the review.

Policies and standards have been established and implemented to enforce appropriate user account password expiration, length, complexity, and history. All Broadcom personnel are required to follow Broadcom's password policy for all domains as well as local user accounts for all assets.

Access to the production environment is controlled through a designated set of access points and restricted to the product teams. Users are authenticated to access points using AD domain credentials depending on where the production assets are located. Passwords, along with two-factor authentication used to access network devices are restricted to authorized individuals and system processes based on job responsibilities and are changed on a periodic basis.

Cryptographic controls and approved algorithms are used for information protection within the production environment and are implemented based on Broadcom's policies and standards. Cryptographic keys are managed throughout their lifecycle (e.g., ownership, generation, storage, distribution, periodic rotation, and revocation) in accordance with key management procedures.
Broadcom maintains a detailed inventory of all information systems. All such assets are assigned ownership by a designated department or team within Broadcom and prioritized based on the asset's business value and criticality to the organization. The classification process is owned by the Governance Risk and Response group within the Global Services Organization. Information and data assets are subject to the data management policy that defines parameters for the ownership, classification, security,

storage, and retention of data. Software and hardware assets are subject to the information systems management policy that defines parameters for the acquisition, development, maintenance, security, and disposal of information system assets. Steps are taken to protect assets commensurate with the respective asset's classification and its data sovereignty. Review of asset inventory, ownership, and classification is performed at least semi-annually.

The inventory of servers is monitored and maintained by the product team. On a monthly basis, the Broadcom Financial team checks for completeness and accuracy of the inventory to ensure that it represents the production environment appropriately. Broadcom has created and implemented processes to control the delivery and removal of information assets through a centralized ticketing system. In addition, network architecture is maintained as part of the inventory process. Metadata of the assets are collected and maintained within the inventory that provides an overview and flow of the network.

SYSTEM OPERATIONS

Technical standards and baselines have been established and communicated for production system deployments. Automated mechanisms and periodic scanning have been deployed to detect and troubleshoot exceptions and / or deviations from the baseline in the production environment. Where applicable, mechanisms are in place for services to re-image production servers with the latest baseline configuration at least on a monthly frequency. Further, OS and product teams review and update configuration settings and baseline configurations at least annually.

Broadcom has implemented procedural and technical standards for the deployment of network devices. These standards include baseline configurations for network devices, network architecture, and approved protocols and ports. Broadcom regularly monitors network devices for compliance with technical standards and potential malicious activities.

Broadcom has implemented agent-based monitoring infrastructure and custom script-based monitoring within the environment to provide automated logging and alerting capabilities. The logging solutions are enabled on all production systems. The monitoring system detects potential unauthorized activity and security events such as the creation of unauthorized local users and local groups. The monitoring agents are responsible for monitoring a defined set of user and administrator events, aggregating log events and sending the aggregated log information to a centralized log repository at regular intervals.

Broadcom has established a policy which restricts the log and monitor access to only authorized staff with a business need to access such systems. Product teams determine the specific events that need to be captured in consideration with a baseline. Administrator, operator, and system activities performed, such as logon / logoff within the environment, are logged and monitored.

For network devices, Broadcom monitors, logs, and reports on critical / suspicious activities and deviations from established baseline security configurations for the network devices. Predefined events are reported, tracked, and followed up on and security data is available for forensic investigations. The logs are retained centrally for forensic related analysis and access to the logs follows the same procedures defined above.

Broadcom has implemented an alerting system to provide real-time alerting through automatic generation of emails and alarms based on the log information captured by the monitoring infrastructure.

Product teams are responsible for configuring the events to be alerted. The event and warning logs are routinely examined for anomalous behavior and, when necessary, appropriate actions are taken in accordance with the incident handling procedures described in the Incident Management section. The product teams manage response to malicious events, including escalation to and engaging specialized support groups. In addition, Broadcom monitors relevant external information to stay up-to-date with current threat scenarios and countermeasures.

Broadcom carries out internal and external scans to identify vulnerabilities and assess the effectiveness of the patch management process. These scans are used to ensure compliance with baseline configuration templates, validate that relevant patches are installed, and identify vulnerabilities. The scanning reports are reviewed by Broadcom's Security as well as Product teams, and remediation efforts are conducted in a timely manner.

Security patches are applied immediately or during a scheduled release to the environment based on the severity of the vulnerability. Processes are in place to evaluate patches and their applicability to the environment. Once patches have been reviewed and their criticality level determined, product teams determine the release cadence for implementing patches without service disruption.

Product teams follow a change process to modify the underlying OS within the platform. All changes are reviewed and tested, at a minimum, for their quality, performance, impact on other systems, recovery objectives and security features before they are moved into production using a defined release process. Test windows have been established for reviewing and testing of new features, and changes to existing features and patches.

Penetration testing (pen test) is performed at least annually on the system. The pen test scope is determined based on Broadcom's areas of risk and compliance requirements.
Broadcom has implemented an Incident Management framework that includes defined processes, roles, communications, responsibilities, and procedures for detection, escalation and response to incidents internally and to customers.

Broadcom has established Incident Response procedures and centralized tracking tools which consist of different channels for reporting production system incidents and weaknesses. Automated mechanisms include system monitoring processes for alerting security teams per defined and configured events, thresholds, or metric triggers. Incidents may also be reported via email. Customers are made aware of their responsibilities of reporting incidents that shall be looked into without any negative consequences. Broadcom's incident response provides 24x7 event / incident monitoring and response services. The teams assess the health of various components along with access to detailed information when issues are discovered.

Additionally, Broadcom conducts yearly tests of the Incident Management SOPs and response capabilities. Reports related to information security events are provided to management on a quarterly basis.
Broadcom's product teams use the established incident classification, escalation, and notification process for assessing an incident's criticality and severity, and accordingly escalating to the appropriate groups for timely action. The security team documents, tracks, and coordinates responses to incidents. Where required, security incidents are escalated to the privacy, legal, or executive management team(s) following established forensic procedures to support potential legal action after an information security incident.

Post-mortem activities are conducted for customer impacting incidents or incidents with high-severity ratings. The post-mortems are reviewed by the security team during monthly review meetings with senior management. Incident and security post-mortem trends are reviewed and evaluated on a periodic basis and, where necessary, the platform or security program may be updated to incorporate improvements identified because of incidents.

CHANGE MANAGEMENT

The Change Management process has been established to plan, schedule, approve, apply, distribute, and track changes to the production environment through designated responsibilities with the objective of minimizing risk and customer impact. It further controls the integrity and reliability of the environment while maintaining the pace of change required for business purposes.

Software, system, and configuration changes, including major releases, minor releases and hot fixes, are managed through a formal change and release management procedure, and tracked using a centralized ticketing system. The categorization of these changes is based on priority and risk associated with the change. Changes are requested, approved, tracked, and implemented throughout the release lifecycle, which includes product and engineering planning, release management, deployment and post deployment support phases. Change requests are documented, assessed for their risks and evaluated / approved for acceptance by the designated personnel.

Patches are released through the periodic OS release cycle in accordance with change and release management procedures. Emergency out-of-band security patches are expedited for more immediate release.

Formal security and quality assurance testing are performed prior to the software release through each pre-production environment (i.e., development and test/sandbox) based on defined acceptance criteria. The results of the quality assurance testing are reviewed and approved by the appropriate personnel prior to moving the release to production. Changes are reviewed for their adherence to established change and release management procedures prior to closure. Once deployed, changes are monitored for success; failed implementations are immediately rolled back, and the change is not considered as completed until it is implemented and validated to operate as intended.

The Symantec SES Enterprise Platform System product team's software development practices, outlined in its Software Development Lifecycle (SDLC) methodology, is with aligned Broadcom's Secure Software Development Lifecycle Standard. The Standard introduces security and privacy control specifications during the feature/component design and throughout the development process, which are reviewed through designated security roles.

Broadcom's SDLC baseline includes tasks to be performed which identify tools or processes that ensure teams are developing their services in a secured manner. As part of onboarding onto the SDLC process, the product teams (engineering and operations) work together to determine any additional SDLC steps to be performed specific to the service. Additionally, teams are required to perform threat modeling exercises which are reviewed and approved by the security and/or system architect. Each product team has a product owner who is responsible for ensuring appropriate completion of the SDLC tasks. The product owner reviews the SDLC tasks and gives the overall sign off for completion of the SDLC process.

COMPLEMENTARY USER ENTITY CONTROLS (CUECs)

Broadcom's controls related to the Symantec SES Enterprise Platform System cover only a portion of overall internal control for each user entity of the Symantec SES Enterprise Platform System. It is not feasible for the criteria related to the system to be achieved solely by the Symantec SES Enterprise Platform System. Therefore, each user entity's internal control should be evaluated in conjunction with the Symantec SES Enterprise Platform System's controls and the related tests and results described in Section 4 of this report, taking into account the related complementary user entity controls identified for the specific criterion. For user entities to rely on the controls reported herein, each user entity must evaluate its own internal control to determine whether the identified complementary user entity controls have been implemented and are operating effectively.

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

Management of user entities is responsible for the following:

Criteria	Complementary User Entity Controls (CUECs)
CC2.1	• User entities have policies and procedures to report any material changes to their overall control environment that may adversely affect services being performed by the Symantec SES Enterprise Platform System according to contractually specified time frames. • Controls to provide reasonable assurance that the Symantec SES Enterprise Platform System is notified of changes in: • user entity vendor security requirements • the authorized users list
CC2.3	• It is the responsibility of the user entity to have policies and procedures to: • inform their employees/users that their information/data is being used and stored by the Symantec SES Enterprise Platform System • determine how to file inquiries, complaints, disputes which would get passed onto the Symantec SES Enterprise Platform System
CC6.3	• User entities grant access to the Symantec SES Enterprise Platform System's system to authorized and trained personnel. • User entities deploy physical security and environmental controls for all devices and access points residing at their operational facilities, including remote employees or at-home agents for which the user entity allows connectivity.
CC6.7	• Controls to provide reasonable assurance that policies and procedures are deployed over user IDs and passwords that are used to access services provided by Broadcom.

SUBSERVICE ORGANIZATIONS AND COMPLEMENTARY SUBSERVICE ORGANIZATION CONTROLS (CSOCs)

Broadcom uses AWS as a subservice organization for data center colocation services. The Symantec SES Enterprise Platform System controls related to the SES Enterprise system cover only a portion of the overall internal control for each user entity of the Symantec SES Enterprise Platform System. The description does not extend to the services provided by the subservice organization that provides colocation services for IT infrastructure. Section 4 of this report and the description of the system only cover the Trust Services Criteria and related controls of Broadcom and exclude the related controls of AWS.

Although the subservice organization has been carved out for the purposes of this report, certain Trust Services Criteria are intended to be met by controls at the subservice organization. CSOCs are expected to be in place at AWS related to physical security and environmental protection, as well as backup and recovery. AWS' physical security controls mitigate the risk of fires, power loss, climate, and temperature variabilities.

Broadcom management receives and reviews the SOC 2 report of AWS on an annual basis. In addition, through its operational activities, Symantec SES Enterprise Platform System management monitors the services performed by AWS to determine whether operations and controls expected to be implemented at the subservice organization are functioning effectively. Management also has communication with the subservice organization to monitor compliance with the service agreement, stay abreast of changes planned at the hosting facility, and relay any issues or concerns to AWS management.

It is not feasible for the criteria related to the Symantec SES Enterprise Platform System to be achieved solely by the Symantec SES Enterprise team. Therefore, each user entity's internal control must be evaluated in conjunction with the Symantec SES Enterprise Platform System's controls and related tests and results described in Section 4 of this report, taking into account the related complementary subservice organization controls expected to be implemented at the subservice organization as described below.

Complementary Subservice Organization Controls (CSOCs)
- Broadcom Integrated Cyber Defense (ICD) Team is responsible for restricting firewall access to authorized personnel.   - Broadcom ICD Team is responsible for firewall maintenance activities.
- AWS is responsible for restricting data center access to authorized personnel.   - AWS is responsible for the 24x7 monitoring of data centers by closed circuit cameras and security personnel.

Complementary Subservice Organization Controls (CSOCs)
• AWS is responsible for the installation of fire suppression and detection, and environmental monitoring systems at the data centers. • AWS is responsible for protecting data centers against a disruption in power supply to the processing environment by an uninterruptible power supply (UPS). • AWS is responsible for overseeing the regular maintenance of environmental protections at data centers.

SPECIFIC CRITERION NOT RELEVANT TO THE SYSTEM

There were no specific security or confidentiality Trust Services Criterion as set forth in TSP Section 100 that were not relevant to the system as presented in this report.

REPORT USE

The description does not omit or distort information relevant to the Symantec SES Enterprise System, while acknowledging that the description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to his or her own particular needs.