OpenGov, Inc.

Type 2 SOC 3

2023

SOC 3 FOR SERVICE ORGANIZATIONS REPORT

December 16, 2022 to December 15, 2023

Table of Contents

SECTION 1

ASSERTION OF OPENGOV, INC. MANAGEMENT

ASSERTION OF OPENGOV, INC. MANAGEMENT

December 22, 2023

We are responsible for designing, implementing, operating, and maintaining effective controls within OpenGov, Inc.'s ('OpenGov' or 'the Company') OpenGov Services System throughout the period December 16, 2022 to December 15, 2023, to provide reasonable assurance that OpenGov's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, Processing Integrity, and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA, *Trust Services Criteria*. Our description of the boundaries of the system is presented below in "OpenGov, Inc.'s Description of Its OpenGov Services System throughout the period December 16, 2022 to December 15, 2023" and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period December 16, 2022 to December 15, 2023, to provide reasonable assurance that OpenGov's service commitments and system requirements were achieved based on the trust services criteria. OpenGov'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 "OpenGov, Inc.'s Description of Its OpenGov Services System throughout the period December 16, 2022 to December 15, 2023".

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

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

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period December 16, 2022 to December 15, 2023 to provide reasonable assurance that OpenGov's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organizations controls and complementary user entity controls assumed in the design of OpenGov's controls operated effectively throughout that period.

Suresh Seshadri

Suresh Seshadri
CFO
OpenGov, Inc.

SECTION 2

INDEPENDENT SERVICE AUDITOR’S REPORT

INDEPENDENT SERVICE AUDITOR’S REPORT

To OpenGov, Inc.:

Scope

We have examined OpenGov accompanying assertion titled “Assertion of OpenGov, Inc. Management” (assertion) that the controls within OpenGov’s OpenGov Services System were effective throughout the period December 16, 2022 to December 15, 2023, to provide reasonable assurance that OpenGov’s service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, Processing Integrity, and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA *Trust Services Criteria*.

OpenGov uses AWS and Azure to provide cloud hosting services. The description indicates that complementary subservice organizations controls that are suitably designed and operating effectively are necessary, along with controls at OpenGov, to achieve OpenGov’s service commitments and system requirements based on the applicable trust services criteria. The description presents OpenGov’s controls, the applicable trust services criteria, and the types of complementary subservice organizations controls assumed in the design of OpenGov’s controls. The description 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 organizations controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at OpenGov, to achieve OpenGov’s service commitments and system requirements based on the applicable trust services criteria. The description presents OpenGov’s controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of OpenGov’s controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization’s Responsibilities

OpenGov 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 OpenGov’s service commitments and system requirements were achieved. OpenGov has also provided the accompanying assertion (OpenGov assertion) about the effectiveness of controls within the system. When preparing its assertion, OpenGov is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor’s Responsibilities

Our responsibility is to express an opinion, based on our examination, on management’s assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization’s service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management’s assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Independence and Ethical Responsibilities

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the examination engagement.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within OpenGov's OpenGov Services System were suitably designed and operating effectively throughout the period December 16, 2022 to December 15, 2023, to provide reasonable assurance that OpenGov's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects, if complementary subservice organizations controls and complementary user entity controls assumed in the design of OpenGov's controls operated effectively throughout that period.

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

Restricted Use

This report, is intended solely for the information and use of OpenGov, user entities of OpenGov's OpenGov Services during some or all of the period December 16, 2022 to December 15, 2023, business partners of OpenGov subject to risks arising from interactions with the OpenGov Services, and those who have sufficient knowledge and understanding of the complementary subservice organizations controls and complementary user entity controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.

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

A-LIGN ASSURANCE

Tampa, Florida
December 22, 2023

SECTION 3

OPENGOV, INC.’S DESCRIPTION OF ITS OPENGOV SERVICES SYSTEM THROUGHOUT THE PERIOD DECEMBER 16, 2022 TO DECEMBER 15, 2023

OVERVIEW OF OPERATIONS

Company Background

OpenGov was founded in 2012 with the objective of providing cloud-based multi-tenant software solutions serving state and local government organizations. The mission of OpenGov is to power more effective and accountable government. OpenGov is based in San Jose, California.

OpenGov provides cloud-based, enterprise resource planning (ERP) software to over 1600 local governments, municipalities, state agencies, school districts, and other county-level entities. Within the ERP, the specific applications include OpenGov Budgeting & Planning, OpenGov Procurement, Enterprise Asset Management, Permitting and Licensing and the OpenGov Reporting & Transparency platform.

In September of 2022, OpenGov acquired Cartegraph, an asset management software company founded in 1994, that also serves the public sector. The full integration of Cartegraph's systems, teams and processes was completed in June 2023, and their core product, "Enterprise Asset Management" is in scope this year starting June 15, 2023.

Description of Services Provided

OpenGov provides cloud-based multi-tenant software solutions to public sector organizations throughout the United States. The company was founded to simplify and streamline how non-Federal government entities perform their finance, accounting, and reporting functions.

OpenGov's core suites include Budgeting and Planning, Procurement, Reporting and Transparency, Permitting and Licensing and Enterprise Asset Management.

High level suite offerings include:

- Budgeting and Planning
  - Collaborative Budgeting
  - Capital Planning
  - Online Budget Books
  - Workforce Planning
  - Financial Projections
- Procurement
  - Automated solicitation development
  - Optimized supplier engagement
  - Centralized contract management
  - Integrated collaboration, evaluation, and contract awarding systems
- Reporting and Transparency
  - Cross-suite reporting integration
  - Reporting Dashboards
  - Interactive summaries
  - Performance reporting
  - Community feedback
  - Emergency communication
  - Strategic planning and initiatives
  - Community-informed budgeting
  - Stakeholder engagement
  - Open Data
- Permitting and Licensing
  - Agile workflow processing software utilized across many cities within the United States to process applications or permits in the following areas:
    - Code Enforcement
    - Public Works

        - Business Licenses
        - Community Development
- Enterprise Asset Management
    - Asset management software for planning and workflow management in cities and counties across the country. Multiple departments use this software to deploy work crews and projects in the following areas:
        - Parks and Recreation
        - Storm Water Distribution
        - Facilities and Transportation

Principal Service Commitments and System Requirements

OpenGov designs its processes and procedures related to the development of Budgeting and Planning, Procurement, Reporting and Transparency, Enterprise Asset Management and Permitting and Licensing to meet its service objectives. The objectives are based on the service commitments that OpenGov makes to its customers, applicable laws and regulations that govern its services, and the financial, operational, and compliance requirements that OpenGov has established for the services. OpenGov aligns with the NIST Cybersecurity Framework and implements the NIST 800-53 series security controls whenever possible.

Security commitments to OpenGov customers are documented and communicated through its contract terms and conditions, its OpenGov/Trust page on its corporate website, and in the security addendums that are included with each customer contract. OpenGov serves only public institutions at the state and local levels, therefore OpenGov often utilize their contract language to ensure clarity around their unique security requirements. In addition to inheriting entity-level security controls from its cloud hosting providers, Amazon Web Services and Microsoft Azure, OpenGov also operates a robust corporate security program to ensure that its people, processes, and technology maintain the expectations of its customers and the requirements of its mission. The OpenGov security team is committed to fostering a culture of security throughout the company, enabling employees to conduct their required activities securely.

Governance around its security culture is found in the robust security policies managed by the Global Security Team. The security principles and guidance contained in these documents define parameters around access control (adopting least privilege), encryption (data in transit and at rest), threat and vulnerability management, risk management, and many others. In addition to the policies that govern the development, maintenance, and monitoring of its applications, OpenGov also provides extensive security guidance to its employees, through information security and acceptable use policies, as well as through annual training and phishing assessments.

Components of the System

Infrastructure

Primary infrastructure used to provide OpenGov’s OpenGov Services System includes the following:

Primary Infrastructure		
Hardware	**Type**	**Purpose**
CloudFlare	Web application firewall (WAF), domain name system (DNS), Domain Registration DNS and secure sockets layer (SSL)	Protects applications, application programing interfaces (APIs) and websites with WAF, denial-of-service attack (DDoS), API gateway, bot management and DNS and SSL certificates and Management for Custom Domains

Primary Infrastructure		
Hardware	**Type**	**Purpose**
AWS Environment Accounts	Segmenting its Environments, Flow and permissions	Environments are separated by accounts, which largely fall under 4 categories. • Development • Integration • Staging • Production
Virtual Private Cloud (VPC)	AWS VPC	Each account has 2 VPC's configured. The first VPC is where compute resources run and the second VPC is where infrastructure that stores data is run. These two VPC's are then peered together
Firewall	AWS Security Groups	Stateful firewall that restricts access to only the ports needed by external entities to connect with OpenGov services
Virtual Private Network (VPN)	Aviatrix VPN	Aviatrix Gateways are run in the Engineering Operations account and the compute VPC which hosts the VPN is then peered with the compute VPC's of the respective accounts. Product level profiles are created which allow engineers to only connect to the Compute VPC where their products are running
Teleport	Teleport	Teleport is used to provide Engineering access to the workloads running in the Compute VPC for debugging purposes. These connections are fully auditable and OpenGov is able to review commands and the output of those commands for auditing purposes
ALB	AWS Application Load Balancers	Automatically distributes incoming application traffic to the correct Ingress Controller
Proxy Server	Nginx Proxy Server	Automatically routes traffic to the correct service and distributes incoming traffic across multiple replicas
Kubernetes	AWS Elastic Kubernetes Service (EKS)	Container orchestration that automatically deploys its applications to the appropriate nodes in the cluster
Workload Autoscaling	Horizontal Pod Autoscaling and AWS Autoscaling groups	OpenGov leverages Horizontal Pod Autoscaling and AWS Autoscaling Groups where appropriate to automatically add capacity during times when there is increased load on its systems
Elastic Cloude Compute (EC2) Instances	Linux	OpenGov uses AWS Linux managed instances for of its Kubernetes workloads. This helps OpenGov to ensure that OpenGov is up to date on the latest patches and security features
Online Transaction Processing (OLTP) Database	AWS Relational Database Services (RDS)	PostgreSQL relational database management system software (RDBMS) for application data persistence and OLTP use cases

Primary Infrastructure		
Hardware	**Type**	**Purpose**
OLAP/Data Warehouse Database	AWS Redshift and DynamoDB	OpenGov uses AWS Redshift and DynamoDB to store, and query structured and semi-structured data for OLAP use cases
MongoDB	Atlas MongoDB	OpenGov uses Atlas MongoDB to store, and query unstructured data for OLAP use cases
Event Bus	Confluent Kafka	OpenGov uses Kafka as an asynchronous event bus that allows its services for coordination
Continuous Integration	Jenkins and GitHub Actions	OpenGov uses a combination of GitHub Actions and Jenkins to execute testing, build processes, and quality checks prior to deploying services to testing and production environments
Deployment	Spinnaker	Spinnaker is used by release managers to release the latest software into its production environments at the end of each sprint

Software

Primary software used to provide OpenGov's OpenGov Services System includes the following:

Primary Software		
Software	**Operating System**	**Purpose**
ADP	Software as a Service (SaaS)	OpenGov utilizes ADP for many of its Human Resource (HR) functions, including payroll, benefits administration, onboarding, PRO tracking and tax documentation
Artifactory	SaaS	OpenGov utilizes Artifactory for resource and container repository services
Atlassian	SaaS	OpenGov utilizes Atlassian's Confluence and Jira applications as its systems of record. Confluence serves as a document repository across teams and departments and is also used for internal information sharing. Jira is its ticketing system for IT and Engineering functions
AWS	Infrastructure as a Service (IaaS)	AWS is its cloud hosting platform for Budgeting and Planning, Procurement, Platform, and Enterprise Asset Management
CloudConvert	SaaS	OpenGov utilizes CloudConvert for file conversion services
Cloudflare	SaaS	OpenGov utilizes Cloudflare as its WAF
CloudStorageSec.com	SaaS	CloudStorageSecurity is utilized to scan uploads to its Procurement application for malware
Confluent	SaaS	OpenGov utilizes Confluent for managed Kafka services

Primary Software		
Software	**Operating System**	**Purpose**
DockerHub	SaaS	OpenGov utilizes DockerHub for container repository services
Esri/ArcGIS	SaaS	OpenGov utilizes Esri/ArcGIS for enterprise asset management (EAM) map services and login to the EAM product
Google Suite	SaaS	OpenGov utilizes the Google suite for e-mail communications and document collaboration
GitHub	SaaS	OpenGov utilizes GitHub as its code repository / VCS
Grafana	SaaS	OpenGov utilizes Grafana for centralized application and infrastructure analysis and monitoring
Lacework	SaaS	OpenGov utilizes Lacework for vulnerability scanning across its cloud assets such as servers and cloud infrastructure
Launch Darkly	SaaS	OpenGov utilizes Launch Darkly for feature flag management in its product suites
Lucidum	SaaS	Lucidum provides centralized asset management for OpenGov resources
Microsoft Azure	IaaS	Azure is its cloud hosting platform for Permitting and Licensing
Okta	SaaS	OpenGov utilizes Okta as its central identity provider for employee's. Okta provides single-sign-on (SSO) for corporate applications/resources
Orca	SaaS	OpenGov utilizes Orca for vulnerability scanning across its cloud assets such as servers and cloud infrastructure
ReliaQuest	SaaS	ReliaQuest is its managed security services provider
Salesforce (Slack)	SaaS	Slack is its internal collaboration and communication tool utilized across the enterprise
Salesforce Cloud	SaaS	Salesforce is its customer relationship management tool used to support its go-to-market (GTM) teams end to end
SendGrid	SaaS	OpenGov utilizes SendGrid as e-mail delivery service to send transactional and marketing e-mails
Teleport	SaaS	OpenGov utilizes Teleport for identity-native (Okta-native) infrastructure access
Tonic	SaaS	Tonic is utilized to anonymize data in its Permitting and Licensing and Procurement suites

Primary Software		
Software	**Operating System**	**Purpose**
Zoom	SaaS	Zoom is its virtual meeting and communication platform

People

OpenGov has over 750 employees organized in the following functional areas:

Corporate: Executive staff responsible for setting company objectives, defining operating models, evaluating and conducting mergers and acquisitions, growing investments and interacting with board members.

Financial: Led by the Chief Executive Officer, the financial team is responsible for budgeting and planning, accounts receivable and payables, corporate accounting functions, payroll, procurement, and billing.

Legal: its general counsel and staff are responsible for legal matters within OpenGov, including policy, vendor and customer contracts, litigation, and more.

Security: Management of the people, processes and technology necessary to manage the security of OpenGov. This includes risk management, vendor management, incident response, detecting and monitoring, compliance, infrastructure and advising on customer engagements and contracts.

Business Operations and Systems: This includes its corporate IT functions, including tools, equipment, collaboration and communication tools, business systems, onboarding, SSO management and account provisioning, etc.

Research and Development (R&D): Led by the Chief Technology Officer (CTO), the R&D organization is responsible for engineering functions related to the development, testing, change management, implementation and production of its application suites.

Product: Led by the Chief Product Officer, the Product teams focus on the customer requirements, design features, platform requirements and user experience associated with applications and suites. The Product teams collaborate with the R&D organization to establish the technical and budget requirements needed to create and implement features on a quarterly basis.

Field Operations: Led by its President of Field Operations, this organization houses customer facing teams within OpenGov. its Sales team is responsible for acquiring new customers and business for OpenGov. The Customer Support teams act as a help desk for its customers, engaging with them via defined SLA's to provide guidance and solve problems relating to customer implementations of its applications. its Professional Services teams are contracted as part of the sales agreement to manage the training and implementation of its services within the customer environment on a project basis. The Customer Success Team is assigned once a customer is onboarded to grow and maintain the relationship, share updates on new features, guide on possible use cases and overall drive the renewal of the contract. The Marketing team is responsible for demand generation for OpenGov services. They accomplish this through advertisements and press engagements, conducting webinars and its annual customer conference, creating public facing content about the services of OpenGov, and managing the participation in conferences and events for the OpenGov user community.

People Team: Led by its Senior Vice-President (SVP) of People, this team manages traditional Human Resources functions. These include recruitment, onboarding, training, employee benefits, compensation analysis, performance management, leadership development, and driving company culture.

Data

OpenGov defines and classifies its data in the following ways:

- Any Data that is entered through the ERP SAAS service by a Customer or a constituent (Third-party Service user) is Classified as Customer Data and is classified as Highly Confidential Data.
- Any Data that is Intended for Release through its Reporting and Transparency platform remains Highly Confidential until the Customer releases the data as Public Data.
- Data in transit as part of an Integration is Customer data and is Highly Confidential.
- Any Report, Story, Output, or Input directly from a customer or generated by the customer is Highly Confidential until released to the Public by the customer, which becomes Public Data.
- Any internal OpenGov Report input or output that includes Customer Data is Classified as Highly Confidential Data.
- Any Customer Data in a transaction Process or Storage is Encrypted and Considered Highly Confidential Data.
- Any Production System with direct access to Customer Data is Classified as a “Production System,” and any data related to the system is Classified as Highly Confidential.
- Security Information and Logging/Monitoring of Production Systems, along with any data output, is considered Highly Confidential.
- Other Systems and data are Classified in accordance with the Information Classification Policy and include appropriate controls based on NIST CSF and NIST SP800-53 Controls.

Data Protections

OpenGov has several protections and controls specific to data across its Technology Platform. its Data Classification Policy classifies Data; Customer data is encrypted in storage and transport by FIPS encryption guidance. Data handling takes place specific to appropriate network zones, and Production data is separated from other activities to include pre-production, development, testing, and QA. File Integrity Management is in place across its entire infrastructure. its Security tooling monitors the data integrity of resources that make up its Cloud ERP offering, to include: system files, data storage, and other SaaS-related resources. its product lines include error handling, reporting, and remediation guidance. its logging and monitoring and ops management capability allows OpenGov to identify errors, incidents, vulnerabilities, and service issues for quick identification and remediation in support of security and operational SLAs. Access is provided in accordance with the concept of least privilege and within the parameters of the role of the individual requiring access.

Data Availability

OpenGov’s databases use a multi-AZ deployment strategy to provide enhanced availability and durability. OpenGov captures regular backups and snapshots of its databases which are stored in regional data centers at a regular cadence to be used in the unlikely event of a data loss.

Data is replicated in real-time to separate data centers across AWS and Azure availability zones, which allows OpenGov to switch to a replicated database in the event of a data center or hardware fault, limiting data loss to one minute.

Data Isolation and Confidentiality

Application services are configured to run in isolated namespaces and containers on the cluster hosts with strict resource limits that prevent data leaks and unexpected or malicious activity in one service from affecting others. A minimum number of replicas of each service is deployed for high availability.

Processes, Policies and Procedures

Formal IT policies and procedures exist that describe logical access, computer operations, change control, and data communication standards. Teams are expected to adhere to the OpenGov policies and procedures that define how services should be delivered. These are located on the Company's Intranet and can be accessed by any OpenGov team member.

Physical Security

The infrastructure supporting the production environment is hosted within AWS and Azure. As such, the responsibility for the physical protections of this equipment is the responsibility of AWS and Azure. For a listing of controls implemented by AWS and Azure, please refer to the 'Subservice organizations' section, below.

Logical Access

OpenGov's access and authorization strategies are founded on the principles of Least Privileges, and Role-Based Access Controls which are governed by NIST password guidelines. Internally, system owners will (whenever possible) connect their applications/systems with OKTA to achieve Single-Sign-on and multi-factor authentication (MFA). This also allows for automated onboarding and offboarding of OpenGov Users.

OpenGov follows the "least privilege" concept. Only the minimum necessary system preferences required to perform job duties are granted to an individual. The following measures have been put in place to ensure compliance with the least privilege requirements:

Explicit authorization is granted thru the account authorization process to receive authorized access to a service provider-defined list of security functions and relevant security information.

Individuals with access to information system accounts, roles, or other security functions are required to use a unique, non-privileged account when performing non-administrative functions.

Privileged accounts on the information system are restricted to predefined personnel or roles.

Information systems regularly audit the execution of privileged functions.

Non-privileged users are prevented from executing privileged functions, including disabling, circumventing, or altering implemented security safeguards or countermeasures.

Approved authorizations for logical access to the system will be enforced in accordance with the OpenGov Authorization and Access Policy and should be, identity-based, role-based, attribute-based and governed by OpenGov's Access Review Committee.

Usage restrictions, configuration and connection requirements, and implementation guidance have been established and documented for each type of remote access allowed by OpenGov. Remote access to the information system is authorized before allowing such connections.

Wireless access to information systems are explicitly authorized before establishing connections and wireless access to the system is protected using authentication and encryption while ensuring authentication is applied to users, devices, or both as necessary.

OpenGov has implemented usage restrictions and implementation guidance for organization-controlled mobile devices. Endpoint connections, given they meet established usage restrictions, are authorized and full-device encryption and/or container encryption will be implemented to protect the confidentiality and integrity of the information on defined endpoints.

Customer’s access OpenGov services through the Internet using the SSL functionality of their web browser. These customers supply a valid user ID and password to gain access to customer cloud resources authenticating against customer Active Directory (AD) or LDAP. Passwords conform to customer password configuration requirements or OpenGov’s password requirements enforced by Auth0.

Computer Operations - Backups

OpenGov was architected to be fully cloud-based to ensure availability.

Customer data is backed up offsite with its cloud service providers on a continuous basis. OpenGov takes full advantage of features like automated RDS backups, automated AMI snapshots, and availability zones. Environmental systems are designed to minimize the impact of disruptions to operations, and multiple geographic regions and Availability Zones increase resilience in the face of most failure modes, including natural disasters or system failure.

OpenGov also maintains its own defined policies and procedures for operational backups. Backup tests are run periodically as defined by its policies to ensure its data is backed up as expected. its procedures define its RPO and RTO, and its incident response and disaster recovery plans and procedures require annual testing to ensure impacted employees are aware of their responsibilities.

Computer Operations - Availability

Incident response policies and procedures are in place to guide personnel in reporting and responding to information technology and security incidents. Procedures exist to identify, report, and act upon system security breaches and other incidents. Incident response runbooks are in place to properly triage, classify and mitigate incidents.

OpenGov continuously monitors the utilization of its cloud infrastructure to ensure that service delivery matches its service level agreements. OpenGov follows best practices for auto-scaling and capacity management to ensure its current and future operating models are maintained.

OpenGov relies on its cloud service providers for the patching of its infrastructure based on their publicized policies and procedures and defined contractual requirements.

OpenGov has implemented a patch management program to ensure its applications are patched in accordance with vendor recommendations and according to its Threat and Vulnerability Management policy. Vulnerabilities are analyzed to determine their level of risk to OpenGov applications and implemented based on its defined procedures.

Change Control

OpenGov maintains a documented System Development Lifecycle program to ensure development activities are performed to documented procedures. A mature Change Management program is in place, including the control of processes for initializing, changing and monitoring the configurations of its system and applications throughout the product life cycle.

OpenGov embraces an agile development model to support its growing suites. its unified change management process includes guidance for:

- New software releases including new feature releases and hotfixes.
- Infrastructure maintenance and updates.
- Updates to internal tooling used within OpenGov e.g., Confluence, JIRA, GitHub etc.

Jira Service Management is its system of record to create, view and approve change requests. Detailed procedures for submitting, approving/denying, and completing a change request are communicated widely via Confluence.

OpenGov has migrated to a serialized approval flow to enable a more streamlined and single ownership approach, outlined in its Change Management Policy.

Quality assurance testing and User Acceptance Testing (UAT) results are documented and maintained with the associated change request. Development and testing are performed in an environment that is logically separated from the production environment. Management approves changes prior to migration to the production environment and documents those approvals within the ticketing system.

Version control software is utilized to maintain source code versions and migrate source code through the development process to the production environment. The version control software maintains a history of code changes to support rollback capabilities and tracks changes to developers.

Data Communications

Firewall systems are in place to filter unauthorized inbound network traffic from the Internet and deny any type of network connection that is not explicitly authorized. Network address translation (NAT) functionality is utilized to manage internal IP addresses. Administrative access to the firewall is restricted to authorized employees, and that access is reviewed on a weekly basis.

For public facing Internet applications and services provided by OpenGov for the use of its customers: Cloudflare Services, including but not limited to reverse proxy and web application firewall, are used to filter and block nefarious traffic.

Redundancy is built into the system infrastructure supporting the data center services to help ensure that there is no single point of failure that includes firewalls, routers, and servers. In the event that a primary system fails, the redundant hardware is configured to immediately take its place.

Penetration testing is conducted to measure the security posture of a target system or environment. The third-party vendor uses an accepted industry standard penetration testing methodology specified by OpenGov. The third-party vendor’s approach begins with a vulnerability analysis of the target system to determine what vulnerabilities exist on the system that can be exploited via a penetration test, simulating a disgruntled/disaffected insider or an attacker that has obtained internal access to the network. Once vulnerabilities are identified, the third-party vendor attempts to exploit the vulnerabilities to determine whether unauthorized access or other malicious activity is possible. Penetration testing includes network and application layer testing as well as testing of controls and processes around the networks and applications and occurred from outside the network. Results of the penetration test were shared with executive management and added to the risk register for remediation.

Simulated phishing assessment are also conducted by the Global Security Team to assess the awareness of employees on how to identify a phishing e-mail and how to report it properly for investigation and mitigation.

OpenGov has implemented a robust security stack for the detection and monitoring of threats to its environment. Vulnerability scanning is performed continuously according to its defined requirements. These technologies are customized to test the organization's infrastructure and software in an efficient manner while minimizing the potential risks associated with active scanning. Retests and on-demand scans are performed on an as needed basis. Scans are performed during non-peak windows. Tools requiring installation in the OpenGov system are implemented through the Change Management process. Scanning is performed with approved scanning templates and with bandwidth-throttling options enabled.

Authorized employees may access the system through the Internet through the use of leading VPN technology. Employees are authenticated through the use of a MFA system.

Boundaries of the System

The scope of this report includes the OpenGov Services System performed in the San Francisco, California facilities.

This report does not include the cloud hosting services provided by AWS and Azure at the various facilities.

Changes to the System in the Last 12 Months

OpenGov expanded the scope of the system to include 2 additional suites: Enterprise Asset Management and Permitting and Licensing. Enterprise Asset Management was fully integrated effective June 15, 2023 and Permitting and Licensing was fully integrated effective September 15, 2023. For more details on the offerings related to these products refer to the “Description of Services Provided” above.

Incidents in the Last 12 Months

No significant incidents have occurred to the services provided to user entities in the 12 months preceding the end of the review period.

Criteria Not Applicable to the System

All Common/Security, Availability, Processing Integrity, and Confidentiality criteria were applicable to the OpenGov Services System.

Subservice organizations

This report does not include the cloud hosting services provided by AWS and Azure at the various facilities.

Subservice Description of Services

AWS and Azure provide cloud hosting services.

Complementary Subservice organizations Controls

OpenGov’s services are designed with the assumption that certain controls will be implemented by subservice organizations. Such controls are called complementary subservice organizations controls. It is not feasible for all of the trust services criteria related to OpenGov’s services to be solely achieved by OpenGov control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of OpenGov.

The following subservice organizations controls should be implemented by AWS and Azure to provide additional assurance that the trust services criteria described within this report are met:

Subservice organizations - AWS		
Category	**Criteria**	**Control**
Common Criteria	CC6.4, CC7.2	Physical access to data centers is approved by an authorized individual.
		Physical access is revoked within 24 hours of the employee or vendor record being deactivated.
		Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.

Subservice organizations - AWS		
Category	**Criteria**	**Control**
		Physical access points to server locations are recorded by closed circuit television camera (CCTV). Images are retained for 90 days, unless limited by legal or contractual obligations.
		Physical access points to server locations are managed by electronic access control devices.
		Electronic intrusion detection systems (IDS) are installed within the data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents.
Availability	A1.2	Data centers are protected by fire detection and suppression systems.
		Data centers are air conditioned to maintain appropriate atmospheric conditions. Personnel and systems monitor and control air temperature and humidity at appropriate levels.
		Uninterruptible Power Supply (UPS) units provide backup power in the event of an electrical failure in Amazon-owned data centers.
		Data centers have generators to provide backup power in case of electrical failure.
		Contracts are in place with third-party colocation service providers which include provisions to provide fire suppression systems, air conditioning to maintain appropriate atmospheric conditions, UPS units, and redundant power supplies.
		Monitoring and alarming are configured by Service Owners to identify and notify operational and management personnel of incidents when early warning thresholds are crossed on key operational metrics.

Subservice organizations - Azure		
Category	**Criteria**	**Control**
Common Criteria/Security	CC6.4, CC7.2	Procedures have been established to restrict physical access to the Azure datacenter to authorized employees, vendors, contractors, and visitors.
		Security verification and check-in are required for personnel requiring temporary access to the interior Azure datacenter facility including tour groups or visitors.
		Physical access to the Azure datacenter is reviewed quarterly and verified by the Datacenter Management team.
		Physical access mechanisms (e.g., access card readers, biometric devices, man traps / portals, cages, locked cabinets) have been implemented and are administered to restrict access to authorized individuals.
		The Azure datacenter facility is monitored 24x7 by security personnel.
Availability	A1.2	Datacenter Management team maintains and tests datacenter-managed environmental equipment within the facility according to documented policy and maintenance procedures.

Subservice organizations - Azure		
Category	Criteria	Control
		Environmental controls have been implemented to protect systems inside datacenter facilities, including temperature and heating, ventilation, and air conditioning (HVAC) controls, fire detection and suppression systems, and power management systems.
		Datacenter physical security management reviews and approves the incident response procedures on a yearly basis. The incident security response procedures detail the appropriate steps to be taken in the event of a security incident and the methods to report security weaknesses.
		Backups of key Azure service components and secrets are performed regularly and stored in fault tolerant (isolated) facilities.
		Critical Azure components have been designed with redundancy to sustain isolated faults and minimize disruptions to customer services.
		Customer data is automatically replicated within Azure to minimize isolated faults.
		Data Protection Services (DPS) backs up data for properties based on a defined schedule and upon request of the properties. Data is retained according to the data type identified by the property. DPS investigates backup errors and skipped files and follows up appropriately.
		Backup restoration procedures are defined, and backup data integrity checks are performed through standard restoration activities.
		Offsite backups are tracked and managed to maintain accuracy of the inventory information.
		Production data is encrypted on backup media.
		Azure services are configured to automatically restore customer services upon detection of hardware and system failures.

OpenGov management, along with the subservice organizations, define the scope and responsibility of the controls necessary to meet all the relevant trust services criteria through written contracts, such as service level agreements. In addition, OpenGov performs monitoring of the subservice organizations controls, including the following procedures:

- Annual reviews of third-party attestations, security audits or related documentation for each service provider.
- Frequent online meetings with service partners to keep service delivery needs top of mind.
- Monitoring external/public communications (such as news stories, social media posts or customer complaints) relevant to the vendor or service provider.
- Continuous monitoring of tool capabilities as related to contracts or SLA's and documenting requests for change or improvement as needed.

COMPLEMENTARY USER ENTITY CONTROLS

OpenGov's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all of the Trust Services Criteria related to OpenGov's services to be solely achieved by OpenGov control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of OpenGov's.

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

OpenGov service providers and user entities are expected to:

1. Understand and comply with contractual obligations to OpenGov.
2. Notify OpenGov of any changes made to technical or administrative controls.
3. Maintain their own systems of record.
4. Ensure the supervision, management and control the use of OpenGov services by their personnel.
5. Develop, test and maintain their own disaster recovery and business continuity plans that address the inability to access or utilize OpenGov services.
6. Immediately notify OpenGov of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.