System and Organization Controls (SOC) 3 Reporting

Independent Service Auditor's Report

A SOC 3 Independent Service Auditor's Report on BI Incorporated Description of Its TotalAccess Electronic Monitoring System Relevant to

Security, Availability, and Confidentiality

throughout the Period July 1, 2025, to October 15, 2025

TEVORA

17400 Laguna Canyon Road, Suite 150 | Irvine, California 92618

Management's Assertion Regarding the Effectiveness of Its Controls over the BI TotalAccess® Electronic Monitoring System Based on the Trust Services Criteria for Security, Availability, and Confidentiality

We are responsible for designing, implementing, operating, and maintaining effective controls within BI Incorporated (BI) TotalAccess Electronic Monitoring System (system) throughout the period July 1, 2025, to October 15, 2025, to provide reasonable assurance that BI service commitments and system requirements relevant to security, availability, and confidentiality were achieved. Our description of the boundaries of the system is presented in **Attachment A** and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period July 1, 2025, to October 15, 2025, to provide reasonable assurance that BI service commitments and system requirements were achieved based on the applicable trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy. BI objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in **Attachment B**.

The Service Organization uses Amazon Web Services, Cognitec, Transperfect, Verizon, GeneSys, and Voice Biometrics Group (subservice organizations) for cloud hosting, facial recognition, language translation, device connectivity, and call center services. This assertion and the description of the boundaries of the TotalAccess Electronic Monitoring System based on the Trust Services Criteria for Security, Availability, and Confidentiality (Attachment A) indicate that complementary user entity controls that are suitably designed and operating effectively are necessary to achieve BI service commitments and system requirements based on the applicable trust services criteria. The accompanying description of the boundaries of the TotalAccess Electronic Monitoring System based on the Trust Services Criteria for Security, Availability, and Confidentiality presents the types of complementary subservice organization controls assumed in the design of BI controls. The actual controls at the subservice organizations are not disclosed.

This assertion of the description of the boundaries of the TotalAccess Electronic Monitoring System based on the Trust Services Criteria for Security, Availability, and Confidentiality indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at BI to achieve service commitments and system requirements related to BI based on the applicable trust services criteria. The accompanying description of the boundaries of the TotalAccess Electronic Monitoring System based on the Trust Services Criteria for Security, Availability, and Confidentiality presents the complementary user entity controls assumed in the design of BI 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 July 1, 2025, to October 15, 2025, to provide reasonable assurance that BI Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria.

December 15, 2025

Report of Independent Service Auditors

To: Management of BI Incorporated

SCOPE

We have examined the accompanying assertion of BI Incorporated (BI or Service Organization) related to its TotalAccess Electronic Monitoring System (system) titled, "Management's Assertion Regarding the Effectiveness of its Controls over the TotalAccess Electronic Monitoring System based on the Trust Services Criteria for Security, Availability, and Confidentiality" (assertion) that the controls within BI were effective throughout the period July 1, 2025, to October 15, 2025, to provide reasonable assurance that BI service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).

The accompanying assertion and the description of the boundaries of the TotalAccess Electronic Monitoring System based on the Trust Services Criteria for Security, Availability, and Confidentiality (Attachment A) indicate that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at BI to achieve service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the TotalAccess Electronic Monitoring System based on the Trust Services Criteria for Security, Availability, and Confidentiality presents the complementary user entity controls assumed in the design of BI 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.

The Service Organization uses Amazon Web Services, Cognitec, Transperfect, Verizon, GeneSys, and Voice Biometrics Group (subservice organizations) for its hosting of physical and virtual servers, network management, and data protection and storage services. The accompanying assertion and the description of the boundaries of the TotalAccess Electronic Monitoring System based on the Trust Services Criteria for Security, Availability, and Confidentiality indicate that certain service commitments and system requirements based on the applicable trust services criteria can be met only if certain types of controls that management expects to be implemented at the subservice organizations are suitably designed and operating effectively. The description of the boundaries of the TotalAccess Electronic Monitoring System based on the Trust Services Criteria for Security, Availability, and Confidentiality presents the types of complementary subservice organization controls assumed in the design of the Service Organization's controls. Our

examination did not include the services provided by the subservice organizations, and we have not evaluated whether the controls management expects to be implemented at the subservice organizations have been implemented or whether such controls were suitability designed and operating effectively throughout the period July 1, 2025, to October 15, 2025.

SERVICE ORGANIZATION'S RESPONSIBILITIES

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

SERVICE AUDITOR'S RESPONSIBILITIES

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

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that controls were not effective to achieve BI service commitments and system requirements based on the applicable trust services criteria
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve BI service commitments and system requirements based the applicable trust services criteria

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

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

SERVICE AUDITOR'S INDEPENDENCE AND QUALITY CONTROL

We have complied with the independence and other ethical requirements of the Code of Professional Conduct established by the AICPA. We applied the statements on quality control standards established by the AICPA and, accordingly, maintain a comprehensive system of quality control.

INHERENT LIMITATIONS

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual report users may consider important to meet their informational needs.

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

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

OPINION

In our opinion, management's assertion that the controls within BI TotalAccess Electronic Monitoring System were effective throughout the period July 1, 2025, to October 15, 2025 if complementary subservice and user entity controls contemplated in the design of the Service Organization's controls operated effectively, to provide reasonable assurance that BI service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Miami, FL
December 15, 2025

Attachment A—Description of the Boundaries of BI Incorporated TotalAccess® Electronic Monitoring System

Company Overview

BI Incorporated (BI or the Company), founded in 1978 and acquired by The GEO Group, Inc. in 2010, is a leading provider of electronic monitoring technologies and community supervision services to government agencies across the United States and its territories. The Company supports community corrections agencies who monitor individuals on parole, probation, and pre-trial release through innovative, reliable tools that promote compliance, while enabling supervised individuals to remain in the community. BI solutions are designed to provide agencies with timely, accurate location and status information while maintaining strong controls over security, availability, and confidentiality.

Description of Products and Services Provided

The in-scope system is the BI TotalAccess Electronic Monitoring System (TotalAccess or the System), a cloud-based, multi-tenant platform that delivers integrated case management and real-time monitoring capabilities to local, state, and federal agencies.

TotalAccess combines a secure web application with back-end infrastructure and associated mobile applications. Authorized agency personnel access the System via role-based logins to enroll supervised individuals, assign monitoring technologies, configure real-time alerts (e.g., geolocation zone violations), review event data, and manage cases. Data streams from monitoring devices flow into TotalAccess, triggering alerts and enabling officer notification and response.

The scope of this examination includes the infrastructure, servers, software, and processes within the BI authorization boundary that supports TotalAccess, mobile applications, as well as the receipt and processing of data transmitted from devices used by agency personnel or worn or used by supervised individuals. Excluded from scope are the physical monitoring hardware and devices themselves, cellular transmission networks, customer-initiated third-party integrations via APIs, and non-monitoring services (e.g., legal advisory, translation, or marketing offerings).

Components of the TotalAccess® System

- **Infrastructure**—The System operates in a cloud-hosted environment managed by subservice providers. BI maintains logical control over virtual infrastructure, networking configurations, and application hosting within defined boundaries.

- **Software and Applications**—Core components include the backend system for processing and data storage, web-based user interface for case management and alerting, and mobile applications that enable field access for authorized personnel.
- **People**—Dedicated teams oversee security, operations, and compliance, including an information security function responsible for policy governance, risk assessment, vulnerability management, and incident response. Access provisions and reviews are performed by designated account managers and application owners.
- **Data**—The System processes sensitive location, alert, and case data pertaining to supervised individuals and agency personnel. Data is logically segregated by customer agency (multi-tenant isolation), classified according to sensitivity, and protected through encryption in transit and at rest.
- **Processes**—Key operational processes include, but are not limited to, logical access management, user access reviews, change management, incident detection and response, vulnerability scanning and remediation, system monitoring, and backup and recovery procedures.

Control Environment Overview

BI Incorporated maintains an integrated control environment designed to provide reasonable assurance that the System achieves its objectives related to security, availability, and confidentiality. Select high-level aspects include:

- **Logical and Physical Access Controls**—Access is granted on a least-privilege, role-based model. New hires receive automated provisioning from Human Resources (HR) systems, while terminations trigger daily revocation across all platforms. Quarterly access reviews are performed by application owners, with evidence retained of population completeness and termination actions. All remote access and password recovery require Multi-Factor Authentication (MFA).
- **Password Management**—Strong composition rules are enforced (minimum length, uppercase/lowercase, numeric, special characters, minimum character changes, and password history).
- **Data Protection**—Customer data is logically separated to prevent cross-agency access. Encryption is applied to data in transit and at rest.
- **Change Management**—System changes are managed through defined processes. During the period of July 1, 2025, to October 15, 2025, no material changes were implemented that affected the achievement of the applicable Trust Services Criteria.
- **Security Operations**—Continuous monitoring, vulnerability scanning, and an incident response process are in place to identify, assess, and respond to potential threats in a timely manner.

Subservice Organizations

BI Incorporated relies on subservice organizations for certain supporting functions, primarily cloud infrastructure hosting and related services. Controls at these subservice organizations related to physical and environmental safeguards are excluded from the scope of this examination. BI monitors subservice organization performance and controls through periodic review of third-party assurance reports (e.g., SOC reports) and contractual compliance.

Responsibilities of Users of the System

The security, availability, and confidentiality of the TotalAccess System is a shared responsibility between BI Incorporated and its customer agencies. Certain controls necessary to achieve the Trust Services Criteria are the responsibility of customer agencies, including:

- Management of agency-specific user permissions, policies, and login credentials
- Proper configuration of agency-defined alerts, zones, and integration settings
- Protection of agency endpoints and networks used to access the System

BI controls are designed with the assumption that customer agencies implement reasonable complementary controls in their environments.

This description provides a high-level overview of the TotalAccess Electronic Monitoring System and relevant control environment as of October 15, 2025, and throughout the period July 1, 2025, to October 15, 2025.

Attachment B—Principal Service Commitments and System Requirements

BI Incorporated designs its processes and procedures related to the TotalAccess Electronic Monitoring System to meet its objectives for the services provided. These objectives derive from service commitments made to customer agencies (governmental entities), applicable laws and regulations, and the Company's own operational and compliance requirements.

Security, availability, and confidentiality commitments to customer agencies are documented and communicated in customer agreements, service descriptions, and related contractual terms. Such commitments are standardized and include, but are not limited to, the following:

- BI maintains commercially reasonable administrative, physical, and technical safeguards to protect the security, availability, and confidentiality of the System and customer data.
- Logical access controls are implemented based on least privilege, with ongoing monitoring and review.
- An incident response process is in place to identify, respond to, and communicate security events in a timely manner.
- Vulnerability management processes identify and remediate vulnerabilities promptly.
- Customer data is logically separated to prevent unauthorized cross-tenant access.
- Encryption technologies protect data at rest and in transit.
- BI does not disclose confidential information except as required to perform services or as permitted by agreement.
- BI uses commercially reasonable efforts to ensure System availability consistent with service objectives.

BI establishes operational requirements that support the achievement of these commitments, relevant laws and regulations, and other system requirements. These are communicated through policies, procedures, system design documentation, and contracts. Information security policies provide an organization-wide approach to protection, covering system design, development, operation, and employee responsibilities. Standard operating procedures document key processes required for System operation.

BI Incorporated has not omitted or distorted information relevant to TotalAccess while acknowledging that this description has been prepared to meet the common needs of a broad range of report users and may not include every aspect of the system that each individual user may consider important.