8-K 1 trck8k.htm CURRENT REPORT

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
Washington, DC 20549

FORM 8-K

CURRENT REPORT

Pursuant to Section 13 or 15(d) of the
Securities Exchange Act of 1934

Date of Report (Date of earliest event reported): August 7, 2020

TRACK GROUP, INC.

(Exact name of Registrant as specified in its Charter)

Delaware	000-23153	87-0543981
(State or other jurisdiction of incorporation)	(Commission File No.)	(IRS Employer Identification No.)

200 E. 5th Avenue, Suite 100, Naperville, Illinois 60563
(Address of principal executive offices)

(877) 260-2010
(Registrant's Telephone Number)

Not Applicable
(Former name or address, if changed since last report)

Check the appropriate box below if the Form 8-K filing is intended to simultaneously satisfy the filing obligation of the registrant under any of the following provisions (see General Instruction A.2. below):

□ Written communications pursuant to Rule 425 under the Securities Act (17 CFR 230.425)

□ Soliciting material pursuant to Rule 14a-12 under the Exchange Act (17 CFR 240.14a-12)

□ Pre-commencement communications pursuant to Rule 14d-2(b) under the Exchange Act (17 CFR 240.14d-2(b))

□ Pre-commencement communications pursuant to Rule 13e-4(c) under the Exchange Act (17 CFR 240.13e-4(c))

Indicate by check mark whether the registrant is an emerging growth company as defined in Rule 405 of the Securities Act of 1933 (17 CFR 230.405) or Rule 12b-2 of the Securities Exchange Act of 1934 (17 CFR 240.12b-2) □

If an emerging growth company, indicate by check mark if the registrant has elected not to use the extended transition period for complying with any new or revised financial accounting standards provided pursuant to Section 13(a) of the Exchange Act □

Item 1.01 Entry into a Material Definitive Agreement.

On August 7, 2020, Track Group, Inc. (the "*Company*") entered into a forty-one month Monitoring Services Agreement (the "*Agreement*") with Gendarmeria de Chile, the Republic of Chile's uniform prison service ("*Gendarmeria*"). Pursuant to the terms of the Agreement, the Company provides Gendarmeria with GPS monitoring devices, certain services, and software to be used for offenders ordered into a corrections program by the Chilean courts. In exchange for the products and services provided by the Company, Gendarmeria shall make periodic payments, the sum of which shall be determined based on the duration of use of individual units of equipment.

The foregoing description of the Agreement does not purport to be complete, and is qualified in its entirety by reference to the full text of the Agreement, attached to this Current Report on Form 8-K as Exhibit 10.1, and incorporated by reference herein. Exhibit 10.1 has been translated into English from its original text in Spanish.

Item 9.01 Financial Statements and Exhibits.

See Exhibit Index.

SIGNATURES

Pursuant to the requirements of the Securities Exchange Act of 1934, the registrant has duly caused this report to be signed on its behalf by the undersigned hereunto duly authorized.

TRACK GROUP, INC.

Date: August 17, 2020

By: */s/ Peter K. Poli*

Peter K. Poli
Chief Financial Officer

EXHIBIT INDEX

Exhibit No.	Description
10.1*	Monitoring Services Agreement between Track Group, Inc. and Gendarmeria de Chile, the Republic of Chile's uniform prison service, dated July 29, 2020

* Confidential portions of the exhibit have been redacted from the filed version of the exhibit and are marked with a [***]

Exhibit 99.1

CERTAIN IDENTIFIED INFORMATION HAS BEEN EXCLUDED FROM THE EXHIBIT BECAUSE IT IS BOTH (i) NOT MATERIAL, AND (ii) WOULD BE COMPETITIVELY HARMFUL IF PUBLICLY DISCLOSED. REDACTED MATERIAL IS MARKED WITH A [***].

CONTRACT

TELEMATIC MONITORING SERVICES FOR OFFENDERS
TRACK GROUP CHILE S.P.A
&
GENDARMERÍA OF CHILE

In Santiago of Chile, on the 29 of July 2020, on the one hand, Christian Arnaldo Alveal Gutiérrez, Chilean, national identity card No. 11,351,205-9, in his capacity as National Director of the Gendarmerie of Chile, according to will accredit, a public service dependent on the Ministry of Justice and Human Rights, domiciled at Rosas street #. 1264, commune of Santiago, Metropolitan Region, hereinafter "the Service" or "the Institution" and, on the other hand, Diego Peralta Valenzuela, Chilean, national identity card No. 5,009,310-7,and Vesca Paola Camelio Ursic, Chilean, identity card No. 8.322.805-9, representing, as will be accredited the company Track Group Chile S.p.A. RUT: 76,321,923-2, with address at Enrique Foster Sur Street #. 29, floor 5, commune of Las Condes, Metropolitan Region, hereinafter “the supplier”, who state that they have agreed to the following contract, according to the clauses that are expressed below:

FIRST: PURPOSE OF THE CONTRACT.

Through this contract, the provider agrees to provide the telematics monitoring service for offenders, in accordance with the requirements established by the Institution through the bidding process ID 634-35-LR17, which constitutes the main object of the contract, and from which a series of obligations originate.

The service that is contracted must faithfully comply with the conditions established in the administrative and technical bases, and what is required in its annexes, and must correspond, exactly, in terms of said characteristics, to those that the supplier detailed in its offer.

In accordance with the foregoing, the service to be provided must include, among other aspects, the provision of monitoring software; provision, installation, replacement and removal of monitoring devices; training of Gendarmerie personnel; the enablement, start-up and maintenance of the comprehensive monitoring and management system, in its entirety, of the National Monitoring Center and the Regional Center for Simultaneous Monitoring, all in accordance with the provisions of the technical bases and the offer by the provider.

SECOND: IMPLEMENTATION.

1. Planning.

a) MILESTONE No. 1 “Activities necessary for commissioning: Migration process, data reception, system configuration and infrastructure enablement”:

CERTAIN IDENTIFIED INFORMATION HAS BEEN EXCLUDED FROM THE EXHIBIT BECAUSE IT IS BOTH (i) NOT MATERIAL, AND (ii) WOULD BE COMPETITIVELY HARMFUL IF PUBLICLY DISCLOSED. REDACTED MATERIAL IS MARKED WITH A [***].

The supplier must comply with all the activities contemplated in Milestone No. 1 within 120 calendar days, as provided in section number X, of the technical bases, its annexes and other aspects of its offer.

In the development of milestone No. 1, the supplier will be guided by the deadlines set out in the Gantt letter that accompanied the technical annex No. 18 of its offer, regarding the duration, start and end of the detailed activities for the projects of authorization of the National Monitoring Center, Regional Center of Simultaneous Monitoring, and the provisional authorization of the Monitoring Center. The provider will keep the Institution's Technical Counterparty informed of the progress of the activities contemplated in the Gantt letter.

For these purposes, the Institution must formally deliver the dependencies, drawing up the corresponding minutes and inventory, from which time the terms will begin to count.

The activities that the supplier must carry out, considered within Milestone No. 1, are the following:

a.1) Habilitation of the National Monitoring Center and the Regional Simultaneous Monitoring Center.

a.2) Provisional habilitation of a monitoring center, of modular architecture, in order to ensure the continuity of the service for a period of at least 180 days, while carrying out the own infrastructure habilitation works. For these purposes, you must appoint a project manager, with whom the technical counterpart will interact.

a.3) Installation of all the necessary hardware, software and telecommunication links in the communications room, and enabling of backup, in virtual cloud.

a.4) Installation of the monitoring system, considering all the hardware, software, local data network cabling, power backup and necessary telecommunications links, including remote connectivity activities with the Social Reintegration Centers, through from the Gendarmerie of Chile backbone.

a.5) Training and delivery of proposed training manuals for the use of required computer applications, and related hardware elements, including those related to power backup equipment, anti-fire system, etc.

a.6) Delivery of acceptance test protocol, which must include, at least, the verification of the functionalities indicated in letter b) of number X of the technical bases, which must be approved by the Institution.

a.7) Compliance with the Gantt Letter delivered under the previous contract, which contains the general migration planning, and which will begin the last six months before the end of the respective contract.

The minimum processes that planning must ensure during migration are:

1. - Backup of historical information in the database.
2. - Backup of the database configuration files.

3. - Backup of the configuration files of parameters defined in the processing servers. The supplier must submit a document detailing the model or structure of the database.
4. - Device change process in case of parallel operation between companies.

In accordance with said processes and the information provided, the provider must initiate the data migration process towards the offered system, trying to configure it, so that it meets the objective of maintaining it for at least six months counted from the end of the previous contract, the continuity of the current telematics monitoring service of offenders, with the monitoring devices provided under the previous contract.

Once the supplier notifies the technical counterpart of the Gendarmerie, which is in a position to start the commissioning of the project, or once the term of 120 calendar days contemplated for its execution has expired, it will proceed to receive Milestone No. 1.

Said reception will have a term of 10 working days, period in which, the Institution will proceed to the verification of the fulfillment of each one of the programmed activities, determining, definitively, if the project is or not, in conditions to start the commissioning. In service. For these purposes, the Gendarmerie may require technical reports, both from Service officials and external professionals.

In case of non-compliance in the delivery of this Milestone, for reasons attributable to the supplier, Gendarmerie will be empowered to start the procedure for collecting the corresponding fine.

Any circumstance that may imply the concurrence of causes not attributable to the supplier, such as fortuitous event or force majeure, must be informed, in writing, to the Gendarmerie, within 48 hours after its verification, for the purposes of its evaluation and subsequent resolution.

b) MILESTONE N ° 2 “White March” (pre-opening trying period): The objective of the white march is to refine the configurations and make the necessary adjustments for the commissioning of the contracted service. For this, the provider will have a period of 60 calendar days, counted from the reception in accordance with Milestone No. 1, during which all the functionalities of the offered system must be tested, that is, those required in the technical bases and its annexes, as well as those differentiating and value-added elements considered in the awarded offer.

The white march will have, as a minimum, the verification of the following functionalities:

b.1) Detect and identify in real time, the place where the offenders is, establishing the appropriate warning mechanisms to prevent the limits established by the judicial authority from being crossed.

b.2) Provide, continuously and reliably, precise information on the location, in coordinates, within the Chilean geography, where the offenders is, continuously, in the case of intensive probation, or partially, in the case of night confinement.

b.3) Have the necessary mechanisms to detect and report any fraud or falsification of the aforementioned information.

b.4) Warn when the offender is outside an inclusion zone, or is close to an exclusion zone, judicially established.

b.5) Communicate timely incidents that occur in accordance with the previous letters, as well as communicating warnings to staff

b.6) Accessibility via website, allowing remote users to access the location information of the offenders.

b.7) Generation of reports.

b.8) Review of the operation of the monitoring and administrative management system, allowing the review of alarm drops, map traces, alarm management, etc.

Access and operation from the outside to the IFT module (technical feasibility report) will be tested. This process must be done through interconnection, so the provider must have a web service.

These tests will be carried out with the participation of "friendly users" designated by the Gendarmerie, and must comply with the "Acceptance Testing Protocol", required in Milestone No. 1, and approved by the Institution. The Gendarmerie technical counterpart will witness and direct, at all times, the development of the White March.

After the tests, the supplier must deliver to the Gendarmerie a written report that accounts for the results obtained, the criteria used in this analysis and the instruments used for the measurements. This report will be countered with the results report prepared by the technical counterpart.

Once the deadline for its execution has been met, the Gendarmerie will proceed to Reception of Milestone No. 2, within 10 business days, a period intended to certify the correct operation of the project, which will be done using the “Protocol of acceptance”, previously indicated. For these purposes, the Gendarmerie may count on the support of Service officials or external professionals.

In the event of non-compliance in the delivery of this milestone, for reasons attributable to the supplier, the Gendarmerie will be empowered to start the procedure for collecting the corresponding fine in accordance with articles No. 49 and 56 of the administrative bases.

Any circumstance that may imply the concurrence of causes not attributable to the supplier, such as fortuitous event or force majeure, must be informed in writing to the Gendarmerie, within 48 hours after its verification, for the purposes of its evaluation and subsequent resolution.

If this milestone is concluded, it is verified that the system does not comply with the technical requirements established in the bases, and the supplier does not rectify them within the maximum term established for it in accordance with the technical bases, the system will not be received, and it will proceed to apply fines, being able to resolve the early termination of the contract.

If the supplier satisfactorily complies with all the requirements, the “Commissioning” can begin.

a) MILESTONE N ° 3 "Commissioning": Corresponds to the start of operation of the project itself, with all its functionalities, in accordance with what is offered by the supplier, with what is required in the administrative and technical bases, and its annexes. This stage will begin once certified by the technical counterpart, the acceptance of Milestones No. 1 and 2.

This milestone will contemplate an initial stage of six months, during which the device replacement process must be carried out with the outgoing company, from those that were installed before the new supplier came into operation, as appropriate.

Throughout the process, the provider must ensure continuity in the operation of the service.

If the supplier satisfactorily complies with all the requirements, the “commissioning " may begin.

2. Deliverables.

Once the project has been accepted and the commissioning has started, the supplier must deliver the following to the Gendarmerie:

a. Database model

b. Data Dictionary

c. Necessary technical manuals for all installed hardware and software, including those related to power backup equipment, firefighting systems, etc.

d. Procedures protocols for all activities necessary for the operation of the monitoring system, including those related to energy backup equipment, anti-fire system, etc.

e. Architecture of the proposed platform.

This information must be kept updated throughout the term of the contract.

THIRD: PRICE AND METHOD OF PAYMENT.

The total price of the provision of services will be [***], for the entire period of the contract.

All costs, expenses and eventual taxes that the execution of the contract and the faithful fulfillment of the contractual obligations are considered included within the economic offer.

Payments will be made monthly, according to the number of monitored devices, installations and uninstalls executed, in the corresponding period, multiplied by the price offered by the provider, as appropriate.

The Institution is empowered to deduct the fines that are paid from the statements of pending payments.

The payment, according to the supplier's offer, will be calculated according to the following detail:

Daily monitoring price per item	Offer (net values)	Offer (gross values)
[***]	[***]	[***]
[***]	[***]	[***]
[***]	[***]	[***]
[***]	[***]	[***]

These values are not subject to adjustments.

To proceed with the payment, the Technical Counterpart, regulated in the seventh clause of this contract, must previously carry out the approval and certification of the services. For this, the supplier must deliver a monthly report of income and expenses related to the continuous monitoring service and domicile, as well as the installations and uninstallations carried out.

This report can be made in written or digitized form, and must be delivered to the Institution, through the computerized management system provided by the provider, which must also allow, in real time, to view the respective supporting records that justify the monthly collection amount.

The report must be delivered in a timely manner, and must contain, at least, the following information:

a) Installed, replaced and uninstalled devices;
b) Devices active and monitored daily, according to the type of technology used;
c) Monthly payment, according to what is stated in the supplier's offer;
d) Fines paid in the previous month;
f) Minutes of unavailability of the system;
g) Everything else that has been entrusted by the Institution, related to the correct and efficient execution of the contract.

During the term of the contract, the contents required in this report may be modified according to the requirements made by the Institution.

Payments will be made within the term of thirty calendar days, counted from the presentation of the respective invoice, prior approval and certification of the technical counterpart of the Institution, and always, provided that the provider does not record unpaid balances of remuneration and / or o security contributions with their current workers or contracted workers, in the last two years, with a maximum of 6 months, within the framework of the subsidiary responsibility derived from said labor and social security obligations, established in article 183-D, of the Code of Labor, which must be accredited with the corresponding certificates, attesting to the amount and status of compliance with such obligations, issued by the respective Labor Inspectorate, or by suitable means that guarantee the veracity of the status of compliance.

In case of registering debts of this nature, with their current workers or with workers hired in the last two years, the first payment statements will be destined to the payment of said obligations, and the provider must prove that all the obligations are settled, upon completion of the half of the contract execution period, with a maximum of six months.

The institution will require the supplier to comply with said payments, for this it must present, in the middle of the period of execution of the contract, the vouchers and forms that demonstrate full compliance with the obligations or the certificate of labor and social security record No. 30, granted by the Labor Directorate, a document that cannot be more than 30 days old from its delivery.
The breach of these obligations by the provider will be considered serious and will empower the Institution to terminate the contract early.
It is expressly stated that it does not constitute an obligation of the Gendarmerie, nor does it assume responsibilities of any kind, if the number of offenders to whom the telematics monitoring service is applied is not met, based on the information provided in the process bidding, without prejudice to the rules established for payment in this article.

FOURTH: TERM AND EXECUTION OF THE CONTRACT.

The contract will have a duration of forty-one months, including the implementation stage, and will come into effect from the date the administrative act that approves it is fully processed, which will be published on the website. The total processing of the act supposes its notification, which according to the general rules, will be understood as practiced, after twenty-four hours counted from its publication on the portal www.mercadopublico.cl.

However, the extension of its validity beyond each annual budgetary year will be subject to the existence of sufficient resources for this purpose, in the Institution's annual ordinary budget. Therefore, the Gendarmerie of Chile is, since now, empowered to terminate the contract, before the original term indicated, invoking as a basis the lack of sufficient resources in the budget year in question. Said unilateral decision by the Gendarmerie will not imply the payment of any sum for any concept other than the payment of the services actually provided by the provider, until the date indicated in the corresponding notification that the Institution practices to make known the circumstance indicated.

Considering the nature of the contracting and the functions of the Gendarmerie as a public service, the provider undertakes to continue monitoring services that

are operational at the time this contract comes into effect. In relation to this, in accordance with the provisions of the technical bases, the provider must execute all the actions foreseen in the implementation stage, including all the previous activities necessary for the Commissioning of the monitoring service for the time stipulated in the bases, and in accordance with the provisions of the offer, especially in technical annex N ° 18 containing the Gantt letter delivered by the supplier.

The provider must deliver the telematics monitoring service, working and implemented 100%, within the stipulated and offered deadlines, complying with all that is stated in the technical bases, regarding the implementation and Commissioning of the project. For these effects, the system must function loosely to monitor all the offenders in force and those who enter the system.

FIFTH: THE ESSENTIAL OBLIGATIONS OF THE CONTRACT.

The provider must comply with all the obligations included in the provision of the contracted service, in accordance with the provisions of its technical offer and the requirements of the administrative and technical bases. Understanding as essential obligations the following are detailed:

1. - TELEMATIC MONITORING SERVICE.

1.1. Monitoring system.

The provider must provide a computer system that allows managing and controlling the monitoring of offenders and that also has functions that allow for administrative management control.

The monitoring and administrative management system must have a user maintainer, which allows managing accounts and accesses, as the technical counterpart deems appropriate.

The supplier undertakes to improve or update the system, in accordance with the provisions of point 3.7, section number IX of the technical bases.

The system must comply with all the conditions described in the technical bases and the supplier's offer, especially in that described in technical annex No. 1. In this sense, the system must comply with the following, as a minimum:

a) Be able to identify, in real time, the place where the offender and / or the victim is, establishing the appropriate warning mechanisms, which allow detecting the transfer or breach of the limits established by the judicial authority and / or those incidents that affect the control of the offender or the protection of the victim.

For these effects, “real time” shall be understood as the period of time in which the system is configured to produce the visualization effect of the subject's displacement, understanding that when using communication networks, technologies always carry a certain degree of latency or intermediate time of seconds, in which the signal is transmitted, travels, enters the software, is processed and manifests itself on the monitoring map.

In accordance with what is offered in technical annex No. 1, the system must reflect a follow-up, in real time, of less than one minute.

b) Provide, in a continuous and reliable way, precise information on the location, in coordinates (GPS), within the Chilean geography, to determine, with a tolerable margin of error, of a maximum of 24 meters, regarding mixed penalties, freedom intensive surveillance and home confinement.

c) Have the necessary mechanisms to detect and notify any type of attempts to defraud or falsify the information previously indicated.

d) Allow the generation of exclusion, pre-exclusion and inclusion zones; victim protection radios; and, halo of non-approach of offender and victim, activating the respective alarms for non-entry, exit or proximity.

It must generate warnings, warning when the offender is about to cross an inclusion zone, or enter an exclusion zone, or approach the victim, crossing the protection halo, judicially established.

e) Allow immediate communication of incidents that, in the sense indicated in the previous letters, occur, as well as communicating alarms and warnings to competent personnel, for the control of the offenders that the institution will assign, as to all the people who deem appropriate, by any means of communication.

The alarms and warnings must be reflected in the system, after the following lapses of time, counted from the display of the violation in the system, as follows:

e.1. Inclusion zone violation alarm: less than 1 minute.

e.2. Notice of transfer to a pre-exclusion zone: less than 1 minute.

e.3. Exclusion zone transfer alarm: in 30 seconds.

e.4. Proximity warning of the victim to the offender: when the approach halo set for the offender makes contact with the protection halo for the victim, in 30 seconds.

e.5. Approach alarm to the victim: when the offender passes a protection radio zone to the victim, in 30 seconds.

f) The system offered by the provider must be in a web environment, allowing remote users, authorized by the Gendarmerie, to access the information of the offender, their location or that of the victim. The supplier shall provide a test environment to manage the updates that are necessary, without generating stops or interruptions in the normal functions of the system.

g) The provider must document the network architecture of the comprehensive telematics monitoring system and, in particular, detail the connectivity parameters at the network level, the different stages that make up the solution, and the aspects of computer security, such as, for example, access rules and filters at the firewall level, which will protect the system from intruders and attacks. In addition,

it must document the way in which the information will be backed up and recovered, in the event of incidents, ensuring zero loss of information.

h) The proposed solution must allow uninterrupted operation 24 hours a day, every day of the year. Mechanisms that ensure the operational continuity of the service will be considered, according to the offer presented. To achieve this availability, redundant elements, power supplies, fans, mirrored disk arrangements, data links, etc. will be used. The provider must have Tier III Hosting, in addition to infrastructure with application backup systems and redundant databases, as indicated in its technical offer.

i) The system must function loosely to monitor all the offenders who enter the system. If the number of monitored people generates difficulties that affect the expected functionalities of the integral system, the supplier must adopt the pertinent measures that ensure the normal operational continuity of the system. The proposed computer solution will allow simultaneous monitoring from the National Monitoring Center, the Regional Simultaneous Monitoring Center, or other places that the Service requires, with prior authorization and access controls by the Institution.

j) The software must be configurable to the needs of the Institution during the term of the contract, and must allow the following functionalities:

j.1. Modify the state of the warnings generated by the devices.

j.2. Identify and allow the use of visible and distinctive elements of the warnings generated by the devices (colors, icons, etc.).

j.3. You must submit the automatic calculation of the sentence expiration date, and allow manual modifications.

j.4. It must allow the automatic activation of offenders who has been suspended, either by court order or by calendar.

j.5. It must allow to be able to program suspensions, for a determined period of time, which must deactivate alarm drops, such as charging for the service.

j.6. You must generate automatic notices and alerts for offender cases that meet some of the following conditions: suspension, end of the control period, activations or other indication from the competent court. In these cases, the system must have a tool that allows reporting, through automatic reporting and sending of email, to a group of users defined by the Institution or via interconnection.

j.7. The traces generated by the system must be able to distinguish distinctively, when the elapsed time exceeds one minute, between the last trace and the next one; and, you must discriminate between those traces, depending on the GPS signal, cellular triangulation, recovery of traces due to signal loss, and those that indicate signal loss.

k) The software system interface must be in Spanish.

l) The software applications must allow the hierarchy of user and management levels through, at least, the following profiles:

- Viewer user
- Operator user
- Super administrator user

m) Must generate work orders, manage and schedule installations, uninstalls, technical supports, etc., in order to keep in mind and coordinate the execution of said activities, among the different participants in the process.

n) It must register all the events and incidents that occur, in order to carry out a control over them, and provide systematized information, according to the requirements that are formulated, and have statistics on the information generated in the systems.

o) The system must give full support to all the functions that emerge from the process diagrams, according to technical annexes No. 11 to 17.

* The functions indicated in letters m), n) and o) above must be able to be operated by both Monitoring Centers and by the Social Reintegration Centers of the country.

p) The records must consider the following minimum information:

p.1. Individualization of the offenders: full name, RUT, sex, date of birth;

p.2. Individualization of the cause: substitute penalty subject to control; court; court region; RUC; RIT; crime, according to the crime table provided by the institution; and, data of the victim;

p.3. Monitoring data: Social Reintegration Center where it is controlled; inclusion and / or exclusion zones; compliance schedule; technical feasibility requests, indicating the result of the report and the reasons for the non-feasibility, as appropriate; copy of the entered sentence; installation schedules; installations carried out; judicial decisions entered; technical supports made; non-compliance reports; effective days of control and the days that control was breached; uninstalls performed, indicating the reasons for the uninstallation.

q) The system must contain, within its functions, the creation of dynamic reports and statistical tables, according to institutional needs, and as established in the technical bases and as offered in technical annex No. 1.

It should allow the automated extraction of filtered data, according to institutional requirements, from the different components of the comprehensive monitoring and administrative management system, thus classifying itself, according to its functionalities.

q.1. Reports and statistical tables of the monitoring system. It must be carried out based on the data of the monitoring system, the incidents it registers, and the offender monitored, in accordance with the following minimum requirements:

● List of technical feasibility requests, having to detail the processing status, if it is pending, rejected, approved or sent.

● Event log: summary report with what happened during the previous night, indicating the warnings (pre-alarms and alarms) produced. All this must be indicated with the time of occurrence, operator, offenders and victim involved (if applicable).

● Summary of offenders who registered warnings, separated by type of sentence (partial confinement or intensive probation).

● Offenders in a valid state in the system.

● Offenders who registered alerts.

● Individual report of offenders subject to night confinement, which must detail the time of entry, time of departure and alerts.

● Individual report of offenders subject to night confinement, mixed sentence and intensive probation, which must detail time of entry, time of departure and alerts.

q.2) Reports and statistical tables of the administrative management system

The system must be in a WEB environment, allowing users from regions and local monitoring coordinators (CLM), to connect and generate administrative management, regarding installations, uninstalls and technical support.

The system must allow obtaining management control data from local coordinators, which allow measuring the workload, the states of their processes, the reports generated by administrative tasks, among others.

Among the reports that may be requested are:

a) List of installations carried out.

b) List of uninstalls performed.

c) List of monthly preventive and corrective maintenance visits made to the Monitoring Center.

d) List of relevant alarms for a given period.

e) List of training services developed.

f) List of other relevant activities not contained in the above and that are part of the contractual obligations.

g) Offenders in force in the system.

All reports described in letter q) must include bar, line and pie charts, with individual and aggregated data, and must be able to be exported to standard formats, such as Excel, PDF, Word, etc., and must indicate :

● Individualization of the Offenders;

● Details of the cause;

● The own records of the report generated, including dates, descriptions and / or definitions of the report's activity.

r) Requests for technical feasibility reports

An administrative management, technical feasibility and statistical reporting system must be provided, in accordance with what is offered by the supplier and with what is established in the technical bases, the purpose of which is to validate and submit requests for evaluation of the monitoring; keep an individual record of the main actions carried out by offenders; and, to be able to extract general statistics on the operation of the system, due to the requirements formulated by the Institution.

This system must contemplate in its design, at least the following:

r.1. The provision of a WEB platform, in which the authorized subjects will be able to formulate their technical feasibility requests to the Institution, remotely.

r.2. The provision of tools to carry out a prior process of validation of the applicants, and another of evaluation regarding the sufficiency and relevance of the information provided in the request, for the provider to carry out the technical feasibility monitoring examination.

According to the merit of the validation and review that is carried out, you can:

a) Do not validate the application and automatically return it to the applicant. This, in case the information provided is incomplete and / or inconsistent.

b) Validate the request and send it to the provider, in order for it to rule on the feasibility or not of monitoring specific addresses and / or sites, based on objective technical parameters, within 24 hours of the request being made.

c) Carry out, prior to validation, a detailed background check and face-to-face verification, if requested, which must be submitted within 72 hours, if necessary, as it is deemed necessary, greater degree of precision and detail, that it is necessary to know certain characteristics of addresses, and / or to ensure with certainty the geographical location of the same.

A background verification process may be required, through the following actions:

c.1. Attend the address in person, in order to assess physical characteristics.

c.2. Attach a map or photographic record, for which the technical feasibility report is requested.

c.3. Expressly indicate the percentage of cellular coverage insured at the respective address.

c.4. Indication of particular aspects to keep in mind when ensuring monitoring, be they geographic, housing, infrastructure, connectivity, among others.

Once the report has been evacuated, the Institution will proceed to evaluate the final validation of the request for the technical feasibility report, and must rule on it within 24 hours.

The feasibility report may be "positive", "negative" or "not recommended", the latter when, due to the revision referred to in point c.3., Above, the presence of some technical circumstance that make the inconvenience of proceeding to the monitoring, even when you have enough cellular coverage to carry it out.

The system must also be able to automatically evacuate the response, by sending an email to the respective registered account.

1.2. - COVERAGE OF THE SERVICE.

It corresponds to the percentage of the national territory covered by the cellular mobile data network, with mapping of maps, at the level of street names and numbering of addresses.

The coverage must correspond to the detail offered by the supplier in technical annex No. 1, and in the lists and maps required in the technical bases, and, regardless of the percentage, must cover all the communes in the country.

National cellular coverage must be available from the companies Movistar, Claro and Entel, reaching a level of at least 99.4% of all the antennas published in the country, depending on coverage, availability and saturation. .

1.3. - MAPS SYSTEM.

The supplier must present a solution of maps with cartographic survey, at the level of numbering and street names that allow the accurate identification of private homes and specific public sites, in accordance with what is offered in technical annex No. 1.

The system must also include a distinctive sign that allows identifying, at least, the following relevant places:

● All the Gendarmerie units.

● All current educational establishments, in the registry of the competent public body.

● All current health facilities, in the registry of the competent public body.

● All police stations and police stations and police stations.

● All Courts of Justice, Courts, and dependencies of the Public Ministry.

● Shopping centers, supermarkets, stadiums, churches, squares and parks.

● Other relevant public bodies.

Maps must be able to be customized, specifying the layers that can be superimposed on those offered, that identify certain places.

The supplier must update the maps provided with the frequency offered in technical annex No. 1, and according to the following criteria:

a) Ex officio, with a periodicity of four months.

b) At the request of the party, according to the specific requirements of the Telematics Monitoring Department, every two months or less, in the face of the discovery of new areas and / or sites not covered by the mapping system, with the required degree of detail.

c) Additionally, three requests per year are contemplated, with no less than five points of interest in each of them.

The updates should specifically consider the cartographic survey at the level of numbering and street names, and of those communes that do not yet have that level of detail, aiming to cover all the communes of the national territory, and update, with the committed frequency, the information on the layers mentioned above.

This obligation will be verified, through a procedure determined by the Institution, respecting the general rules established in the bases, in accordance with the provisions of article No.43 of the administrative bases.

1.4. – SERVICE LEVEL AGREEMENT FOR THE AVAILABILITY OF THE MONITORING SYSTEM.

It corresponds to the percentage of available minutes per year of the offered system, that is, the state in which the system is capable of monitoring, with all the hardware and software functions installed, including the telecommunications necessary for it.

The supplier must comply with the availability offered, which must guarantee an availability level of, at least, 99.93% of the available minutes per year, on the monitoring control and display in real time, with drop controls by alerts, and permanent monitoring of the link network and devices, and their transmission, which is equivalent to a maximum average of 30 minutes of monthly unavailability.

The system must remain 100% available during the entire term of the contract, except for the exceptions expressly contemplated in this contract.

The provider shall provide access to monthly communication link availability reports, and to all the active and available services of the monitoring and administrative management system.

You must report, on line, communication drops or latencies in control, through an external application that allows you to collect a history of these failures, equivalent to 0.3% tolerance.

The requirements, in relation to the service levels agreement to the availability of the system, include the monitoring system itself and the telephone service.

Each scheduled preventive or corrective maintenance job must be requested and authorized by the technical counterpart. The request must be made in writing, 48 hours in advance, and may not generate unavailability of the system, under any circumstances.

The request for scheduled jobs must contain, at least, the following information:

a. Name, national identity card or passport, position, company, contact telephone number and email of the engineers and / or technicians responsible for the scheduled work.

b. Purpose of scheduled work.

c. Scope of scheduled work, indicating what stage of the entire system it affects.

d. Start and end time of scheduled work.

e. Rollback actions.

It is the provider's responsibility to coordinate such information with subcontractor companies, so that the Gendarmerie of Chile is duly informed regarding the scheduled work.

Failure to comply with the service level of the monitoring system offered implies the collection of fines, in accordance with the provisions of clause eight of this contract and the provisions of the administrative and technical bases, which will be measured in accordance with the provisions of article No. 43 of the administrative bases, in accordance with point 3.9 of the technical bases.

1.5- DATA CENTER.

The bidder must have a TIER III Data Center, certified by the Uptime Institute, which must be in the national territory, and comply with all the other characteristics and certifications offered by the provider, described in technical annex No. 1.

All costs associated with the enabling or contracting of services must be borne by the provider.

The Data Center must save all the active equipment, servers, databases, systems that comprise the telematics monitoring solution. The updating of the Hardware must be ensured, maximum every two years.

The Data Center must provide the following functions and characteristics:

a) Monitoring servers with their respective licenses, exclusively dedicated to the bidding system. Sharing of servers with third parties is not allowed.
b) Software with the monitoring server applications and their respective licenses.
c) Database engine software with their respective licenses.
d) Standard database system with mirrored disk arrays.
e) Hardware necessary for data connectivity with redundant links, which allow access to the Gendarmerie data processing, database and backbone servers. The

configuration services of routers and connectivity, as well as the enabling and laying of cabling, fibers, connectors, etc., will be the responsibility of the provider, as offered, ensuring autonomous sources of energy, for a period of 8 hours or more.
f) Firewall hardware and software that allow defining a safe area through security policies. It must provide a physical and hardware firewall for the servers, with support for up to 80 million packets per second, constantly updated servers, and the latest version of the antivirus. Protection at the data center level against malicious attacks, in addition to a high capacity and availability network.

1.5.1. - COMMUNICATION ROOM WITH DATA CENTER.

The provider must set up a communications room in the National Monitoring Center and in the Regional Simultaneous Monitoring Center, in accordance with what is offered in technical annex No. 1, and what is established in the technical bases.

Without prejudice to complying with the additional elements offered by the supplier, the minimum elements that the proposed architecture for the equipment of processing racks and database of the room must have are the following:

a) Monitoring servers with their respective licenses, with exclusive dedication to the contracted system.
b) Monitoring server application software and their respective licenses.
c) Database engine software with their respective licenses.
d) Hardware necessary for data connectivity with redundant links that allow access to the Institution's data servers, databases and backbone. The configuration services of routers and connectivity, as well as the enabling and laying of cabling, fibers, connectors, and others, will be the responsibility of the provider.
e) Hardware and firewall software that allow defining a safe area using security policies.

The architecture must comply with the proposal, and contain as many redundant elements as necessary, to ensure high availability, at the software and hardware level.

The supplier must replace, if necessary, due to failure or obsolescence, the hardware equipment installed in the communications room, to guarantee the operational continuity of the contracted service, a situation that will not represent any cost to the Gendarmerie of Chile.

1.6. - ENCRYPTION OF THE INFORMATION.

The provider must comply with the levels of encryption proposed in its solution, between the devices and the monitoring system, ensuring the highest percentage of data protection.

1.7. – BACKUPS.

It will be the provider's obligation to always keep backups of the database, with access available in permanent reading form, and with online backup.

2. - CHARACTERISTICS OF THE DEVICES AND IN RELATION WITH THE TELEMATIC MONITORING SYSTEM.

The devices used for telematics monitoring and those for victim protection must comply with what is offered and the technical requirements demanded by the Institution.

From the beginning of the execution phase, each installation carried out must be with new devices, which have the respective manufacturer's certification, which must be presented by the installation technician. This obligation will extend throughout the first year of service execution.

2.1. CHARACTERISTICS OF OFFENDER AND VICTIM MONITORING DEVICES.

The devices must comply with the technology and characteristics offered by the provider and, in accordance with the technical bases, must meet the following characteristics:

a) Unambiguous identification. The device must enable the offender and the victim to be identified unequivocally in the monitoring system.

b) Positioning of the monitoring. The device must reflect the position of the offender and / or victim, either in the form of coordinates or in the form of presence or absence, within a given geographical area, according to the configurations formulated in the offered map system. There will be areas of inclusion that will restrict the displacement and permanence of offenders at his home, during judicially predefined times, in the case of the penalty of partial imprisonment.

c) Installation of the device and manipulations. The monitoring devices must be easy to install and adjust, and be equipped with a tamper detection mechanism that is capable of detecting this type of event and transmitting it to the Monitoring Centers.

“Tampering” is considered any attempt of improper administration, attempt to dispose of it, opening the box containing the receiver, physical damage to the equipment, and improper removal from the tracking device or unit, which does not allow the optimal operation of the service of telematics monitoring.

For this, and without prejudice to the tampering alarm, the device must contain, at least, a physical / material security mechanism that, if corrupted, allows to leave irrefutable empirical evidence of its malicious manipulation, being able to verify, visually, improper manipulation by offenders

d) Transmission of data. The data transmitted by the solution must, in turn, be able to be transferred to the Monitoring Centers, through a communication system, allowing this transfer in an autonomous way, at least every 1 minute, and can be configured remotely so that this transfer can be done in a longer or shorter time, according to the needs of the Gendarmerie.

e) Establishment of inclusion areas. The solution must be capable of configuring an inclusion parameter or zone, which will establish the maximum distance or the measured radius from the location of the tracking and reception device or unit, up to which the offender may move away. This value must be able to be configured through the programming carried out from the Monitoring Center.

For GPS-based solutions, the margin of measurement error, between the actual location of the offender and / or victim, monitored, and the coordinates sent by the device, must be less than 24 meters.

f) Approximate location of monitoring for eventual signal loss. In the event that the device loses or decreases its satellite signal, a communication system must be provided that, using assisted geo-referencing, is capable of connecting to the mobile telephone network, in order to allow it to identify, on a map, the approximate location of the subject, even when the device is not facing the sky or is in underground locations. For such purposes, the solution must consider the use of cellular triangulation and GPS technologies.

The system must also include an audit and control tool for the CELL-ID information or identifier of the cell phone base station, to which the offender is connected, so that the system can detect the user's location in a specific moment, even if retroactively

g) Device characteristics. Those devices that are in permanent contact with the body of the offender, must be hypoallergenic and resistant to water, high operational temperatures, temperature changes, humidity and extreme conditions. These characteristics must be certified by recognized bodies in the field.

h) Electric field levels. The transmitting device must comply with the maximum electric field levels allowed by the Undersecretary of Telecommunications (SUBTEL) so as not to generate relevant interference with other electronic and / or telecommunications devices. In the event that a direct connection to electrical current is required, this should not cause excessive overheating of the device, which may cause harm to users. These characteristics must be certified by recognized bodies in the field.

i) Alarms, warnings and warnings. The device, together with the monitoring system, must be able to self-generate different levels of warnings, within the latency margins established in the technical bases (IX 1.1. Letter e), both for entry into exclusion zones and for exits of inclusion zones, as well as, the zones of pre-exclusion, and the one of approach to the victim, that allow generating pre-alarms, which should, if necessary, be able to be determined remotely.

The device, together with the monitoring system, must be able to detect anomalous circumstances in the signal transmission, which unexpectedly reflect movements in unrealistic speeds and distances, in terms of their actual occurrence, such as alarm jumps, and must discriminate this circumstance anomalous of other types of displacements and alarms that are produced by the true monitoring action.

j) Need for two-way communication. The devices for those offender to intensive probation and those for the protection of the victim must also allow two-way communication between the offender and / or the victim and the Monitoring Centers, through the device itself and / or an additional device, which the offender must necessarily carry constantly. This communication channel will be used to transmit warnings from the Monitoring Centers and, where appropriate, to warn the victim of the proximity to the offender, activating the respective protocols.

k) Storage of information on the device. The device, together with the monitoring system, must include a mechanism for the conservation and recovery of information. This mechanism should be able to retrieve information retroactively in the event of faults, signal losses, complete battery discharge and shutdown of the same, in such a way that they reflect, with a lag, in the system, the displacements it made during these periods and possible alarms, in case of having violated the conditions imposed by the court, everything, as soon as the system manages to recover communication with the device.

l) Battery charge level. The device must have an autonomous power supply system, information on the state of charge of the battery and an alert to the Monitoring Centers, when the state of charge of the battery is low.

m) Alarms. The device, together with the monitoring system, must transmit alerts and alarms to the Monitoring Centers, when the offenders exceeds the limits established in the respective resolution, for their movement, or those limits established in the action protocols of Gendarmerie, aimed at avoiding a potential failure to comply with the sentence or those circumstances that affect the control of the sentence, through telematics monitoring.

n) Detection of fraud attempts. The device must detect and report to the system, attempts from external sources that produce illegal interference (Jamming) or malicious blocking (shielding) of the GPS signal, trying to defraud the functionality of the device.

ñ) Sanitation processes. The device must be capable of undergoing a sanitization process, after each uninstallation, in order to be able to be reused, in accordance with the reuse parameters established in the technical bases.

o) Characteristics of the clamping mechanism. The clamping mechanism or, where appropriate, the strap that the device has, must be, at least, plastic, hypoallergenic, industrial grade, lined, whose material composition does not allow easy deterioration or breakage with simple cutting tools of common use and nature, according to the technical description of the products, offered in the technical offer, accessories catalog and home device.

p) Weight. They may not weigh more than 200 grams, for which their accessories will not count. Likewise, the size must allow its easy concealment in any of the extremities that is installed.

q) Certifications and backup cellular coverage on the device. There must be homologation certificates, issued by entities validated by the competent authority (SUBTEL), which certify that the device has a multi-frequency band with commercial bands, from the different telephone service provider companies in

the country (OMR), that have their own network and that offer telephony services through it.

The monitoring device for intensive probation and victim protection must have at least one cellular signal chip. Notwithstanding this, the devices may have more than one cellular signal chip from different companies, in order to ensure cellular coverage of the service.

r) Useful life and reuse. The devices must have the useful life offered, however, one year after their first installation, they must be replaced by a new one, when the first technical support occurs as a result of failures, which relate to causes of signal loss or failure in voice communications or data transmission.
If, after a year of use, there are evidences of failures that motivate the realization of 3 technical supports, as a result of signal losses or shortcomings in voice communications or data transmission, the device must be decommissioned and replaced by a new one.

The technical counterpart may require the provider, covered by qualified reasons to ensure good service and avoid incidents of public connotation, the installation of a new device, mainly in cases of intensive probation and protection of the victim.

s) Device identification code. Each device must have a unique distinctive registration code, serial number or enrollment, for the purposes of its individualization and monitoring of its usage history.

t) Recharge time and operating autonomy. The recharge may not extend for more than one continuous hour, and must ensure 48 running hours of autonomy of the device.

The recharge of the device intended for monitoring partial seclusion may not be extended for more than 2 continuous hours, ensuring at least 72 running hours of autonomy of the device.

2.2. - SPECIFIC CHARACTERISTICS OF THE DEVICE FOR THE VICTIM.

In addition to the characteristics mentioned above, the device for the victim must consider, in accordance with article 23 bis of Law No. 18,216, the following minimum technical requirements:

a. Allow in the monitoring system, unequivocally, the knowledge of the victim's location, visually distinguishing on the map the victim's last position. The system must reflect, at all times, its location, and generate a halo around it, adjustable in meters.
b. The device, together with the monitoring system, must warn the proximity to the offender, in accordance with pre-established parameters with the Institution.
c. The device, together with the monitoring system, must allow the knowledge and visualization of the exact location of the victim within the national territory, and the communication of their position to the Monitoring Center, through some technological means other than voice, such as text messages with location map sending, their combination, or any other development that improves their functionality.
d. Allow two-way communication between the victim and the Monitoring Centers.

e. Allow the system to emit a noticeable signal at the Monitoring Centers, in the event of proximity between the offender and the victim (S.O.S. alarm)

* Certifications common to all devices:

The devices to be installed in the home of the offender, the body of the offender or the victim, must use a wireless data transport network to communicate with the Monitoring Centers. In case of using the GPRS cellular data network, a dedicated APN must be created in the Core MPBN of the mobile operator associated with the offeror, and have at least one level of data encryption, either at the device level, and / or on the communication channel, and / or end-to-end encryption, etc. The provider must detail their security levels throughout the communication section.
The resistance of the devices must be internationally certified, according to degrees of protection, through the ANSI / IEC 60529-2004 Degrees of protection standard, DIN 40050-9 standard or its equivalents.

2.3. - INSTALLATION, SUPPORT AND REMOVAL OF DEVICES.

A comprehensive solution must be provided to achieve the proposed objectives, considering performing the technical feasibility certification, installation, technical support and removal of the monitoring devices, together with the Gendarmerie, throughout the national territory. This service must consider, at least:

a. - The “technical feasibility certification”, which will consist of the issuance of a document, called the “technical feasibility certificate”, indicating the possibility of supervision of the offender, through the contracted telematics monitoring system. In case the result is negative, said certificate must be founded.
b. - The supply, installation and removal of the required devices, for the implementation of the system, in a timely manner, in accordance with what is required in the bidding conditions and what is offered.
c. - Provide permanent technical support, remotely, through professional support, in the event of failures that arise in the handling of the devices. If the solution of the damage is not possible, the supplier must proceed to make the repairs in situ.

For the device installation process, the provider will be accompanied by an official designated by the Institution. In the event that the technology offered requires an installation to be carried out at the offender´s home, the provider must provide the necessary transportation to mobilize his or her staff together with the Gendarmerie official, from the respective Social Reintegration Center to the home of the offender, and from the latter to the Center for Social Reintegration. The costs associated with this transport will be borne by the provider.

For the installation of each device, the following instructions must be considered:

1. - See Technical Annex N ° 12, attached to the bases “Application process and technical feasibility analysis for the installation of a telematics monitoring device”.

2. - See Technical Annex N ° 13, attached to the bases “Process for the installation of a telematics monitoring device in the offender´s home”.

3. - See Technical Annex No. 14, attached to the bases “Installation Process of a telematics monitoring device for the victim”.

To control compliance with the sentence, the following instructions must be considered:

1. - See Technical Annex No. 15, attached to the bases “Process for controlling the penalty of partial imprisonment”.

2. - See Technical Annex No. 16, attached to the bases “Process of control of the sentence of intensive probation”.

3.-See Technical Annex Nº 17, attached to the bases “Process for controlling the end of the monitoring and removal of devices”.

2.4. - Maximum response time for assists.

The provider undertakes to maintain a remote assistance response time, between 2 to 2.5 hours, and face-to-face assistance, between 12 to 23.5 business hours, a period that will count from the time the formal request is made, in any part of Chile, to provide technical assistance, such as installation, uninstallation, replacement of devices and technical support in case of failure, among others.

Technical feasibility reports must be delivered between 12 and 23.5 business hours, since the request is made.

The installations, replacements and withdrawals of devices must be made between 24 and 47.5 business hours from the request is made. Business hours shall be understood as the corresponding business days, in accordance with the provisions of Law No. 19,880 of 2003.

3. - Authorization of the National Monitoring Center and the Regional Simultaneous Monitoring Center:

The supplier must enable the National Monitoring Center and the Regional Simultaneous Monitoring Center, in accordance with the provisions of technical annex N ° 6, with all the technical requirements established in the technical bases and its annexes, and complying with all other contemplated characteristics in your offer.

This obligation must be fulfilled from the delivery of the units provided by the Gendarmerie.

The National Monitoring Center will be located on Rosas Street No. 1,274, second floor, Santiago commune, Metropolitan Region, and the Simultaneous Monitoring Regional Center, at Panamericana Norte Kilometer No. 40, former prison of Puerto Montt, commune of Puerto Montt, Los Lagos Region.

The latter center will operate continuously and simultaneously with the National Center, focusing on the monitoring of offenders from a reduced number of regions, in accordance with the guidelines issued by the technical counterpart.

This operation may change to national coverage, 100% of the continental territory, in the event of catastrophes or other circumstances qualified by the Institution, which affect, hinder or impede the normal operation of the National Center. For these purposes, an action protocol will be signed, and the provider must arbitrate all means for the normal maintenance of operations.
The authorization of these centers must comply with the design proposed in the technical offer and that required in technical annex No. 6, regarding the uses of spaces and furniture, which will be supplied by the supplier.

3.1. - Number and characteristics of Hardware and software of the National Monitoring Center, Regional Center of Simultaneous Monitoring and Social Reintegration Centers.

The provider must permanently maintain the necessary technology and physical support, equipment, licenses and data link to perform the functions of telematics monitoring of offenders and victims.

You must implement the National Monitoring Center, for 30 operators and 5 supervisors; the Regional Center for Simultaneous Monitoring, for 18 operators; and, enable an individual PC for each of the 38 Social Reintegration Centers, all in accordance with the requirements described below:

Operator Computers

In order to efficiently administer and operate the system, the following equipment must be provided and kept in permanent operation, which must comply with all the specifications offered by the supplier in technical annex No. 1:

- 38 personal computers (PCs) with 27-inch screens, for the National Monitoring Center;
- 18 personal computers, with 27-inch screens for the Regional Center for Simultaneous Monitoring;
- 40 personal computers (PCs), with 27-inch screens, for each of the Social Reintegration Centers;
- 3 tablet with monitoring application for remote supervision (Samsung 7”), for the National Monitoring Center.

All computers must have access to mobile internet or fixed network at least 2GB speed.

If the creation of new Social Reintegration Centers is arranged by the competent authority, the provider must deliver a personal PC for each one of them, with a maximum of 6 additional teams to the indicated amounts.

They must include all the hardware facilities that are deemed convenient, to make the task of the operators more efficient and effective, considering, for this, not only functional aspects, but also ergonomic aspects (example: physical arrangement of the equipment on the work stations). Work, seat comfort, etc.), due to the levels of concentration and time that operators must dedicate to this work, having to endure the requirements that the Institution makes in this matter during the term of the contract.

Operators' computers must have the necessary slack in their hardware, incorporate Windows operating system, Microsoft desktop software (text editor, spreadsheet and email), and include upgradeable anti-virus software. All these software's must be installed with their respective license.

Software.

The software must comply with all the specifications detailed in the offer, be of a professional level or higher, have up-to-date licenses, and consider the Office 365 alternative with SharePoint.

All licensing must be delivered in the period of migration and infrastructure enablement.

Printers.

The supplier must deliver to each Monitoring Center, at least one monochromatic multifunction printer, with network connectivity of at least 45 pages per minute, with a minimum scanner of 80 pages per minute, which allows the digitization of sheets, in letter and legal format, and must be able to scan emails in PDF format. In addition, a 23 pages per minute color LED laser printer, up to 2,400 X 600 pixels.

The delivery of necessary supplies and toner must be considered, for the multifunctional, minimum, the equivalent of 10,000 pages, in a month; and, for the printer, a minimum of 2,000 pages, in a month, in addition, to include maintenance, support, replacement of parts, and even change of machines, if necessary.

3.2. - GENERAL VISUALIZATION SYSTEM OF THE CENTERS.

The supplier must supply, install, configure and maintain permanently operational, for the National Monitoring Center, 2 65-inch, 4K televisions, equivalent to 4 full HD, and one 85-inch, 4K, full HD, with input for PC, HDMI input, component video input and USB connection.

According to what is offered, they must have a content transmission system via connect Pro, which allows projecting any PC of the Monitoring Center by network on televisions, video Walls and projectors.

You should consider that these monitors will be on 24 hours, every day of the year.

In all televisions, a connection must be provided that allows the projection of the image to at least one computer equipment per television, in addition to hiring a TV service. Cable with at least a basic channel grill, for the entire duration of the contract.

For the Regional Center, at least one television with similar characteristics to those previously indicated (65 inches, 4K, equivalent to 4 full HD), content transmission system via Connect Pro, brand Kramer, must be supplied.

In addition, the supplier must supply, install and configure a multimedia projector and a curtain for each of the centers. Each projector and curtain must meet the following minimum requirements:

a) Multimedia projector that supports a resolution of at least 1920x1080 pixels of 3,000 lumens Full HD Epson and two 2.40 X 1.80 meter electric backdrops. It must allow an image to be projected at least 180 cm wide, with clarity, with video input ports (RCA connector), RGB port (15-pin mini sub). The projector must be configured to project the visualization from any PC of choice, from the operator room.

b) Minimum projector lamp life of 3,000 hours, with their respective replacement lamps.

c) The projector must be installed, for which the supply of the support structure and its installation must be considered.

d) Seamless opaque white wall curtain, which should be located in the center of the wall where the images will be projected.

3.3. - TELEPHONE CENTER.

The provider must provide and maintain a telephony service for both Monitoring Centers in accordance with the specifications established in the bidding rules and in its technical offer, which has at least 35 telephone equipment for the National Monitoring Center, and 18 equipment for the Regional Center for Simultaneous

Monitoring, and that allows operators to carry out national internal communications to fixed and mobile networks.

You must have two telephone annexes for communication with Carabiners of Chile, as part of the service and the network.

The service must have, at least, everything established in point 3.3 of section number IX, of the technical bases.

In the event of a power cut, the telephone service must have a minimum autonomy of 15 minutes through UPS; the system and all its components must be connected to the backup electrical network provided by the generator.

3.4. - CALL RECORDING SYSTEM.

The system must comply with the requirements of the technical bases, and other additional characteristics contemplated by the supplier in its offer.

For voice communications, the system must record all the communications established in the Monitoring Center, for which the provision and installation of an audio recording, editing, reproduction and administration system that complies with the functions and characteristics indicated in point 3.4 of section number IX, of the technical bases.
The storage period of the backed up audio files will be the duration of the contract. Before the end, the Institution will be able to migrate the stored audio files and extract them to the format that the system must have, allowing and facilitating said procedure.

3.5. - SATELLITE TELEPHONY SYSTEM.

According to what is offered, the supplier must deliver a total of seven satellite telephones, which comply with all the characteristics and specifications indicated in the bidding conditions and technical offer of the supplier, with an active balance of 12 continuous hours in each device, to be used in emergency or disaster calls. A satellite phone will be delivered to Carabiners of Chile, in order to ensure communication through it with CENCO.

Additionally, coaxial cable installations and base stations are added to allow coverage while inside the Centers and / or in the buildings they operate.

The cost of maintaining the satellite telephone service will be borne by the provider, during the term of the contract. The balance must be available again at the end of the emergency.

The satellite phone system must comply with the technical characteristics offered by the provider, without prejudice to the minimum specifications and accessories indicated in point 3.5 of section number IX, of the technical bases.

3.6. - RENEWAL OF THE HARDWARE EQUIPMENT INSTALLED IN THE MONITORING CENTERS.

The supplier must replace, if necessary, due to failure or obsolescence, the equipment, to guarantee the operational continuity of the contracted service, a situation that will not represent any cost for Gendarmerie of Chile.

3.7. - SYSTEM UPDATES.

The provider must have developers to update the system. Updates of the monitoring and administrative management systems must be carried out for a minimum of 600 hours, in the first year of the contract.

The following years, updates will be made if requested by the provider, tending to be the minimum, or when the Institution requires it, if necessary and as available.

3.8. - MEASUREMENT IN FAULT OF TIMELY TRANSMISSION OF DATA (OFFLINE DATA).

The provider must provide a timely measurement of data, for each device, during the respective measurement period, through an application or system that allows reporting the amount of data online and offline, recording the time lag with which they were received. , distinguishing from each other, in different colors.

The report must contain filters, serial numbers of the devices, names of the offender, and must be issued in a period of time convenient for the Institution.

3.9. - REQUIREMENTS FOR THE APPROPRIATE AUDIT IN ACCORDANCE WITH SERVICE LEVELS.

The Institution will have procedures and / or tools for the inspection of the services provided, in accordance with the provisions of the administrative bases, distinguishing with respect to the following levels of service, as regulated in point No. 3.9 of the technical bases:

a) Availability of the service;
b) Measurement of the timely transmission of data from the telematics monitoring service (offline data);
c) Pre-billing for installation, uninstallation and monitoring days;
d) Manuals;
e) Training;
f) Regional Center for Simultaneous Monitoring;
g) Map update;
h) Technical feasibility reports;
i) Maintenance of equipment;
j) Satellite phones;
k) Labor obligations;

4. - REQUESTED SERVICE LEVELS (SLA).

Every time a request is made, from any session, that requires a service from the

provider, it will be registered in a project management control system, which must contain an incident monitoring service.

For each item of the service, it will be necessary to generate a project to support the device, unavailability of the system, maintenance, the telephone exchange, the security cameras, and the biometric registry of access doors.

In the event of an incident, the provider must have a call center, every day of the year, where incidents will be recorded. It will be the supplier's responsibility to register the ticket, and then inform, by email, a detail of what is registered with all their data, and in the manner indicated in point No. 4 of item number IX, of the technical bases.

The incident registration system must be in a web environment, being possible to access it, from inside or outside the Institution.

The application must be provided, installed and configured by the provider, on a server arranged by him, giving himself the necessary accesses to be able to obtain reportability and follow-up of incidents.

4.1. - Support and assistance on site.

The provider must provide support and assistance, available permanently, 24 hours a day, every day of the year. The support must be oriented to:

a) Support of the monitoring system, device, telephone service, security cameras and biometric registration of access doors.
b) Support to the operators and supervisors of the Monitoring Center and, in general, to Gendarmerie personnel who require it.
c) Programming and supervision of preventive and corrective maintenance activities.
d) Other functions to be defined during the operation of the Monitoring Center.

For these functions, regardless of the support and assistance system that is designed, there must be a professional official from the provider, preferably a computer engineer, who is available 24 hours a day in the Monitoring Center, and who has the capabilities to resolve any event of the agreed upon levels of service, in addition to dealing with eventual failures of an urgent nature or other similar requirements.

4.2. - Repair and replacement of equipment in the event of failure.

The bidder shall repair and replace, by original and new parts and pieces, the equipment and accessories delivered as part of this service, when necessary.

4.3. - Terms for the installation, replacement, removal and technical support of the devices.

a. Gendarmerie will inform the supplier of the requests for installation and / or removal or replacement of the devices at least 48 hours before their execution. This implies that you must be prepared, within said period, to be able to attend where the Gendarmerie requests within the period offered for face-to-face

assistance, that is, within a period between 24 and 47.5 business hours. In case of no-show, the corresponding fines will be applied.

b. In the event that the device requires technical support, the provider will have a maximum period of 2.5 hours to solve the problem remotely, counted from when the Gendarmerie or the same provider notifies the problem. Weekends and legal holidays are excluded. In the event that the remote support does not solve the problem, within the indicated period, the provider must inform the Gendarmerie and the corresponding fines will be applied.

c. Regarding the request for the technical feasibility report for the installation of a telematics monitoring device at the domicile of the offender, the supplier must review and validate if there is technical feasibility, reporting the response online, through the WEB portal, within a maximum period 23.5 business hours. Since the consultation on the portal has been made, delivering the respective feasibility report.

If prior to validation, review and verification actions are required, the provider will have a period of 72 hours to report on the result of its review process.

d. In the case of telephone services, the response time to solve the problem, remotely, will be a maximum of one hour, counted from when the Institution or the provider has notified the problem. If the remote report does not solve the problem within the deadline, you must go to the field and give a solution in the maximum time of two hours.

e. If the services of security cameras or biometric reader in security doors have problems, the time to evaluate remotely will be 3 hours, if you do not solve the problem within the next 2 hours, you must go to the field and solve the incident.

4.4. - Preventive and corrective maintenance service.

The maintenance service must be carried out monthly or every two months, according to what is offered by the supplier in technical annex No. 9.

The provider shall deliver to the technical counterpart of the Institution, the planning of the preventive maintenance services and a monthly report of the preventive and corrective maintenance services carried out the previous month, on the first business day of each month. Strict compliance with the dates planned by the contractor will be required.

In the case of equipment installed in the communications room of the Monitoring Center, a schedule of maintenance services must be delivered on the first business day of each month.

Any modification of these schedules must be informed and justified to the technical counterpart for their authorization.

Preventive Maintenance.

Each technician participating in the maintenance procedures must sign a confidentiality commitment, which must be delivered by the provider to the Institution's technical counterpart.

The supplier must prepare forms for carrying out preventive maintenance services in each system. Once the maintenance work is completed, the corresponding tests must be carried out to ensure the continuity of the service.
The forms must contain, at least, the following information:

- Name of the technician who performs the maintenance service;
- Date and time of entry or start of maintenance work;
- Date and time of completion of maintenance work;
- List of all the tasks carried out, indicating the status before maintenance and the final status after maintenance, and the respective observations of each task.

If maintenance considers the task of measuring values, for example, percentage of use of the File System, they must be recorded in the form, which must also contain the range of values allowed for each of them.

If there are forms delivered by third parties, the provider must complete them, attaching the report of the external third party that performs the maintenance, to the maintenance report that will be submitted to the Institution.

Gendarmerie reserves the right to attend preventive maintenance services carried out in the field.

The provider will be responsible for updating the topology diagrams of each system, if modifications are made to them. These updates must be delivered no later than one day after the changes have been made.

Any maintenance work that is required to be carried out and that involves a subcontractor must be supervised continuously and in person by technical personnel authorized by the supplier. The authorization to enter the Monitoring Center that is being subject to the maintenance of subcontractor personnel must be previously requested from the Gendarmerie.

The Gendarmerie will have the right to withdraw the entry permit of a supplier's worker or any subcontractor, in which case they must substantiate their decision, without prejudice to the provisions of article No. 44 of the administrative bases regarding the right of veto. Likewise, you will have the right to request the replacement of the personnel. This will be applicable when you are not satisfied with the service provided by a provider worker.

The provider may not connect remotely to any of the data networks of the Monitoring Centers, without prior authorization granted by the Gendarmerie.
All access to reading, operation or modification of any system or database of the Monitoring Center or equipment installed in the communication room, must be previously authorized by the Gendarmerie.

Preventive maintenance report.

The general maintenance of the system must comply with what is offered by the supplier, and as a minimum, with the aspects indicated in technical annex N ° 9, attached to the bases “general requirements for the execution of maintenance services” and technical annex N ° 19 “preventive maintenance procedure of the communications room and monitoring centers”.

For the specific maintenance of computer systems, you should take as an example of a report, technical annex N ° 10, attached to the bases "monthly report of alarms and performance of the hardware and software of the monitoring platform."

Corrective maintenance report.

All equipment repairs should be carried out according to the original manufacturer specifications.

The supplier must generate a corrective maintenance report every time an action of this nature is carried out. This report must be submitted no later than 48 hours after the failure, which must contain, at least, the following information:

- Place, date and time;
- Responsible for the repair procedure;
- Fault description;
- Cause of malfunction;
- Technical solutions adopted (repair, replacement, etc.);
- Post-repair system performance level.

Gendarmerie reserves the right to attend corrective maintenance services carried out in the field.

4.5. - Updating and / or modifying the system.

When requesting an update or change in the system, the supplier must comply with the procedure and deadlines stipulated in point N ° 4.5 of section number IX, of the technical bases.

5. - Technical feasibility management report procedure.

The provider must have a WEB system, which can be the same as the monitoring system that allows administrative management as indicated in the technical bases. This system must be operational at all times, every day of the year, and must allow the registration of everyone, to generate requests for technical feasibility reports.

Requests must be answered by the provider, through the system, within 23.5 business hours from the validation of the request.

The general procedure for managing requests for technical feasibility reports will be that regulated in point No. 5, section number IX, of the technical bases, and the forms described in said numeral must be used.

6. - Training and manuals:

It will be the sole responsibility of the provider to guarantee specialized training to the personnel of the Telematics Monitoring Department of the National Monitoring Center, the Regional Center of Simultaneous Monitoring and the local monitoring coordinators (CLM in Spanish) of the Social Reintegration Centers (CRS in Spanish) of the country, from the start and continuously throughout the

provision of the service, always in collaboration and under the supervision of the corresponding Department.

The provider undertakes to carry out unlimited training for the CM in Santiago, when required by the Gendarmerie, and to agree for the CMRS (Regional Center of Simultaneous Monitoring) in Puerto Montt. In turn, it undertakes to provide all the on-line (remote) training that is required of it, for all personnel that perform functions at the national level in the electronic monitoring of offenders. The trainings will be carried out after coordinating activities with the Head of the Telematics Monitoring Department.

The technical counterpart, when there are well-founded reasons for good service that warrant it, may extend the training to the personnel of other entities dependent on the Institution, as well as other public institutions that by their nature are related to the Telematics Monitoring Department in these matters.

100% of the staff of the Telematics Monitoring Department must be trained at the initial moment of the provision of services. This training may not last less than 40 hours, owing 30% of the total hours, to be devoted to the subjects indicated in point 6.3 of section IX of the technical bases. For these purposes, it is estimated that the Telematics Monitoring Department will have a staff of approximately 150 officials to train.

In addition, in order to maintain an adequate provision of the service, initial training must be provided, in the terms indicated in the preceding paragraph, to new officials who serve in the Department.

All costs associated with the training activities, including travel costs to regions to carry out training in the CRS, will be borne by the provider, except for those related to the transfer and residence of the officials to be trained

6.1. - Subjects to train.

Gendarmerie personnel must be trained in the following specified matters:

a. Training of operators regarding the platform and monitoring system.
b. Training for local monitoring coordinators regarding the installation / uninstallation of mobile devices.
c. Training regarding the administrative management system, technical feasibility and statistical reporting.
d. Training regarding the computerized system for registering and automatically storing information regarding the operational and administrative management of the contract.
e. Descriptive training on the procedures for using the following elements:

- Telephone exchange and satellite telephones.
- Administration of the access control system.
- Air conditioning and climate system.
- Anti-fire system.
- Generator set and backup batteries.

Training, operation and problem solving manuals must be delivered for each of the topics specified in the previous paragraph, in accordance with the provisions of technical annex No. 7 of the bidding conditions.
The delivery of the manuals must be carried out within the period established in the Gantt Letter presented by the supplier.

6.2. - Training agenda.

The supplier must prepare the training as offered and in accordance with the provisions of technical annex N ° 7, “proposed agenda for training and deliverable manuals for operators of the monitoring platform”, and technical annex N ° 8, which establishes the “proposed agenda for training and manuals for installers of mobile and fixed devices”, both attached to the bases. In addition, you should consider training software tools or statistical, administration and job management modules.

You must deliver a printed manual, of each chapter, to each one of the participating students and its corresponding electronic version (PDF, WORD, or other, on 5 replicated CDs and a pendrive), being able to add more topics, if you deem it necessary. In addition, you should consider training in the statistical, administration, and job management modules.

6.3. - Other matters to consider.

Communicative skills.

In order to achieve an efficient and persuasive domain in the handling of verbal expression techniques, a diction and communication course should be considered for the operators and supervisors of the Monitoring Centers.

Conflict and crisis management.

The training plan should consider the training of the operators and supervisors of the monitoring system, aimed at acquiring knowledge, techniques and strategies, which allow it to minimize the impact of any contingency, generated by emergency situations and / or crises. This training must provide competencies and skills that allow operators to respond, promptly and professionally, to emergencies that arise due to their function.

The agenda of communication skills training, conflict and crisis management, will be agreed between the provider and the Gendarmerie.

6.4. - Language of training and manuals.

The training and manuals must be delivered in Spanish. The use of technical initials and acronyms in English is allowed, which must be explained in a glossary of technical terms.

In addition to the manuals delivered to each student in each course, 2 copies of quick reference manuals for troubleshooting (troubleshooting) must be delivered for each of the subjects to be trained. Likewise, the set of backups must be delivered in electronic format (PDF, WORD, or other) on 5 replicated CDs and on a USB stick.

6.4. - Place of training.

The trainings will be carried out in dependencies provided by the provider, without prejudice to the fact that they may also take place in authorized spaces of the Institution.
You must have all the materials and laboratories necessary to carry out the required training, and consider a 20-minute coffee break (tea, coffee, mineral water, juice and cookies), mid-morning and mid-afternoon, during each day of the training provided.

6.5. - Evaluation of the training teacher.

The training teacher will be evaluated, at the end of the course, by his students, through a survey, which will measure:

a. Ease of explaining concepts;
b. Use of practical examples;
c. Level of handling of the subjects that it exposes;
d. Level of motivation for students to actively participate in classes.
In case the teacher evaluation survey shows less than 70% satisfaction, the provider must repeat the course and assign a new trainer.

6.6. - Training certificate.

A certificate of participation must be delivered, in each of the trainings, when the student registers an attendance greater than or equal to 80%.

SIXTH: FAITHFUL GUARANTEE AND TIMELY COMPLIANCE WITH THE CONTRACT.

In order to confirm the faithful and timely fulfillment of this contract, the supplier has delivered the following guarantee documents:

1.- [***].

2.- [***].

If as a result of the time elapsed during the processing of this contract before the Comptroller General of the Republic, the guarantees provided lose the minimum validity required in the bases, these must be renewed, extended, or new guarantees must be delivered, which comply with all the established conditions. in article 33 of the administrative bases, and that contemplate the minimum term of validity required, that is, equivalent to the term of the contract, increased by 180 calendar days, which must be verified within 30 days from the date publication of the resolution approving this contract fully processed.

The guarantees will be returned once their respective terms of validity have expired, provided that the technical counterpart has certified their total conformity with the provision of the contracted service, and the fulfillment of the labor and social security obligations of the supplier's workers is duly accredited.

The guarantees may be presented for collection, without distinction, when the supplier does not comply with the obligations indicated in this contract, which

contains those established in the administrative and technical bidding conditions and the conditions offered by the supplier.

In the event that companies or any of the guarantees of faithful and timely fulfillment of the contract are collected, due to the application of one or more fines, the supplier must renew said guarantee or deliver a new one, in order to keep the original amounts indicated in this clause, which always requires a correspondent at least 15% of the total value of the contract, including taxes.

The deadline to comply with this obligation will be five business days, counted from the time the provider receives the payment for the original document or documents.

SEVENTH: COORDINATOR OF THE CONTRACT AND TECHNICAL COUNTERPARTY.

The provider names [***], as the coordinator of the contract, who will act as a valid interlocutor with the Institution's technical counterpart. In carrying out his task, the contract coordinator must, at least, carry out the following actions:

a) Represent the supplier in matters related to the execution of the contract.
b) Coordinate the actions that are pertinent to the operation and fulfillment of the obligations of the contract.
c) Report all situations that could affect the proper operation of the contracted service, within 24 hours after they occur, without prejudice to the responsibilities that the provider may incur.
d) Has a cell phone destined for this purpose, and be available twenty-four hours a day, from Monday to Sunday.

Any change regarding the contract coordinator must be informed by a legal representative of the supplier, in writing, at least five days before the change is made. The information should be directed to the Gendarmerie technical counterpart. The Institution will formalize the change, through the corresponding administrative act.

The technical counterpart of Gendarmerie of Chile will be made up of a collegiate entity, called the “Technical Counterpart Commission”, which will be in charge of relating to the supplier for the faithful and timely fulfillment of the contract.

The Technical Counterpart Commission will be made up of the Head of the Telematics Monitoring Department, who will chair it, and a technical commission of officials. In case of absence or impediment, the President will be subrogated by whoever corresponds.

The technical commission will be made up of the following Chilean Gendarmerie officials:

1. - A representative of the National Director;

2. - The Deputy Director of Administration and Finance, or whoever he designates on his behalf;

3. - The Deputy Director of Social Reintegration, or whoever he designates in his representation;

4. - The Operational Deputy Director, or whoever he designates on his behalf;

5. - The Head of the Prosecution Unit, or whoever he designates on his behalf;

6. - The Head of the IT Department, or whoever he designates on his behalf;

7. - The Head of the Department of Technovigilance and Radiocommunications, or whoever he designates on his behalf;

The Technical Counterpart Commission will have the following functions:

a) Decide on the correct execution of the service, each time it is called by the relevant authorities;

b) To pronounce on the origin of the application of fines, within the framework of the procedure established in chapter X, of the administrative bases, and what is regulated in clause eight of this contract;

c) Decide on the early termination of the contract, in accordance with the provisions of chapter XV of the administrative bases, and the provisions of clause ninth of this contract;

d) The others entrusted by the bidding rules.

The president of the technical commission will have the following functions:

a) Supervise, coordinate and supervise the proper fulfillment of the contract and all the aspects considered in the bases, ensuring the faithful, complete and timely fulfillment thereof;

b) Communicate, by any means, with the contract coordinator, giving him formal and substantive observations regarding the development of the service provided;

c) To inspect that the execution of the service strictly adheres to what is indicated in the administrative and technical bases, to what is offered by the provider, and the other antecedents that govern the contracting;

d) To ensure the correct development of the contract, informing, by letter, the Logistics Department and the Accounting and Budget Department, in case fines should be applied, for their discount of the respective payment statements or of the guarantee of faithful compliance , as appropriate;

e) Give approval and reception according to the services, processing payments, as appropriate;

f) Maintain permanent control over the execution of the services, through any means or form that is suitable for these purposes;

g) Authorize in writing, adjustments to the project;

h) Address and resolve relevant or emerging situations, not considered in the contract or in the administrative and technical bases;

i) Exercise the right to veto established in clause No. 16 of this contract;

j) The others entrusted by the administrative and technical bases.

In relation to the provisions of letter e) above, it will correspond to permanently endorse the execution of the service and, consequently, request payment thereof, in accordance with the provisions of the third clause of this contract.

The supplier must grant all the facilities intended for the execution of the control and supervision functions of the technical counterpart of the Gendarmerie of Chile.

EIGHTH: FINE FOR NON-COMPLIANCE.

When the technical counterpart detects a fact constituting non-compliance, which leads to the application of a fine, it will promptly communicate said situation to the supplier, in writing, who will have a period of five days to prepare a technical report of the incident and, where appropriate make your discharges.

The aforementioned report should be addressed to the Head of the Telematics Monitoring Department, in his capacity as president of the Technical Counterpart Commission, and delivered materially to the said Department's secretariat.

In these discharges, the supplier may assert all the rights that Law No. 19,880, of 2003, recognizes as an interested party in an administrative procedure, being able, by way of example, to propose the actions or measures that it deems necessary, as well as, request or accompany the means of evidence that it deems appropriate.

The technical counterpart will have the quality of instructor in the administrative sanctioning procedure that is developed, and by virtue of its executive and decision-making powers, may proceed to:

a) Formally establish, in accordance with the provisions of article No. 43 of the administrative bases, a verification procedure that assures the participants the protection of the principles of audience bilaterality, contradictory and impartiality.

b) Form evaluation commissions, calls to know and suggest the final resolution of the procedure, to the technical counterpart.

c) Order the opening of a trial period, in order to carry out the evidentiary proceedings it deems appropriate.

d) Require, from the supplier, the display of the background that is necessary to determine the degree of compliance with the obligation.

e) Appreciate the evidentiary means that are accompanied, in conscience, looking after institutional interests and contractual good faith.

During the instruction of the procedure, the supplier must make available to the technical counterpart, within the previously granted term, all the documents, antecedents and technological or related means that are requested, in order to facilitate the accreditation or dismissal of the facts procedural matter.

In case of not complying with the above in a timely manner, a fine may be applied for delays in the delivery of information.

Once the instruction of the procedure has concluded, or the expiration of the period for receiving the releases, without having been presented, a report will be issued by the president of the Technical Counterpart Commission, in which the National Director may be proposed to Gendarmerie of Chile, the application or not of a certain sanction, which will be specified through a founded resolution.

The sanction will be notified personally to the provider's legal representative, or through a registered letter, addressed to the provider's address. The notification by registered letter, will be understood as practiced on the third day after entering the corresponding Post office.

The corresponding fines will be administratively processed, without form of judgment, and will be deducted from the payment status or from the guarantee of faithful and timely fulfillment of the contract, if those were not sufficient, in that order of priority.

In all cases, the application of fines may not exceed 10% of the total amount of the V.A.T included. If it exceeds said limit, the Institution may terminate the contract early.

The supplier may claim this act, using the resources and within the terms established by current legislation.

In addition, if the breach will cause damage to the Gendarmerie of Chile, the appropriate legal actions must be initiated, through the competent bodies, without prejudice to giving the corresponding notices to the Directorate of Public Procurement and Contracting.

INFRACTIONAL BEHAVIORS AND FINES

1. - Fines related to levels of service availability.

1.1. - Unscheduled unavailability of the telematics monitoring service:

In the event that the supplier presents a breach in the total available minutes of the contracted monitoring system, in the times indicated in each case, according to the level of availability of the service indicated in numeral 1.4 of section number IX, of the technical bases, a fine equivalent to:

a) [***], if the breach occurs for the period of 1 minute to 60 minutes inclusive, within a calendar month.

b) [***], if the default is greater than 61 minutes and less than or equal to 120 minutes, within a calendar month.

c) [***], if the default is greater than 121 minutes and less than or equal to 150 minutes, within a calendar month.

d) If the breach exceeds 2 hours and thirty minutes of unavailability of the system, the contract will be terminated early, within a calendar month.

1.2. - Non-compliance in response times for access to information:

a) [***] if there are delays, in a month, greater than 20 seconds, in the response time, from 1 to 100 times.

b) [***] if there are delays, in a month, greater than 20 seconds, in the response time, from 101 to 200 times.

c) [***] if there are delays, in a month, greater than 20 seconds, in the response time, on more than 200 times.

The measurement of these times will be applied in accordance with the tools of the telematics monitoring system for offenders, therefore, it is applicable to sentence control operating systems, such as alarm systems, maps, technical feasibility, and others related to matter.

The reporting system or others of an administrative nature that are not related to the penalty control operating systems are excluded from this measurement.

1.2. - Non-compliance in response times for access to information:

a) [***] if there are delays, in a month, greater than 20 seconds, in the response time, from 1 to 100 times.

b) [***] if there are delays, in a month, greater than 20 seconds, in the response time, from 101 to 200 times.

c) [***] if there are delays, in a month, greater than 20 seconds, in the response time, on more than 200 occasions.

The measurement of these times will be applied in accordance with the tools of the telematics monitoring system for offenders, therefore, it is applicable to sentence control operating systems, such as alarm systems, maps, technical feasibility, and others related to matter.

The reporting system or others of an administrative nature that are not related to the penalty control operating systems are excluded from this measurement.

1.3. - Unavailability of the system due to supplier work:

The provider must schedule and report periodic system maintenance jobs, in writing, to the Head of the Telematics Monitoring Department, at least one month in advance, indicating the specific time that such jobs will take. The Head of the Department may accept or reject the request.

In case of accepting, the supplier must adopt the necessary technical measures so that, during the execution of the works, the system is, at all times, operational and available, providing the functionalities inherent to the service for which it was contracted.

The fines indicated in point 1.1., above, will be applied for the same time ranges and amounts, in the event of unavailability of the system during the performance of the work that has been reported.

To determine the circumstance of having verified an unavailability of the system, you must follow the procedures for verifying contractual obligations, which the Institution will prepare in accordance with the provisions of article No. 43 of the administrative bases, without prejudice to the rules established in section IX. , of the technical bases, referring to the requirements of the technical offer.

2. - Fines related to the lack of timely transmission of data from the telematics monitoring service (Offline data).

These fines will be applied in the event that the supplier presents a breach in the number of data "online" (data registered in the system in due course) during a period of specific control of a subject, received in the monitoring system.

These breaches will be considered "offline" data, and is data that was not viewed, recorded and transmitted in a timely manner in the system.

The data offline, will be determined daily, according to numeral 3.8 and 3.9 of section IX of the technical bases, referred to the requirements of the technical offer, and will be subject to the following fines, according to the recorded times of data offline, for each monitored device.

a) [***], between 16 and 30 minutes, inclusive, for each episode of signal loss.

b) [***], between 31 and 45 minutes, inclusive, for each episode of signal loss.

c) [***], between 46 and 60 minutes, both inclusive, for each episode of signal loss.

d) [***], if the time exceeds 60 continuous minutes of signal loss.

Loss of signal (offline) will not be considered those events in which the offender has malicious intervention, such as manipulation and cutting of the strap, concealment of the device by means that block the signal, including failure to charge the device.
3. - Fines related to the installation, uninstallation, replacement or technical support, on site, of the telematics monitoring devices.

In the event that the supplier presents a breach on the day and / or at the time notified by the Gendarmerie to carry out the installation, uninstallation, replacement or technical support, on site, of any of the telematics monitoring devices, which includes the contracted service, in the terms indicated in its offer and in section 4.3 of number IX, of the technical bases, a fine will be applied, for each device involved in the breach, equivalent to:

a) [***], if the breach is more than 30 minutes and less than 60 minutes, to appear at the place determined in the notification made by the Gendarmerie to the supplier.

b) [***], if the breach is equal to 60 minutes, to appear at the place determined in the notification made by the Gendarmerie to the supplier.

c) [***], if the breach is greater than 60 minutes or equal to 120 minutes, to appear at the place determined in the notification made by the Gendarmerie to the supplier.

d) [***], if the breach exceeds 120 minutes, to appear at the place determined in the notification made by the Gendarmerie to the supplier. In this case, the respective installation, uninstallation, replacement or technical support will be considered as failed.

This fine will be applicable to the installation, uninstallation and replacement of beacon or technical support of any other technological means complementary to the offered system that must be installed in the offender, victims or their homes.

The Gendarmerie will determine the day and time of these activities, in relation to the technical offer presented by the supplier, relative to its logistical capacity, as established in the section indicated above in the technical bases.

For the purposes of determining the scheduled hours, the presentation of the technician, and in which the procedure was carried out, it will be as stamped in the act that the local coordinator of monitoring of the Institution will prepare, which will be uploaded to the administrative management system.

4. - Fines related to technical feasibility reports.

In the event that the supplier is in delay in sending the technical feasibility report, requested by the Gendarmerie, in the terms indicated in its offer and in section 4.3. of number IX, of the technical bases, or in case of inaccuracies in the information contained therein, a fine equivalent to [***] will be applied, after 24 hours have elapsed, counted from the validation and request made by the Gendarmerie , sum that will be applicable for each following day of delay.

If there is a delay in relation to the 72 hours that the provider has to report on the result of its review process, when prior to the validation of the request, it is required by the Institution, to carry out actions of review and verification, in the terms provided in point No. 5 of the technical bases, a fine equivalent to [***] will be applied, for each day of delay.

In the event that the provider has positively informed a request for a technical feasibility report, ensuring the existence of sufficient cellular coverage in a specific area and / or home, to carry out telematics monitoring, and it is verified that said coverage is not such, has been lost or is insufficient to carry out the monitoring, due to signal loss, a fine of [***] will be applied for each erroneous technical feasibility report.

Without prejudice to the provisions of article 43 of the administrative bases, for the purposes of verifying the aforementioned circumstance, the technical reports prepared by the Telematics Monitoring Department, the respective Social Reintegration Center, and the response that, in this regard, will be followed. , evacuate the provider.

5. - Fines related to maintenance of the equipment involved in the service.

In the event that the supplier presents a breach in the execution of the maintenance of the equipment involved in the service, in the terms indicated in numeral 4 of section number IX, of the technical bases, a fine equivalent to:

a) [***], for each day of delay in the execution of corrective maintenance on the equipment involved in the service.

b) [***], for each day of delay in the execution of preventive maintenance on the equipment involved in the service.

6. - Fines related to remote technical support and assistance on site.

In the event that the supplier does not meet the technical requirement, does not provide a solution to the problem posed, in the maximum time offered to provide remote technical support in the event of failures in the system and / or devices, or does not inform the Gendarmerie of the impossibility of providing a solution remote within the term indicated in the terms indicated in numerals 4.1 and 4.3 of section number IX "Requirements of the technical offer", of the technical bases, a fine equivalent to [***] will be applied, each time technical support is attended or not performed, the impossibility of remote solution is not reported, or the support officer is not available in the active monitoring center, without prior approval from the head of the monitoring center.

7. - Fines related to delivery and implementation of the project.

In the event that the supplier presents a breach in the delivery of the project to the Gendarmerie, in the terms indicated in its offer and in section number X "Project Implementation", of the technical bases, a fine equivalent to [***], for each day of delay.

Likewise, in the event of specific breaches, in relation to the conditions, terms and deadlines, committed in the Gantt Letter of implementation and operation of the service, referred to in article 15, letter e) of the administrative bases, affecting the migration process referred to in point number X, letter a.6, of the technical bases, a fine of [***] will be applied.

8. - Fines related to training.

In the event that the supplier presents a breach in the execution of the training planning in the service, in the terms indicated in numeral 6 of section number IX "Requirements of the technical offer", of the technical bases, a fine will be applied equivalent [***], for each day of delay in its execution.

9. - Fines related to updating maps.

In the event that the supplier presents a breach in updating the maps provided, in their relevant aspects, in the terms indicated in numeral 1.3 of section number IX, of the technical bases, a fine equivalent to [***] for the official update, and [***] for the update at the request of the Institution, both for each day of delay in the execution of the required update.
10. - Fines related to delivery of manuals.

In the event that the supplier presents a breach in the delivery of manuals, in the terms indicated in its offer and in number 6 of section number IX, of the technical bases, a fine equivalent to [***] will be applied.), for each day of delay with respect to the delivery date indicated in the Gantt letter, of the supplier's offer.

11. - Fines related to the Regional Simultaneous Monitoring Center.

In the event that the supplier presents a breach in the operational delivery of the Regional Center for Simultaneous Monitoring, in the terms indicated in section number VIII and number 3 of section number IX, of the technical bases, a fine equivalent to [***], for each day of delay.

12. - Fines related to support the call registration system.

In the event that the provider presents a breach in the storage of backup files of the call log system, in the terms indicated in number 3.4 of section number IX, of the technical bases, a fine equivalent to [***] will be applied [***], for each unsupported registration.

13. – Fines related to satellite phones.

In the event that the provider has a fault or malfunction in the satellite phones, that communication has no problems in up to 3 consecutive failed communication attempts, or there is no available balance in the terms indicated in number 3.5 of section number IX From the technical bases, a fine equivalent to [***] [***] will be applied, for each team that fails or does not have an available balance.

14. - Fines related to last year of service operation.

In the event that the supplier presents a breach in the delivery of the planning for the last year of operation, in the terms indicated in section number XI "Termination of the Service and migration of the operation of the telematics monitoring system to the new winning company, prior to the contract term", of the technical bases, a fine equivalent to [***] will be applied, for each day of delay.

In addition, in the event that the supplier presents a breach in the execution of the migration processes, in the terms indicated in said section of the technical bases, a fine equivalent to [***] will be applied.), for each day of delay.

15. - Fines related to breach of labor and social security obligations.

In the event that the supplier is in breach of its labor and social security obligations, during the period of execution of the contract, a fine equivalent to 10% of the invoiced amount will be applied, in the respective payment status.

This fine may be issued with a limit of six opportunities. In such case, once a new breach by the supplier is verified, an early termination of the contract must be made in accordance with the provisions of article 74 No. 6 of the administrative bases.

The status of compliance with the provider's labor and social security obligations will be accredited in accordance with the provisions of article 67 of the administrative bases

16. - Fines related to breaches of the technical functionalities compromised for the telematics monitoring system.

In the event that the supplier presents non-compliances, in relation to the technical standards it undertakes, with respect to the various functionalities of the system, a fine equivalent to:

a) [***], in the event of noncompliance with the level of coverage committed, in accordance with the provisions of point 1.2, section IX, of the technical bases.

b) [***], in case of non-compliance in relation to the times committed by the offeror for the instant communication of alarms and warnings, in accordance with the provisions of point 1.1. Letter e) of section number IX of the technical bases.

c) [***], in case of non-compliance in relation to the committed times for the “real-time identification” of the monitored, in accordance with the provisions of point 1.1. Letter a), of section number IX, of the technical bases.

d) [***], in the event of non-compliance in relation to the distances compromised as a tolerated margin of error, to determine the positioning of the monitored, in accordance with the provisions of point 1.1. Letter b) of section number IX of the technical bases.

e) [***], for each day of delay in the delivery of system update or modification, categorized as “low” complexity, in accordance with the provisions of point 4 “requested service levels”, and 4.5 “updating and / or modification of the system”, of the technical bases.

f) [***], for each day of delay in the delivery of updating or modifying the system, categorized as “medium” complexity, in accordance with the provisions of point 4 “requested service levels” , and 4.5 "updating and / or modification of the system", of the technical bases.

g) [***], for each day of delay in the delivery of system update or modification, categorized as "high" complexity, in accordance with the provisions of point 4 "requested service levels", and 4.5 “updating and / or modification of the system”, of the technical bases.

For the purposes of evaluating the functionalities of the system described here, and in accordance with the control powers established in article 43 of the administrative bases, the Institution will carry out quarterly measurement tests, according to the "procedures for verifying compliance with contractual obligations", which are established.

17. - Fines related to delays in the delivery of information.

In the event that the supplier presents delays in the delivery of information regarding the execution of the contract, which has been formally required by the Institution, a fine of [***] will be applied, for each day of unjustified delay, in relation to the term that is expressly and formally agreed.

NINTH: EARLY TERM OF THE CONTRACT.

The contract may be terminated early if any of the causes or circumstances provided for in article 13 of the public procurement law or article 77 of its regulations are verified, namely:

1. Reconciliation or mutual agreement of the contractors.

2. Serious breach of the obligations contracted by the supplier. The following shall be considered as such:

a) Complete unavailability of the system for more than twelve continuous hours, more than six times in a semester (each six month), not attributable to fortuitous cases or natural catastrophes.

b) Unavailability to view more than 30% of those offenders, for more than twenty-four hours, more than six times in a calendar year, not attributable to fortuitous cases or natural catastrophes.

c) Unavailability of the system to view a offenders for more than twenty-four hours, continuously, for more than thirty-six times in a semester (each six month), not attributable to fortuitous cases, natural disasters or improper manipulation by the offender of the monitoring device .

3. Failure to comply with 100% of the functionalities of the Service, that is, both those required in the bidding rules and those offered during the bidding process, within the terms contemplated in section number X, of the technical bases, called "Project implementation".

4. State of notorious insolvency or bankruptcy of the provider, unless the guarantees provided or the existing ones are improved to guarantee compliance with the contract.

5. by requiring the public interest or national security.

6. For registering unpaid balances of wages or social security contributions, with their current workers, or with workers hired in the last two years, without having proven that all the obligations are settled, in the middle of the period of execution of the contract, with a maximum of six months; or, in case of registering repeated non-compliance, in the terms established in article 64 of the bases.
7. For verified repeated breaches of a contractual obligation that has been subject to an administrative fine. “Repeated non-compliance” shall be understood as the occurrence of three non-compliances subject to fines, within a semester (each six month).

8. The others that are established in the bidding conditions.

In all cases, except Numbers 1 and 5, the Institution will proceed to collect the guarantee documents of faithful and timely fulfillment of the contract.

When the president of the Technical Counterparty Commission detects a fact constituting an infringement, which leads to the early termination of the convention, he will promptly communicate said situation to the supplier, in writing, who will have a period of 5 days to carry out your releases.

In these releases, you can assert all the rights that Law No. 19,880, of 2003, recognizes as an interested party in an administrative procedure, being able, by way of example, to propose the actions or measures that you deem necessary,

as well as, request or accompany the means of evidence that it deems appropriate.

The president of the Technical Counterparty Commission will have the quality of instructor, in the administrative procedure that is developed, being able to order the opening of a trial period, in order to carry out the evidentiary proceedings that he deems pertinent.

Once the instruction of the procedure has concluded, or the term to receive the releases has expired, without having been sent, a report will be issued by the president of the commission, in which a proposal may be made to the National Director of the Gendarmerie of Chile the anticipated term of the contract, which must be specified by means of a founded resolution, which will be notified by registered letter, addressed to the address of the supplier, without the need for a court order. The notification shall be deemed to have been made on the third day following the receipt of the respective letter, at the Chilean Post Office corresponding to the provider's address.

The supplier may claim this act, through the resources, and within the terms established by current legislation.

In the event of an early termination of the contract, this will be understood to be completed within the period indicated by the administrative act that puts an end to it, a term that will be counted from the notification to the supplier. As long as you are not notified, all the obligations that correspond to the provider will remain in force.

If the termination of the contract causes damage to the Gendarmerie of Chile, it may exercise the corresponding compensatory actions, without prejudice to the collection of the guarantee of faithful and timely fulfillment of the contract, if applicable.

The contractual and non-contractual responsibility of the supplier will be governed, in everything not established in this clause, by the rules of the Civil Code. The procedure indicated for the case of early termination does not apply to the reconciliation or mutual agreement of the parties.

TENTH: INTELLECTUAL PROPERTY.

The product of the work carried out by the supplier or its dependents, on the occasion of the contract, such as products, diagnoses, designs, reports, manuals and, in general, any work that is carried out, in compliance with this contract, will be the property of Gendarmerie of Chile, who reserves the right to dispose of them freely, without limitations of any kind, and the provider may not carry out any act with respect to them, which is alien to the contract, without prior and express authorization from the Institution.

ELEVENTH: OBLIGATION OF CONFIDENTIALITY

The supplier must keep confidential all the information and background that it knows about the execution of the contract, and may not make use of these, for purposes other than the contract.

All the information that the provider manipulates, because of the execution of the contract, is the property of the Institution, under no circumstances may, by any title or means, reveal, disseminate, publish, sell, transfer, copy, reproduce, interfere, intercept , alter, modify, damage, disable, destroy, in whole or in part, this information, during the term of the contract or after its termination.

This prohibition will affect the supplier, its direct and indirect personnel, its consultants, subcontractors and their personnel, in whatever capacity, who are linked to the contract, in any of its stages, and their responsibility will be joint and several, even after termination.

In case of breach of this clause, Gendarmerie may terminate the contract in advance, in accordance with the provisions of chapter XV of the administrative bases and in accordance with clause ninth of this contract, being empowered to collect the guarantee slip of faithful compliance of the contract, without prejudice to initiating the corresponding legal actions for violation of the pertinent legislation.

TWELFTH: MODIFICATION OF THE CONTRACT.

In order to incorporate the advances that functionality and technology make advisable, due to regulatory requirements, force majeure reasons or situations imposed by the market, the Institution may request to introduce changes during the development of the contract.

Gendarmerie reserves the right, for reasons of convenience, during the execution of the service, to make increases or decreases in the activities involved as long as they are duly justified.

In the indicated cases, if applicable, the supplier must complement or deliver a new guarantee of faithful compliance with the contract, as appropriate.

The modifications agreed upon may not alter the total price of the contract by more than 30% (thirty percent). Said modifications must be approved through the founded administrative act, and the supplier will be obliged to maintain the unit prices per item, established in its offer.

THIRTEENTH: OF THE SYSTEM AND EQUIPMENT.

All the components of licenses and software of the system that the provider develops specifically for the service of telematics monitoring of offenders, object of this contract, will be property of Gendarmerie of Chile, from the entry into force of the contract, and the contractor will not be able to use them in other context that is not the execution of the contract, nor make them available or transfer them to third parties, without their authorization.

All the enabling equipment of the National Monitoring Center and the Regional Simultaneous Monitoring Center, including, among others, the wiring of local networks, gutters, as well as all the documentation, tapes and other magnetic storage and / or backup media, which generated, during the term of the contract, will

be the property of the Gendarmerie, from the entry into force of the contract, being able to have free access to them, in the terms indicated in the first article of the administrative bases.

It is forbidden for the provider, under all circumstances and forms, to seize, extract or retain any type of information related to the services tendered and contracted, including the information systems, documentation and data.

FOURTEENTH: ON SUBCONTRACTING.

The provider must provide the services indicated in the technical bases with its own personnel. However, with respect to those services that due to the nature of the services required by the Gendarmerie, must be subcontracted, and provided that the providers of said services are individualized in the technical offer, they may be subcontracted, under the terms provided in the offer, with such providers.

Notwithstanding the foregoing, any change in said providers must have prior, express and written authorization from the Gendarmerie, through its technical counterpart.

In any case, the contractor, or its legal continuator, will be solely responsible to the Institution for the full and timely fulfillment of the contracted services.

The provider assumes full responsibility for the contracts and subcontracts that it acquires for the execution of the contracted services, totally freeing the Chilean Gendarmerie from any responsibility in this regard.

In addition, at any time, during the term of the contract, in accordance with the provisions of article 183-C, of the Labor Code, the supplier will be required to provide a certificate accrediting the amount and status of compliance with labor and social security obligations, issued by the respective Labor Inspection, or by suitable means that guarantee the veracity of said amount and compliance status, with respect to its workers, as well as the same type of obligations that the subcontractors have with their workers, moreover, with the purpose of making effective the rights that assist Gendarmerie, to be informed, and the right of retention, enshrined in paragraphs 2 and 3, of the aforementioned legal norm, within the framework of derived subsidiary responsibility of said labor and social security obligations, to which article 183-D of the Labor Code refers.

FIFTEENTH: SUPERVISION AND AUDITING.

During the term of the contract, on the dates and in the forms it deems appropriate, the Institution shall be empowered to carry out, directly or through third parties, its supervision, control and comprehensive audit.

The supplier and its subcontractors must grant all the facilities intended for the execution of said supervision, control and audit.

In the event that a supplier or subcontractor obstructs or does not cooperate when faced with a requirement, so that the Institution may have expedited access to the required information, within the framework of supervision; or does not comply, in any way, with the obligations stipulated in paragraph 5 of article one of the administrative bases; or, in violation of letter q) of point 1.1, of section number IX,

of the technical bases, will be subject to the respective fine in accordance with the eighth clause of this contract.

The supervisions, controls, tests, requests for reports and / or tables, and the carrying out of audits, may be extended to those areas related to the scope of
the contract, and to those that without being it, are necessary to properly satisfy the former, all, without prejudice of the legal powers that the General Comptroller of the Republic has in this regard.

For the purposes of controlling and supervising the actual status of contractual obligations, the Institution shall establish procedures for verifying compliance with contractual obligations, in accordance with the provisions of the final paragraph of article 43 of the administrative bases.

This procedure must be established by reasoned resolution and the supplier must be notified before reception in accordance with Milestone No. 2.

SIXTEENTH: RIGHT TO VETO.

The Gendarmerie will have the right to veto the supplier's staff and its subcontractors, with just cause, or when the intervention of said people hinders or hamper the execution of the project.

In these cases, the supplier must replace the vetoed personnel or subcontractor, within 5 business days after the notification of the veto, made by the president of the Technical Counterpart Commission.

Gendarmerie reserves the right to request the supplier, when it deems it appropriate, taking into account the nature of the contracted service, information from its own staff or from its subcontractors regarding: full name, identity card number, and written authorization from the employee, to check your background.

Failure to deliver the requested information, within the 72 hours required, will entitle the Gendarmerie to exercise, without expression of cause, the right of veto referred to in this article with respect to the personnel whose data was not provided.

SEVENTEENH: INSURANCE.

It will be the responsibility of the supplier, during the entire term of the contract, to contract at its cost, the insurance intended to cover the risks that may affect the equipment and devices included in the service provided. Insurance must protect against all covered risks, including natural catastrophes, and malicious or terrorist acts.

The provider must submit the insurance contracts to the Gendarmerie for consideration before their conclusion. Gendarmerie will be empowered to reject insurance and demand another contract, if it considers that the conditions presented do not provide complete coverage, in the terms indicated here.

Also, during the service implementation stage, the provider must have all the necessary insurance to protect the Gendarmerie goods against damage that may occur to them and to people, as a result of the installation of the system.

The provider must prove compliance with this obligation, by means of a certificate from the insurer, stating the contracted insurance, and an authorized copy of the policies, before the start of the operation of the contracted service, for the purposes of its reception. Likewise, during the term of the contract, it must accompany said certification, in case the renewal or extension of the contracted policies is necessary.

In the event that the provider does not take these insurances, or does not renew them, or does not extend them in a timely manner, the Institution may do so, on behalf of the provider, without any responsibility for the Service, if it does not do so.

The Gendarmerie will be empowered to deduct from the amount of any of the payment statements, the price of the premiums that it has paid, duly adjusted, if appropriate, thus reimbursing its value, and the corresponding adjustments.

EIGHTEENTH: ASSURANCE OF ASSETS.

The supplier, in this act, declares and guarantees that all the goods subject to this tender are new and unused, with a manufacture of no more than 1 year, that they are free of defects attributable to the design, manufacture, materials, preparation, or any act or omission of the manufacturer, which may appear during its normal use, under the conditions in which they are normally used.
In case of discontinuance of any of the goods offered, to fulfill the object of the contracted service, and during the term of the contract, you must provide goods of similar characteristics, which will be subject to the same guarantee established in the preceding paragraph and must be compatible with the service offered, and duly authorized by the Gendarmerie technical counterpart.

The guarantee will consider the immediate change or repair of the goods, in the place where they are located, and will operate for the entire duration of the contract.

NINETEENTH: LICENSES AND SOFTWARE UPDATE.

All the programs and software delivered by the provider must have valid licenses for their use, which will be their sole responsibility, as described in their offer.

If necessary, the provider must add the corresponding licenses at his own expense, to ensure the normal operation of the systems.

All software updates and / or replacements must be made with the approval of the Gendarmerie.

TWENTY: DISCLAIMER OF LIABILITY.

Gendarmerie of Chile will not have any labor or legal relationship with the employees who work for the supplier and subcontractors. Consequently, it will not be responsible for remuneration, taxes, social security taxes, insurance against accidents at work or damages to third parties, all of which will be the sole responsibility and responsibility of the supplier and subcontractors.

TWENTY-FIRST: PROHIBITION OF ASSIGNMENT.

The provider may not assign or transfer, in any way, totally or partially, the rights and obligations arising from this contract, except in the case of merger, absorption or division of the company, the obligations will be transferred to its legal continuator , in the same conditions established in the contract.

In these cases, the supplier must inform the Gendarmerie, with respect to the merger, absorption or division decision, at least 3 months in advance of its formalization.

The foregoing is without prejudice to the fact that the supporting documents for the credits, which emanate from these contracts, can be transferred, in accordance with the rules of common law.

TWENTY-SECOND: TERMINATION OF SERVICE AND MIGRATION.

The Gendarmerie will have a period of six months after the end of the contract, to return to the supplier all the monitoring devices that were installed before the new winner entered into operation.

1. - Gantt chart of the migration process.

In the third month of the last year of service, the provider must deliver a Gantt letter with a general migration planning, which will begin the last 6 months, before the end of the contract.

For these purposes, the last year of service shall be understood as the last twelve months of the contract's validity.

The minimum processes that must be ensured during migration are:

1. Backup of historical information, in databases.
2. Backup of database configuration files.
3. Backup of the configuration files and parameters defined in the processing servers. The supplier must submit a document detailing the model or structure of the database.
4. Device change process, in case the new winning company is in operation, in parallel.
5. Enabling a dependency to generate parallel migration. The supplier must provide all the necessary conditions for the authorization of a new site, since the monitoring center must be remodeled by the new winner.
6. Appointment of a project manager, by the supplier, who will be related to the technical counterpart of the Institution. The Head of the Infrastructure Department and the Head of the Telematics Monitoring Department will act as a technical counterpart.

2. - Obligations at the end of the contract.

2.1.-Availability to develop the migration process.

In order to guarantee the full operation and continuity of the service, regardless of which company supports it in the future, the provider must make available to the Gendarmerie, the technical documentation detailing the format and order in which

the Devices send the coordinate data, or any other relevant information, in order to guarantee the recognition of the new location devices by the system software. For example, indicate if TCP or UDP is used, the socket ports used, the order in which it sends the coordinates and other parameters, the encryption of said data, etc.

2.2. - Uninstallation of infrastructure.

Both the furniture and infrastructure installed in the National Monitoring Center and the Regional Simultaneous Monitoring Center will become the property of the Gendarmerie, so the supplier will not be able to remove them, unless the Gendarmerie explicitly requests it. In the latter case, the uninstallation will be at the provider's expense.

3. - To guarantee the optimal migration, after the process is finished, the provider may continue to provide services in parallel, until all the devices owned by him are finished replacing.

TWENTY-THIRD: JURISDICTION.

Any controversy that arises from the signing of the contract and during its validity, until its completion and complete settlement, will be known by the Ordinary Courts of Justice of the commune of Santiago, without prejudice to the powers that correspond to the General Comptroller of the Republic.

TWENTY-FOURTH: DOCUMENTS AND BACKGROUND

The following documents and official history of the service are an integral part of this contract, which are expressly reproduced.

a) The administrative and technical bases, approved by Resolution Procedure No. 1,175, dated December 28, 2016, of the National Director of the Gendarmerie of Chile, with all its annexes, questions, clarifications and responses.

b) The supplier's administrative, technical and economic offer.

c) Act No. 5, of the Evaluation Commission of Purchases of the Service, dated February 12, 2020.

d) Exempt Resolution No. 1,908, dated March 10, 2020, from the National Director of the Gendarmerie of Chile, which declares the offer that it indicates inadmissible, and awards public proposal ID 634-35-LR17, for the contracting of the monitoring service telematics of offenders, due to the evaluation criteria indicated.

e) Exempt Resolution No. 3.601, dated June 26, 2020, from the National Director of the Gendarmerie of Chile, which nullifies the award of the public tender for the contracting of the telematics monitoring service for offender (ID 634-35-LR17) ordered by Exempt Resolution No. 1,908, of March 10, 2020, of this origin, for the reasons it indicates and re-adjudicates the bidder it indicates.

f) All other antecedents and documents that have been issued as a result of the public tender procedure ID 634-35-LR17, re-adjudicated under ID 634-35-R120.

These antecedents will form an integrated whole and will complement each other, considering themselves part of the contract, applying, for these purposes, the preeminence principle of the bases and its annexes as the basic framework for contracting.

TWENTY-FIFTH: DEFINED TERMS.

In case of doubt, the special terms used in this contract will have the meaning given to them in the administrative and technical bases, and their annexes.

TWENTY-SIXTH: APPLICABLE RULES.

The provisions of Law No. 19,886, of 2003, of Bases on Administrative Contracts for the Supply and Provision of Services, and its respective Regulations, contained in Supreme Decree No. 250, of 2004, as well as the provisions in Law No. 19,880 of 2003, which establishes the Bases for Administrative Procedures governing the Acts of the Bodies of the State Administration

TWENTY-SEVENTH: OF PERSONNELS.

The status of Christian Arnaldo Alveal Gutiérrez, to represent the Gendarmerie of Chile, is contained in Supreme Decree No. 34 of January 10, 2019, of the Ministry of Justice and Human Rights, while the status of Diego Almicar Peralta Valenzuela and Vesna Paola Camelio Ursic, to act on behalf and representation of Track Group Chile SpA., is recorded in a public deed issued before the Notary Public Head of the Forty-Eighth Notary Public of Santiago, Don José Musalem Saffie, dated July 12, 2013, Repertory N ° 8.354-2013, modified by public deed dated September 29, 2014, issued before the same Notary Public, Repertoire N ° 12.087-2014, documents that are not inserted because they are known by the parties.

CHRISTIAN ALVEAL GUTIÉRREZ
NATIONAL DIRECTOR
GENDARMERIE OF CHILE

DIEGO PERALTA VALENZUELA
LEGAL REPRESENTATIVE
TRACK GROUP CHILE SPA.

VESNA CAMELIO URSIC
REPRESENTANTE LEGAL
TRACK GROUP CHILE SPA.