MillerMendel
INGENUITY IN TECHNOLOGY

OPEN LETTER FROM MILLER MENDEL, INC.

DATE: November 3, 2020

FROM: Tyler Miller, President & CEO, Miller Mendel, Inc.

RE: Data Privacy and Security Concerns related to Guardian Alliance Technologies' National Applicant Information Center

Miller Mendel, Inc. recently became aware of the Guardian Alliance Technologies ("Guardian") feature called the National Applicant Information Center ("NAIC"). As explained on Guardian's website and sales video, the NAIC database created by Guardian warehouses applicants' personal and private data. Guardian describes collecting applicant personal and private data from numerous agencies and sharing that information between them in a manner that Miller Mendel believes constitutes the commercialization of private applicant data to third parties[1].

The NAIC raises potential legal and ethical concerns, particularly with regard to the commercial use of an applicants' private data, as well as the potential negative impacts it can have for public safety agencies and their applicants. To explore these risks, Miller Mendel engaged its legal counsel, Emily Maass of Immix Law Group, to evaluate Guardian's data handling practices as described in its video, and to provide her feedback, which is included in this letter.

In Miller Mendel's opinion, Guardian's NAIC raises these concerns:

- **Negative public exposure and scrutiny.** While, national trends favor increased protections for personal information, and against technological monitoring, Guardian's NAIC may trigger and incentivize additional legislation, regulation, or common law developments that could further restrict public safety agencies' ability to conduct appropriate, thorough pre-employment background investigations.
- **Litigation risks.** The Guardian NAIC may give rise to claims by individuals who feel their privacy has been unwittingly compromised, or that any alleged waiver was coerced for the applicant to continue in the pre-employment process. There is also a risk of regulatory enforcement actions, applicants' private rights of action, or class action lawsuits. These matters may be further complicated in cases where the public safety agency require applicants to use the Guardian system to be further considered for employment if personal data the applicant

[1] Opined from information provided in the attached legal memorandum concerning when State data privacy regulations may consider personal and private data as "commercialized" and/or "sold".

1425 Broadway #430
Seattle, WA 98122
www.MillerMendel.com

tjm@MillerMendel.com
(206) 333-4322 Direct
(206) 330-2094 Main

provided at the public safety agency's direction is commercialized by the third party software company.

Some Background on the NAIC

In a Guardian sales video posted to YouTube and shared to numerous other websites, Guardian characterizes the NAIC as a database of applicants' personal information. The video illustrates the NAIC is a data warehouse of the applicants' personal information. Guardian then shares that personal information with third party Guardian clients the applicant applied with for employment.[2] Guardian explains in its video (01:00), that if the applicant's answers differ from an answer given to your agency, the Guardian system "immediately" notifies the third party Guardian clients and discloses the conflicting answer the applicant gave to your agency to its third party clients, which may include private investigators.

The attached memorandum from data privacy and security attorney Emily Maass of Immix Law Group explains the legal landscape and risks for public safety agencies that use service providers who manage applicant data. Public safety agencies must evaluate whether a given service provider's systems and procedures create a risk of violating applicants' rights; expectations of privacy; do not fully comply with the data privacy and security laws and/or conflict with data breach notification requirements. Additionally, public agency employers must be careful not to inappropriately persuade or require ("coerce") applicants to use third party systems that collect private data when the service provider uses that data for their commercial benefit.

The following are some questions and considerations agencies should ask about any for-profit service provider, such as Guardian Alliance Technologies:

- If Guardian shares the information the applicant enters in the Guardian system for your agency's hiring process with its third party clients using the Guardian system, how does your agency verify those third parties and their information technology (IT) systems to ensure they are secure in receiving, maintaining and storing your applicant's private, legally protected data?

  What is your agency's legal exposure if the applicant's information collected due to your agency's requirement for the applicant to use the Guardian system is saved on third party IT systems that - 1) potentially do not meet necessary IT security requirements or, 2) their personnel accessing and viewing the information have not been vetted or otherwise approved to access and view such information to the standards and policies your own agency has established?

  Depending on the language of your state's data privacy and security laws, the prior dissemination of the applicant's information to "unvetted" and/or "unapproved" third parties may already have resulted in an unauthorized access event (a "breach"), requiring your agency

[2] According to a press release by Guardian, it has opened its software and NAIC database to private investigation firms/private investigators who are not employees of public safety agencies.

to begin data breach notifications to your applicants who have been required to use the Guardian system. Have you considered your circumstances in light of your state data privacy and security laws?

- If Guardian shares your applicant's private data collected by its Guardian system downstream with third parties, and any one of those third parties' suffers a data breach (including a breach that occurs without the third party even knowing about it), have you considered your agency's ultimate legal responsibility to ensure data breach notification and response protocols occur, as required by your state law?
- It is not uncommon for applicants to include information commonly considered as information falling within the ADA, HIPAA and GINA parameters. If an applicant enters information that discloses conditions falling within these protected areas, and that information is then shared with a third party by the Guardian system, have you taken into consideration the risk that your agency may unknowingly violate legislative disclosure limitations?
- Lateral law enforcement applicants commonly request their current employing agency not be notified they are in the hiring process with a different law enforcement agency, *until such time* a conditional offer of employment is given to the applicant. Based on how Guardian states its NAIC feature operates, if the law enforcement agency currently employing the officer utilized the Guardian system for the background investigation of the applicant, the current employer would likely be notified its officer is in a pre-employment process with a different agency. This practice may impact lateral applicants' willingness to apply at agencies using the Guardian system and may create avoidable conflict between law enforcement agencies. This issue may particularly interest the officer's labor union(s). Have you discussed this with your relevant union?
- Agencies should take into consideration liability exposure in the event a third party agency disqualifies an applicant based on the applicants' responses obtained from the Guardian system to your agency's pre-employment process.
- Agencies using a background software system should consider the impact of legal process served on third party vendors. If a third party agency or private investigator using Guardian is served legal process that requires them to provide information in its possession, this could include private information the applicant provided as part of the requirement for the applicant to use the Guardian system and likely should be under a protective order from a court[3]. Agencies should take into consideration, the potential increased risks from having private applicant data on third party, private investigator owned computers and storage devices.
- Guardian publicly stated applicant information entered into its system is kept "indefinitely." However, public agencies must consider compliance of local and state record retention and

[3] In the current national climate on law enforcement, law enforcement officers are deeply concerned for their safety and the safety of their families. On the typical PHS, applicants to law enforcement positions are required to provide details regarding their relatives (to include children), coworkers, employers (names, where they live, etc.), along with other extremely private information concerning their life history. Dissemination of this information inherently increases the risk those private details may fall into the wrong hands.

destruction requirements, and the risks associated with a software system that fails to comport with local and state requirements.

The attached memo from Attorney Emily Maass is clear:

> "A Background Software System that collects Applicant Data from a public agency's applicants and exchanges that data amongst other public agencies as a value-added service would likely qualify as a 'sale' under [current] legal standard[s]. Further, if a Background Software System collects Applicant Data from a Personal History Questionnaire as part of a free initial service and then shares that Applicant Data with a third party in exchange for a service fee, this transaction qualifies as a "sale" of personal information that exposes the public safety agency to significant legal compliance obligations under most applicable legal standards."

Based upon Guardian's own description of its system, public safety agencies using the system receive "free" applicant "pre-screening"[4] that prompts the applicant to submit his or her personal information and then, includes that personal information in the NAIC for disclosure to other Guardian clients. This scenario is aggravated in that some agencies require the applicant to use the Guardian system. The following caption is taken directly from a public safety agency's instruction to applicants[5].

> "As part of the hiring process, [the Agency] conducts a thorough background investigation of all candidates using the web-based Guardian platform to securely collect all required information and documentation for your investigation within 21 days of receiving the link. All applicants will be **required** to utilize this on-line portal by first creating a log-in for the portal, then following the applicant instructions. Users will be **required** to use this on-line portal, and all necessary documents are **required** to be uploaded into this portal by the applicant. Users will need to use the Chrome web browser on a computer. **No exceptions**." (Emphasis Added.)

In the example above, applicants are being told they must use the Guardian system. Consequently, a state law enforcement agency *is facilitating* the collection of private applicant data for a private business who appears to commercialize that data. It seems the agency will discontinue further processing of the applicant for a sworn law enforcement officer position should they not agree to enter their personal and private information into the Guardian system. An applicant who exercises their right to legally refrain from entering their personal data into a database that then shares that information for commercial benefit should never be retaliated against. If Guardian required the applicant to agree to its Terms of Use that grants Guardian permission to share the applicant's data as noted previously, this

[4] Guardian's "100% Free" triage center video can be viewed by clicking here.

[5] Source: http://agency.governmentjobs.com/alaska/job_bulletin.cfm?jobID=2696213&sharedWindow=0, "NOTIFICATION OF NEXT PHASE" section.

creates potential legal risk for the agency if Guardian uses that data for any commercial purpose that could be legally considered a "sale".

Public agencies and their service providers must follow the Americans with Disabilities Act during the pre-employment process. Requiring an applicant with a protected disability to proceed in the hiring process without reasonable accommodation can pose a liability or union grievance risk to the agency and discriminate against qualified applicants with recognized disabilities. A public safety agency that requires the applicant to utilize a background software system as their initial application may be at elevated legal risk if that agency doesn't inform applicants of an alternative, ADA compliant process.

Guardian's Contracts with Public Safety Agencies

Through public records requests, Miller Mendel obtained copies of several agreements between Guardian and public safety agencies. It is Miller Mendel's opinion in reviewing these disclosed agreements that there is a lack of the common protections for the public agency, conflicts or shortfalls with privacy and data security legal requirements, and terms that conflict with how Guardian is operating, per its own descriptions in its NAIC sales video (linked above) and other published advertising.

In each of the agreements provided from public records requests, none of the reviewed agreements included language between the public agency and Guardian authorizing Guardian to share the public safety agency applicants' data with third parties.

In the attached agreement from the State of Alaska, Miller Mendel noted there are no requirements for Guardian to maintain data related liability insurance ("cyber coverage"), and a lack of any requirement for Guardian to carry and maintain insurance coverage for intellectual property/patent infringement.

The Guardian NAIC raised the following concerns in our review of the attached State of Alaska agreement:

- Pg. 10, Exhibit "A", Section 1.1, states: "'Customer Data' means any data, information or material submitted or uploaded by Customer or during its usage of the Services. Customer Data is *and shall at all times be owned by Customer."* (Emphasis added.)
- Pg. 10, Exhibit "A", Section 3.1, states: "Subject to the terms and conditions of this Agreement, Customer hereby grants to Guardian perpetual, non-exclusive, irrevocable, non-terminable, non-transferable (except as permitted by Section 17 below) permission to access Customer Data in connection with the development, offering and delivery of Guardian's products and services *solely to the extent that Guardian does not disclose or otherwise reveal Customer Data to any third parties."* (Emphasis added.)

- Pg. 11, Exhibit "A", Section 9.2 states: *"Customer represents and warrants that it is and will continue to be in compliance with all applicable privacy and data protection laws and regulations* with respect to any Customer Data. *Customer shall be solely responsible for (i) the accuracy and completeness of all records, databases, data and information provided, submitted or uploaded by Customer or its authorized end users* in connection with this Agreement or use of the Services." (Emphasis added.)
- Pg. 13, Exhibit "A", Section 13.1 states: "Each of the parties agrees to maintain in confidence any non-public information of the other party, whether written or otherwise, disclosed by the other party in the course of performance of this Agreement that a party knows or reasonably should know is considered confidential by the disclosing party ("Confidential Information"). The Confidential Information disclosed by a party constitutes the confidential and proprietary information of the disclosing party and the receiving party agrees to treat all Confidential Information of the other in the same manner as it treats its own similar proprietary information, but in no case will the degree of care be less than reasonable care. The receiving party shall use Confidential Information of the disclosing party only in performing under this Agreement *and shall retain the Confidential Information in confidence and not disclose to any third party (except as authorized under this Agreement) without the disclosing party's express written consent*. The receiving party shall disclose the disclosing party's Confidential Information only to those employees and contractors of the receiving party who have a need to know such information for the purposes of this Agreement, and those employees and contractors must have entered into written agreements with the receiving party containing confidentiality provisions covering the Confidential Information with terms and conditions at least as restrictive as those set forth herein. (Emphasis added.)
- Pg. 16, Exhibit "A", Section 25 states: "*Customer shall comply with all applicable United States, foreign and local laws and regulations*, including, without limitation, export control laws and regulations of the U.S. Export Administration." (Emphasis Added.)

Section 9.2's (pg.11, Exhibit "A") language seems to place the accuracy of information entered *by the applicant* on the State of Alaska. This poses the question of what liability Guardian's client has when the applicant's information is shared with third parties and that information has not been investigated or confirmed by the State of Alaska before dissemination to third parties.

The eSOPH Background System Mitigates and Addresses the Related Topics

Since 2011, Miller Mendel's eSOPH background software system has been offered to public safety agencies across the nation. Today, over 70,000 applicants have been entered into the eSOPH system by dozens of law enforcement agencies across the nation that range in size from some of the smallest to the largest agencies. From the onset of the development of eSOPH in 2010, Miller Mendel partnered with some of the best employment law attorneys and data privacy attorneys.

While sharing information related to applicants who apply to positions of public trust has some benefit for the public safety agency, sharing that information must be done carefully to help ensure

compliance with industry best practices, laws and data security standards. Miller Mendel views it as inappropriate for a service provider to use private, applicant provided data for commercial exploitation. It is important to respect each individual applicants' rights and not risk violating existing laws surrounding those rights, which would inherently erode both applicant and public trust. Miller Mendel believes that:

- The licensing agreement(s) governing public safety agencies use of third party background investigation software systems must clearly state the client (public safety agency) owns all data, including data entered by the applicant and third parties (e.g., references). The security of the system and the related data must meet or exceed CJIS policy requirements and generally be inaccessible by the software company. This prevents unauthorized access and prevents the software company from delivering "readable" data should the software company be served a subpoena or similar legal process.
- Systems that automatically release applicant provided data create unnecessary risk for the public safety agency. Each of the 50 states have their own data privacy and security laws with related data breach notification requirements. These laws will inherently change, state by state as time goes on. If your agency subscribes to a service that becomes non-compliant as result of a change in the data privacy and security law(s) in your state, it's unlikely your agency will have the necessary immediate control over the system to comply with legal changes. Therefore, agencies should not use a service that, on its own and "automatically", shares data inputted by the applicant.
- Recognizing there is value in sharing information regarding applicants to public safety positions, Miller Mendel evaluated several ways of accomplishing this aspect that are legally sound, mitigate risk and calm the nerves of human resources and risk management personnel at public agencies. As a result of these considerations, Miller Mendel (10 years ago) developed the information sharing feature in eSOPH to function as follows:
    - eSOPH does not, on its own, share applicant inputted data. eSOPH displays to other agencies on the system only the agency's name, name of the position applied for and contact information for the agencies the applicant has previously applied. eSOPH does not share any other information automatically. This specific information is not the information *the applicant* entered; it is information public agency's personnel entered.
    - Should an agency want to share information from their eSOPH system with a third party, eSOPH users who have permission rights from the system administrator(s) may share only the 'pieces' of information from the applicant file that have been approved for sharing in compliance with your agency's standards and policies. This allows your agency to first obtain and review a waiver signed by the applicant authorizing such sharing of their information.
    - Each agency may draft their own "Terms of Access" in the eSOPH system that a recipient of shared information must agree to prior to viewing any shared information.

- Applicant information may be shared with agencies who do not use eSOPH; Miller Mendel does not require an agency to be a client to receive shared information from an agency/client using eSOPH. Requiring a recipient to be a client to receive the data could be considered an element of commercializing and selling protected applicant data.
- Links to the shared information are secure and forced to expire within a maximum of three calendar days of initiating the share. Passwords to view the received information are required and generated by the eSOPH system to ensure they meet the password requirements set forth in CJIS policy. Your agency's personnel must provide the password to the recipient of the shared information in a secure manner.
- An audit log designed for supervisors and managers allows them to see all details of sharing that has occurred from the eSOPH system, to include the details of who the recipient was, date shared, who authorized the shared information and what exact information was shared from the applicant file.
- eSOPH system users can receive a notification to their email anytime information is shared by the system.
- Sharing ability from the eSOPH system can be 'locked down' to only allow certain users authorized to share. The sharing feature can also be disabled completely for all users.

There are several concepts on the table nationwide for "police reforms". While Miller Mendel agrees that proper background investigations are essential to helping with overall efforts of hiring ideal candidates, we also respect and care about current laws and applicants' rights and the safety of applicants who become hired law enforcement officers. While it is a public safety agency's responsibility to use efficient and effective hiring tools and practices, it is also their responsibility to respect the rights of everyone, including applicants, and mitigate costly taxpayer funded lawsuit defense and the negative press that comes with unlawful or inappropriate acts.

Miller Mendel respects the law and operates transparently with both our clients and their applicants.

- Miller Mendel engaged subject matter experts on various topics such as data privacy and security, employment law and government contract law, during the initial research and development of eSOPH.
- Miller Mendel maintains relationships with data privacy and security and employment law counsel. Miller Mendel engages these attorneys on an annual basis to review important, high-risk areas such as data privacy and security and employment law, because these areas of law are fluid. In addition, our Terms of Use and Privacy Policies for applicants are reviewed by legal counsel at least annually, as is the licensing agreement used with our clients. Our attorneys are often engaged to understand how the system operates to provide the best legal advice and written agreements to use with applicants and our public safety agency clients.

- Miller Mendel's licensing agreement for the eSOPH system specifically and clearly states that each client owns their data, which includes the data applicants input into the system. That data is encrypted and handled using methods that meet and exceed CJIS and HIPAA standards.

  Only the client can view their unencrypted data. This helps to ensure any legal process served on Miller Mendel, such as subpoenas, cannot result in the release of any "readable" data from a client's eSOPH database.

- With the help of legal counsel, Miller Mendel has completed focused reviews of our data handling practices in the eSOPH system. Through these regular reviews, we ensure that Miller Mendel does not engage in practices that could be considered commercialization of applicant data or a "sale" of such data. An example of steps we have taken to establish Miller Mendel does not commercialize or engage in activity that may qualify as a "sale" of data, includes:

  - Miller Mendel does not create advertisements or "promotions" relating to sharing applicant provided data for any purpose.
  - Miller Mendel does not create marketing materials based on the premise of sharing applicant provided data with third parties.
  - Miller Mendel does not offer "free" services, such as "free pre-screening" that captures personal data entered by the applicant; a practice that can easily be construed as a commercial "trade" between a public agency and the background investigation software company off the backs of applicants.
  - Miller Mendel charges for long term data storage, as the licensing agreement for the eSOPH system clearly states that the client owns their data. We also give our clients robust, customizable automated archive and purging tools to manage their data storage costs and compliance with public records retention and destruction requirements.
  - Miller Mendel's eSOPH system does not, on its own, share *applicant inputted* data. Should agency personnel wish to share applicant inputted information, they can manually initiate this action from within the system in compliance with their agency's current standards and policies governing sharing of applicant data.

Miller Mendel has received a tremendous amount of praise for our operating practices and procedures over the last 10 years. We truly partner with each of our clients to provide a system that addresses their needs and helps to mitigate the liability risks that are inherently associated with pre-employment processes. Miller Mendel would never engage in commercializing data that violates the trust and rights of our clients or their applicants.

After 10 years of business forming valued, trusting relationships with our clients, we have a great concern with what Guardian describes it is doing with applicant data and the impact such practice can have on applicants, agencies and potentially the public safety background investigation industry as a whole.

Since the creation of Miller Mendel, Inc ("MMI") over ten years ago, our mission statement has included the following statement: "MMI places great pride in *straightforward and transparent operational practices* that foster a high level of respect and praise from our government clients." I hope it is clear from this letter, we continue to embrace our commitment to "straight forward and transparent operational practices." We hope you will join us in supporting legally sound, well thought out technology solutions for use in the pre-employment process at your public safety agency.

Please engage your risk management and legal counsel to independently review the content of this letter and make your own determinations as it relates to your agency's risk, compliance, and ability to maintain applicant trust and safety.

Sincerely,

Tyler J. Miller

Tyler Miller
President & CEO

Attachments

- Memo from Data Privacy and Security Attorney Emily Maass, Immix Law Group
- Guardian NAIC Screen Shot from Guardian Website
- State of Alaska Agreement with Guardian Alliance Technologies

Immix Law Group

MEMORANDUM

ATTORNEY: EMILY MAASS

DATE: NOVEMBER 3, 2020

CLIENT: MILLER MENDEL, INC.

SUBJECT: LEGAL COMPLIANCE AND RISK FACTORS FOR BACKGROUND INVESTIGATION SOFTWARE SYSTEMS FOR PUBLIC SAFETY AGENCIES

OVERVIEW

Miller Mendel, Inc. ("MMI") requested an updated review of privacy and data security legal compliance and best practices for background investigation software systems ("Background Software System") for public safety agency use. This memorandum provides an overview of the legal compliance and risk factors of using a Background Software System that shares personal information and other data collected from job applicants ("Applicant Data") as well as other problematic features or practices that may create legal risks for the public safety agencies that use those systems. Note that the legal considerations and risks discussed in this memorandum are not specific to any particular dispute or situation, and legal standards and advice may vary among matters depending on facts and circumstances in a given situation.[1]

Summary of Key Legal Considerations and Risks for Public Safety Agencies

Public safety agencies are responsible for ensuring that Applicant Data submitted to the agency for consideration for employment is collected and processed in accordance with federal, state, and local laws and kept secure from unauthorized access. Public safety agencies using a Background Software System services should be aware of, and should select a Background Software System that accounts for these key considerations:

- Methods to obtain applicant consent to collect and use Applicant Data.
- No unlawful sharing or sale of Applicant Data to third parties.
- Compliance with legal requirements for public agency privacy, security, and hiring practices.

Potential Background Software System Pitfalls and Risks for Public Safety Agencies

With a few exceptions for specific positions (e.g. sworn peace officers), public safety agencies are required to follow federal, state, and local laws and regulations related to employment matters and privacy rights, at all times, including when considering a job applicant.[2] These legal requirements apply whether the public safety agency interacts with applicants directly or through a third-party Background Software

[1] This memorandum is intended to provide MMI with general information on these topics. **Third parties should not rely on the information in this memorandum and should seek independent legal counsel with respect to these topics and any specific matter or dispute.**

[2] The laws and regulations employers have to consider and comply with include, but is not limited to, the Fair Credit Reporting Act, the Health Insurance Portability and Accountability Act, the California Consumer Privacy Act in California, the Oregon Job Applicant Fairness Act in Oregon, and other federal and state laws and regulations.

System. Using a Background Software System does not relieve a public safety agency of these statutory obligations and potential liability for violations, regardless of contractual agreements the public safety agency may have with the Background Software System company. The following provides an overview of potential pitfalls of using Background Software Systems with problematic features or practices and the subsequent legal risks for the public safety agencies that use them.

Shares Applicant Data Unlawfully or Inappropriately

Public safety agencies must be aware if the Background Software System shares Applicant Data in any manner. Some data sharing may be necessary for the Background Software System to function, but agencies will want to avoid Background Software Systems that share Applicant Data for any other purpose, or without offering the public safety agency ultimate discretion and control over what data is shared and with whom. Federal and some state laws restrict how Applicant Data may be shared or grant the applicant the right to instruct the prospective employer to stop sharing their Applicant Data. If an applicant instructs a public safety agency to stop sharing their Applicant Data, the agency must comply with the instruction and also ensure the Background Software System and other downstream recipients subsequently refrain from such sharing. Also, applicants must have the right (and a clear method) to revoke consent that may have been previously given.

Note, however, that if the Background Software System shares Applicant Data on its own accord, without instruction from the public safety agency subscribing to the software for recruiting purposes, then the agency will not know how widely the Applicant Data is shared or with whom. This practice exposes the public safety agency to significant legal risk. First, this practice by a Background Software System prevents the agency from confirming that the Applicant Data is not being shared in conflict with laws applicable to the agency. Without tracking or controlling sharing, a public safety agency's Applicant Data could be shared with any number or type of third parties without the agency's ability to ensure that the information is being shared in a lawful manner. Second, this practice prevents the public safety agency from meetings its legal obligation to instruct downstream recipients to stop sharing when an applicant instructs the agency to stop sharing their Applicant Data or due to other legal obligation requiring the applicant data to be removed from the Background Software System.

Additionally, many states require their public agencies to adhere to strict data security standards and protections[3]. If a public agency collects applicant data in accordance with those standards, but the public agency uses a Background Software System that inappropriately shares Applicant Data with third parties that do not meet those same data security standards, then the public agency is likely in violation of its data security obligations as required by law.

A Background Software System that engages in widespread sharing of Applicant Data significantly increases the likelihood that Applicant Data will be exposed as part of a data breach. All 50 states and Puerto Rico have data breach laws that set out legally required response and corrective actions following an unauthorized disclosure of protected data and, in some states (including Oregon), requirements to take action in regard to data shared with vendors and third parties.[4] In the event of a data breach, the public safety agency that originally collected the Applicant Data is responsible for complying with data breach law requirements such as notifying applicants, downstream data recipients, and taking remedial measures. Keep in mind the applicant only input their Applicant Data to the Background Software System because the public safety agency instructed the applicant to do so, and the Background Software System is therefore and extension of the agency's own pre-employment hiring activities. This means the public safety agency would be liable, and subject to fines, if an applicant is impacted by a data breach as a result of the Background Software System sharing their Applicant Data.

[3] RCW 43.105.215; ORS 276A.300; Calif. Govt. Code § 11549.3 et seq.; Tex. Govt. Code § 2054.0286

[4] *See* list available at https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

Sells or Commercializes Applicant Data

Privacy laws define "sale" very broadly, so that virtually any exchange of applicant data for a benefit could be deemed a sale. In general, if the company offering and licensing the Background Software System to the public safety agency benefits from sharing Applicant Data with third parties, sharing the applicant data may qualify as a "sale" of personal information under applicable privacy laws.[5] Where privacy laws restrict the sale of personal information, the public safety agency would be required to: (1) notify the individual that their personal information may be sold; (2) provide a method for individuals to opt-out of the sale; and (3) where an individual opts out, instruct the third party recipients to not resell the personal information. Additionally, if the Background Software System prejudices or aids in disqualifying applicants who opt-out of data sharing or selling pursuant to their applicable legal rights, they would violate privacy laws in certain jurisdictions and may give rise to other legal liability for the public safety agency.

A Background Software System that collects Applicant Data from a public agency's applicants and exchanges that data amongst other public agencies as a value-added service would likely qualify as a "sale" under this legal standard. Further, if a Background Software System collects Applicant Data from a Personal History Questionnaire as part of a free initial service and then shares that Applicant Data with a third party in exchange for a service fee, this transaction qualifies as a "sale" of personal information that exposes the public safety agency to significant legal compliance obligations under most applicable legal standards. In either case, the result is essentially a private company exploiting its access to Applicant Data collected by the public safety agency without the agency's agreement or control.

Public safety agencies should avoid using Background Software Systems that sell, license, rent, or commercialize Applicant Data in any manner to avoid inadvertently violating laws designed to protect applicants from the commercialization of their personal information. Keep in mind that applicants only submit their Applicant Data to the Background Software System because the public safety agency has directed them to do so in order to be considered for agency employment. For this reason, if a Background Software System engages in any practices that qualify as a "sale" of personal information, the public safety agency would be responsible for meeting these requirements, and also liable if the public safety agency uses a Background Software System that engages in unlawful sales of Applicant Data.

Inadequate Mechanisms to Provide Applicant Notice and Collect Applicant Consent

Federal and state privacy laws protect an individuals' right to control how their personal information is collected and used. Some privacy laws specifically require an employer to obtain the applicants' permission before collecting Applicant Data or putting it to use in certain ways.[6] Also, in many cases, the agency, whether directly or through Background Software System, may only use Applicant Data information as approved by the job applicant or may be required to permit an applicant to opt-out of using the Background Software System without disqualifying or other adverse impact the applicant from the recruitment process. These requirements vary among industries and from state to state.

With this in mind, it is essential that public safety agencies use a Background Software System with functionality to provide applicants with legally required notices about their privacy rights and the use of Applicant Data throughout the pre-employment hiring process, and a mechanism to collect the applicant's consent prior to collecting Applicant Data. Public safety agencies should review and confirm

[5] California and Nevada. Note that the CCPA has exceptions for employment related data and some government activities. However, where a Background Software System is selling the data, those exceptions may not apply, but this remains an open legal question.

[6] For example, the Fair Credit Reporting Act (FCRA) is a federal law that requires employers to give an applicant certain notice presented in a specific format and containing certain information before obtaining a pre-employment credit report. 15 U.S.C. § 1681 et seq. As an example from the state level, in California the employer must notify an applicant before a background check is conducted by an outside screening company (e.g. TransUnion, Experian, or Equifax) that: (a) states the purpose of the report; (b) gives the name, address, and telephone number of the screening company; (c) includes a summary of their rights to see and copy any report about the applicant; and (d) includes a box to check if the applicant wants a copy of the report.

the Background Software System: (1) has a clearly written privacy policy that explains to applicants in simple terms what information is being collected and why, and how the information collected is used or shared; (2) informs applicants about their privacy rights and how to exercise those rights; (3) provides equal service to all job applicants, even those that exercise their legal rights that may include opting out of using the Background Software System. Also, because notice and consent requirements vary among jurisdictions, the Background Software System should allow for a tailored workflow to meet the requirements specific to the public safety agency's jurisdiction and internal policies adopted by the agency's human resources and risk management authority.

Failure to consider these requirements and ensure that the public safety agency's use of a Background Software System complies could increase the public safety agency's risk of exposure to potential liability under federal and state privacy laws. Privacy law violations can result in steep regulatory fines, and in some cases, lawsuits from impacted individuals.

Does Not Meet Requirements Unique to Public Agencies

In addition to legal requirements applicable to employers generally, public agencies are often required to abide by special regulations for their recruiting and hiring activities. Specific requirements differ from state to state, and sometimes at the local level as well, but with the shared purpose and intent of ensuring a fair and transparent recruiting process, and preventing Applicant Data from being used for commercial purposes in the private marketplace for profit of a private company or being subject to a data breach.

Typical controls on public agencies include equal access to the job application process, limitations on the Applicant Data collected, prohibitions against sharing or selling Applicant Data to third parties, and specific requirements to collect, store, and transmit Applicant Data in a secure manner. For example, in Washington State, the courts have interpreted Article I, Section 7 as providing two rights of privacy to public employees: the right to nondisclosure of intimate personal information, and the right to personal autonomy.[7] Also, as of March 2019, Oregon and ten other states, along with roughly half a dozen cities, had each enacted a law prohibiting prospective employers from asking applicants to disclose their prior salary. Prior to the passage of these laws, public safety agencies in those jurisdictions asked applicants to disclose salary information in the Employment section of the Personal History Statement. Once these laws went into effect, public safety agencies were required to adjust the applicant user experience provided by the agency's Background Software System to comply with the new law.

Public safety agencies should keep in mind that a Background Software System used by a public safety agency is an extension of the agency itself. This means the public safety agency is responsible for due diligence in the selection and use of a Background Software System that meets the legal and regulatory requirements that apply to employers generally as well as uniquely to public safety agencies. If the Background Software System fails to meet these standards, the public safety agency faces liability for that failure. Background Software Systems that are not designed to meet this standard may increase the public safety agency's risk of facing costly litigation or and negative headlines.

As federal, state and local legislation changes across the United States, it is important that Background Software System that offer public safety agencies frontend user controls to tailor forms and processes to support compliance with legislative changes as well as changes to the agency's own internal policies, fiduciary duties, and ethics considerations that may come into play. If the Background Software System only offers "out of the box" features not tailorable to the public agency's needs, the public agency risks violating specific requirements and subsequently eroding the public and applicant's trust in the agency and public safety profession in general.

[7] *See, for example, Robinson v. City of Seattle*, 102 Wn. App. 795, 811, 10 P.2d 352 (2000).

Conclusions

Public safety agencies are held to strict standards to protect applicant privacy and ensure a fair and transparent recruiting process. It is essential that public safety agencies select a Background Software System that supports the agency's efforts to meet these standards and promotes applicant and public trust in the agency and its recruiting process. Public safety agencies need to be sure the Background Software System handles Applicant Data carefully, in any case with at least the same level of privacy, security, and confidentiality as the public safety agency would if the applicant submitted the information directly to the agency. At a minimum, a public safety agency should select a Background Software System with legal compliance mechanisms and safeguards built into the workflow, and options to customize the applicant's user experience and how and to what extent the Background Software System processes, stores, and shares the Applicant Data. A Background Software System that shares, commercializes or sells Applicant Data to third parties or otherwise fails to support a public safety agency's privacy and data security measures expose the public safety agency to a broad array of potential risks of legal noncompliance, regulatory violation, or private rights of action asserted by applicants.

In addition to the topics discussed in this memorandum, legal counsel for public safety agencies seeking a Background Software System to support recruiting and hiring processes should give consideration to how a given Background Software System might support the public safety agency's efforts with respect to legal implications of Applicant Data stored on the Background Software System once an applicant becomes an employee, interactions with labor unions, and how use of a Background Software System impacts the public safety agency's compliance with public records laws, civil services commission rules, and legal processes like subpoenas or discovery requests.

guardianalliancetechnologies.com

CENTRALIZED DATABASE OF APPLICANT INFO

Guardian's National Applicant Information Center (NAIC) provides agencies with a way to track answers that applicants have provided to other agencies using Guardian.

Each additional agency that utilizes Guardian enriches your national database.

Overview Video

STANDARD CONTRACT FORM
Goods and Non-Professional Services

The parties' contract comprises this Standard Contract Form, as well as its referenced Articles and their associated Appendices

1. Agency Contract Number	2. Contract Title	3. Agency Fund Code	4. Agency Appropriation Code
C127847	Recruitment Background Investigations Software	See Appendix D	See Appendix D

5. Vendor Number	6. IRIS Document ID #	7. Alaska Business License Number
VCO28988	**200000048**	**N/A**

This contract is between the State of Alaska,

8. Department of	Division	
Public Safety	**Support Services, Recruitment Unit**	hereafter the State, and

9. Contractor

Guardian Alliance Technologies hereafter the Contractor

POC: Ryan Layne, CEO **Phone:** (415) 655-2244 **Email:** ryan@guardianalliancetech.com

Mailing Address	Street or P.O. Box	City	State	ZIP Code
	11 S. San Joaquin St., #804	**Stockton**	**CA**	**95202**

10.

ARTICLE 1. Appendices: Appendices referred to in this contract and attached to it are considered part of it.

ARTICLE 2. Performance of Contract:

2.1 Appendix A (General Conditions), Items 1 through 18, governs contract performance.
2.2 Appendix B sets forth the liability and insurance provisions of this contract.
2.3 Appendix C sets forth the scope of work/services to be performed by the contractor.
2.4 Appendix D sets forth the structure of pricing and compensation between the State and contractor.
2.5 Appendix E (Guardian Master Agreement) is secondary to Appendix A, reflects contractor's terms and conditions in agreement with State statute

ARTICLE 3. Period of Performance: The period of performance for this contract begins July 18, 2019, and ends June 30, 2020.

ARTICLE 4. Considerations:

4.1 In full consideration of the contractor's performance under this contract, the State shall pay the contractor a sum not to exceed
$76,650.00 in accordance with the provisions of Appendix D.
4.2 When billing the State, the contractor shall refer to the Agency Contract Number and send the billing to:

11. Department of	Attention: Division of
Public Safety	**Support Services/Recruitment Unit**
Mailing Address	Attention:
5700 E. Tudor Rd. Anchorage, AK 99507	**Lt. Derek DeGraaf**

12. CONTRACTOR	13. CONTRACTING AGENCY
Name of Firm **Guardian Alliance Technologies**	Department/Division **Public Safety/Administrative Services**
Signature of Authorized Representative	Signature of Procurement Officer Kelly Pahlau
Typed or Printed Name of Authorized Representative **Ryan Layne**	Typed or Printed Name of Procurement Officer **Kelly Pahlau, Procurement Specialist II**
Date **Friday July 19, 2019**	Date 07/22/2019

APPENDIX A
GENERAL CONDITIONS

1. **Inspections and Reports:**
The department may inspect, in the manner and at reasonable times it considers appropriate, all of the contractor's facilities and activities under this contract. The contractor shall make progress and other reports in the manner and at the times the department reasonably requires.

2. **Suitable Materials, Etc.:**
Unless otherwise specified, all materials, supplies or equipment offered by the contractor shall be new, unused, and of the latest edition, version, model or crop and of recent manufacture.

3. **Disputes:**
If the contractor has a claim arising in connection with the contract that it cannot resolve with the State by mutual agreement, it shall pursue the claim, if at all, in accordance with the provisions of AS 36.30.620-AS 36.30.632 IRRELEVANT

4. **Default: (Reserved)**

5. **No Assignment or Delegation:**
The contractor may not assign or delegate this contract, or any part of it, or any right to any of the money to be paid under it, except with the written consent of the Procurement Officer.

6. **No Additional Work or Material:**
No claim for additional supplies or services, not specifically provided in this contract, performed or furnished by the contractor, will be allowed, nor may the contractor do any work or furnish any material not covered by the contract unless the work or material is ordered in writing by the Procurement Officer.

7. **Independent Contractor:**
The contractor and any agents and employees of the contractor act in an independent capacity and are not officers or employees or agents of the State in the performance of this contract.

8. **Payment of Taxes:**
As a condition of performance of this contract, the contractor shall pay all federal, State, and local taxes incurred by the contractor and shall require their payment by any subcontractor or any other persons in the performance of this contract. Satisfactory performance of this paragraph is a condition precedent to payment by the State under this contract.

9. **Compliance:**
In the performance of this contract, the contractor must comply with all applicable federal, state, and borough regulations, codes, and laws, and be liable for all required insurance, licenses, permits and bonds.

10. **Conflicting Provisions:**
Unless specifically amended and approved by the Department of Law, the terms of this contract supersede any provisions the contractor may seek to add. The contractor may not add additional or different terms to this contract; AS 45.02.207(b)(1). The contractor specifically acknowledges and agrees that, among other things, provisions in any documents it sees to append hereto that purport to (1) waive the State of Alaska's sovereign immunity, (2) impose indemnification obligations on the State of Alaska, or (3) seek to limit liability of the contractor for acts of contractor negligence, are expressly superseded by this contract and are void.

11. **Officials Not to Benefit:**
Contractor must comply with all applicable federal or State laws regulating ethical conduct of public officers and employees.

12. **Contract Prices:**
Contract prices for commodities must be in U.S. funds and include applicable federal duty, brokerage fees, packaging, and transportation cost to the FOB point so that upon transfer of title the commodity can be utilized without further cost. Prices for services must be in U.S. funds and include applicable federal duty, brokerage fee, packaging, and transportation cost so that the services can be provided without further cost.

13. **Contract Funding:**
Contractors are advised that funds are available for the initial purchase and/or the first term of the contract. Payment and performance obligations for succeeding purchases and/or additional terms of the contract are subject to the availability and appropriation of funds. In the event of failure to appropriate or a lack of availability of funds, the State will provide the contractor with 30 days' notice prior to termination.

14. **Force Majeure:**
The parties to this contract are not liable for the consequences of any failure to perform, or default in performing, any of their obligations under this Agreement, if that failure or default is caused by any unforeseeable Force Majeure, beyond the control of, and without the fault or negligence of, the respective party. For the purposes of this Agreement, Force Majeure will mean war (whether declared or not); revolution; invasion; insurrection; riot; civil commotion; sabotage; military or usurped power; lightning; explosion; fire; storm; drought; flood; earthquake; epidemic; quarantine; strikes; acts or restraints of governmental authorities affecting the project or directly or indirectly prohibiting or restricting the furnishing or use of materials or labor required; inability to secure materials, machinery, equipment or labor because of priority, allocation or other regulations of any governmental authorities.

15. **Contract Extension:**
Unless otherwise provided, the State and the contractor agree: (1) that any holding over of the contract excluding any exercised renewal options, will be considered as a month-to-month extension, and all other terms and conditions shall remain in full force and effect, and (2) to provide written notice to the other party of the intent to cancel such month-to-month extension at least thirty (30) days before the desired date of cancellation.

16. **Severability:**

If any provision of the contract is declared by a court to be illegal or in conflict with any law, the validity of the remaining terms and provisions will not be affected; and, the rights and obligations of the parties will be construed and enforced as if the contract did not contain the particular provision held to be invalid.

17. Continuing Obligation of Contractor:
Notwithstanding the expiration date of this contract, the contractor is obligated to fulfill its responsibilities until warranty, guarantee, maintenance and parts availability requirements have completely expired.

18. Governing Law; Forum Selection
This contract is governed by the laws of the State of Alaska. To the extent not otherwise governed by Article 3 of this Appendix, any claim concerning this contract shall be brought only in the Superior Court of the State of Alaska and not elsewhere.

APPENDIX B[1]
INDEMNITY AND INSURANCE

Article 1. Indemnification

The Contractor shall indemnify, hold harmless, and defend the contracting agency from and against any claim of, or liability for error, omission or negligent act of the Contractor under this agreement. The Contractor shall not be required to indemnify the contracting agency for a claim of, or liability for, the independent negligence of the contracting agency. If there is a claim of, or liability for, the joint negligent error or omission of the Contractor and the independent negligence of the Contracting agency, the indemnification and hold harmless obligation shall be apportioned on a comparative fault basis. “Contractor” and “Contracting agency”, as used within this and the following article, include the employees, agents and other contractors who are directly responsible, respectively, to each. The term “independent negligence” is negligence other than in the Contracting agency’s selection, administration, monitoring, or controlling of the Contractor and in approving or accepting the Contractor’s work.

Article 2. Insurance

Without limiting contractor's indemnification, it is agreed that contractor shall purchase at its own expense and maintain in force at all times during the performance of services under this agreement the following policies of insurance. Where specific limits are shown, it is understood that they shall be the minimum acceptable limits. If the contractor's policy contains higher limits, the state shall be entitled to coverage to the extent of such higher limits. Certificates of Insurance must be furnished to the contracting officer prior to beginning work and must provide for a notice of cancellation, non-renewal, or material change of conditions in accordance with policy provisions. Failure to furnish satisfactory evidence of insurance or lapse of the policy is a material breach of this contract and shall be grounds for termination of the contractor's services. All insurance policies shall comply with and be issued by insurers licensed to transact the business of insurance under AS 21.

2.1 Workers' Compensation Insurance: The Contractor shall provide and maintain, for all employees engaged in work under this contract, coverage as required by AS 23.30.045, and; where applicable, any other statutory obligations including but not limited to Federal U.S.L. & H. and Jones Act requirements. The policy must waive subrogation against the State.

2.2 Commercial General Liability Insurance: covering all business premises and operations used by the Contractor in the performance of services under this agreement with minimum coverage limits of $300,000 combined single limit per claim.

APPENDIX C
SCOPE OF WORK

1. Purpose
The purpose of this contract is for the Contractor to provide a comprehensive software solution that integrates with NEOGOV; it will allow the DPS Recruitment unit to conduct background investigations for Trooper, Court Service Officer, and Deputy Fire Marshal applicants from beginning to end, on one digital cloud-based platform.

The State of Alaska, Department of Public Safety (DPS) will use these to accomplish the following: Allow DPS Recruitment Unit to e-mail a link to a digital portal, so that an applicant can apply online and submit waivers and documents. Then, DPS Recruitment Staff can assign the digital file to a Background Investigator for investigation within the software suite.

2. Order of Precedence
The order of precedence for the contract between the Contractor and DPS is established by the order of the following documents:

1. Any amendment to the executed contract with the more recent amendment taking precedence over a less recent amendment.
2. The “Standard Contract Form Goods and Non-Professional Services and Appendices”.
3. The Contractor’s quote
4. The Contractor’s Master Agreement terms and conditions

The above numbered documents are, collectively, the “contract.” In the case of any conflict or inconsistency arising under the contract documents, a document identified with a lower number in this subsection shall supersede a higher numbered document to the extent necessary to resolve any such conflict or inconsistency. No conflict or inconsistency shall be deemed to occur in the event an issue is addressed in one of the above-mentioned contract documents but is not addressed in another of such documents.

Where terms and conditions specified in the Contractor's quote differ from the terms and conditions in contract documents 2, as identified above in section 2 Order of Precedence, the terms and conditions of documents 2 shall apply. Where terms and conditions specified in the Contractor’s quote supplement the terms and conditions in contract documents 2, as identified above in section 2 Order of Precedence, the supplemental terms and conditions shall apply only if specifically accepted by the Procurement Officer in writing.

3. Contractor Performance and Deliverables
The Contractor shall perform the scope of work, provide the deliverables, and meet any delivery and completion dates outlined below:

Provide cloud based, software services, with an anticipated usage of about 365 background investigations per year. As part of this contract, the contractor will provide technical support, unlimited users within DPS, and will maintain CJIS compliance.

The Contractor shall perform the tasks, services, and deliverables set forth within this Scope of Work to DPS’s satisfaction. The Contractor shall be responsible for all communications regarding the progress of performance of the contract and shall discuss with DPS any issues, recommendations, and decisions related to the contract. The Contractor shall be the sole point of contact on all matters related to the performance of the contract.

DPS Project Manager
The DPS Project Manager is responsible for monitoring the operations and performance of the Contractor for contract compliance, and to coordinate actions and communications between DPS and the Contractor. The DPS Project Manager for this contract is:

Attn: Lt. Derek DeGraaf, DPS Recruitment Unit
5700 E. Tudor Road
Anchorage, Alaska 99507
Phone: 907-269-5759
E-mail: derek.degraaf@alaska.gov

4. Remedial Action
In addition to any remedies available to DPS under law or equity, DPS at its sole discretion may require one or more of the following remedial actions if the Contractor fails to cure findings of breach, or as otherwise provided for herein:

- DPS may take reasonable steps to provide for such cure and may offset the costs of such cure against the contract pricing in effect at the time of occurrence of a breach.
- Reduce and/or offset payment to reflect the reduced value of goods or services received.
- Withhold payment or require payment of actual damages caused by a breach.
- Terminate the contract pursuant to section 5 Termination.

Withholding of payment by DPS for the failure of the Contractor to perform shall not relieve the Contractor from its obligations under the contract.

5. Termination
Termination for Cause
The occurrence of any of the following events shall be an event of default under the contract and cause for termination:

- A material breach of any term or condition of the contract.
- Any representation or warranty by Contractor in its quote that proves to be untrue or materially misleading.
- Any default or non-compliance as otherwise specified in the contract.

DPS may terminate the contract if DPS provides the Contractor written notice of default and the Contractor has failed to cure the default within 30 calendar days. If DPS terminates the contract for default, DPS reserves the right to take any action it may deem necessary including, without limitation:

- Exercise any remedy provided by law or equity.
- Withhold payment until the default is remedied.
- Offset of damages against payment due.

Termination for Convenience

DPS may terminate the contract at its convenience, in whole or in part, by providing the Contractor written notice 30 calendar days prior to termination of the contract.

If DPS terminates the contract for convenience, DPS is liable only for payment in accordance with the payment provisions of this contract for goods or services provided before the effective date of termination.

The Project Director, by written notice, may terminate this contract, in whole or in part, when it is in the best interest of the State. In the absence of a breach of contract by the contractor, the State is liable only for payment in accordance with the payment provisions of this contract for services rendered before the effective date of termination.

Effect of Termination

Upon termination by DPS, the Contractor shall:

- Stop work as directed by DPS. Place no further orders or requests of subcontractors, if any, for goods or services;
- Take actions necessary, or that DPS may direct, for the protection and preservation of the goods or services;
- Terminate all orders and subcontracts to the extent that they relate to the performance of work terminated by the termination notice;
- Deliver or otherwise make available to DPS all data, reports, estimates, confidential information, summaries and such other information and materials, as may have been accumulated by the Contractor in performing the contract, whether completed or in process.

END OF APPENDIX C SCOPE OF WORK

APPENDIX D
COMPENSATION

The Contractor will be compensated for goods or services rendered to the State of Alaska, Department of Public Safety (DPS) in accordance with the contract terms and conditions, and as follows:

1. Unless otherwise stated in this contract, price adjustments will not be allowed during the renewal process. The price for this contract will remain firm and not fluctuate for the entire term of the contract, to include any and all renewals or extensions. Any request for an adjustment to the time, scope, or cost of the contract that will impact the pricing will only be considered at the Contractor's written request based on justification through sufficient supporting documentation and is subject to approval based upon legislative or department appropriations.

2. The period of performance for the initial contract term shall begin on the Service Commencement Date of 07/18/2019 and expire on 06/30/2020.

3. This contract includes the following renewal options, to be exercised solely at the discretion of the State.

Renewal Option #1	07/01/2020	through	06/30/2021
Renewal Option #2	07/01/2021	through	06/30/2022
Renewal Option #3	07/01/2022	through	06/30/2023
Renewal Option #4	07/01/2023	through	06/30/2024

The State will not be responsible for payment of goods or services rendered outside the valid term of this contract, there will be no exceptions.

4. If a renewal option is not exercised by DPS, the contract shall be considered expired on the expiration date noted above and does not require notification of such by DPS. All exercised renewal options shall be executed via written amendment to the contract. DPS may enter into a month-to-month holdover extension, prior to the expiration of the current contract term. All exercised month-to-month holdover extensions shall be executed via written amendment to the contract. DPS will provide the Contractor written notice 30 calendar days prior to cancellation of any month-to-month holdover extension. The total cumulative dollar amount of each month-to-month holdover extension shall not exceed the unanticipated amendment limitations stated in Alaska Administrative Manual 81.700. All other terms and conditions specified by the contract shall remain the same during any month-to-month holdover extension period.

5. The compensation for the entire duration of the contract, including all renewal option periods, shall not exceed $76,650.00. The compensation for the initial contract term and each renewal option year shall not exceed the dollar amounts identified below:

Initial Contract Term = $15,330.00
Renewal Option #1 = $15,330.00
Renewal Option #2 = $15,330.00
Renewal Option #3 = $15,330.00
Renewal Option #4 = $15,330.00

The price for goods or services shall be based on the Contractor's quote dated 05/14/2019.

6. The Contractor shall submit a properly documented invoice monthly to DPS. Payment to the Contractor is contingent upon the Contractor delivering a properly documented invoice, no later than 30 days after the completion of a deliverable, to DPS and after DPS confirms receipt of goods or services. DPS retains the right to request additional justification and/or documentation as it deems necessary to ensure appropriate payment of the invoice.

Every invoice shall include the following information:

- Contract # 127847;
- Identification of the billing period;
- An itemized listing of deliverables and charges for the invoiced period;
- Total amount billed;
- Date invoice was submitted for payment;
- Entity name, contact information, and Alaska vendor number.

Contractor shall send invoices to:

Attn: Lt. Derek DeGraaf
5700 E. Tudor Road
Anchorage, Alaska 99507
Phone: (907) 269-5979
E-mail: dps.recruit@alaska.gov

Questions concerning payment must be addressed to the DPS point of contact identified above.

7. Final invoices must be received by DPS no later than 30 days following the termination or expiration date of the contract.

8. The State is not responsible for and will not pay local, State, or federal taxes. All costs associated with the contract must be stated in U.S. currency.

9. The State is a government entity and it is understood and agreed that the State's payments herein provided for may be paid from Alaska State Legislative appropriations; and approval or continuation of a contract is contingent upon Legislative appropriation. The State reserves the right to terminate the contract in whole or part if, in its sole judgment, the Legislature of the State of Alaska fails, neglects, or refuses to appropriate sufficient funds as may be required for the State to continue such payments; or if the Executive Branch mandates any cuts or holdbacks in spending, or if funds are not budgeted or otherwise available. Further, in the event of non-appropriation, the State shall not be liable for any penalty, expense, or liability; or for general, special, incidental, consequential, or other damages resulting therefrom.

<u>For State use only:</u>
Fund: 1004
Unit: 6540
Object: 3032
Appropriation Unit: 122701000

END OF APPENDIX D COMPENSATION

Exhibit A
Guardian Master Agreement

1. DEFINITIONS.

1.1 "**Customer Data**" means any data, information or material submitted or uploaded by Customer or during its usage of the Services. Customer Data is and shall at all times be owned by Customer.

1.2 "**Services**" means access to and use of Guardian's software system by a specific and limited number of Customer employees as set forth in Exhibit A hereto, including all updates, bug fixes, error corrections or other minor enhancements or improvements thereto.

2. SERVICES. Subject to the terms and conditions of this Agreement, Guardian hereby agrees to provide Customer with the Services. Guardian shall use its reasonable efforts to make the Services available online within one business day following the execution of this Agreement. Customer's use of the Services is subject to any restrictions indicated in Exhibit A.

3. LICENSE GRANT.

3.1 Access and Use Of Customer Data By Guardian. Subject to the terms and conditions of this Agreement, Customer hereby grants to Guardian perpetual, non-exclusive, irrevocable, non-terminable, non-transferable (except as permitted by Section 17 below) permission to access Customer Data in connection with the development, offering and delivery of Guardian's products and services solely to the extent that Guardian does not disclose or otherwise reveal Customer Data to any third parties.

4. SERVICE LEVELS. Guardian hereby agrees to provide the Services in accordance with the Service Level Objectives on Exhibit B.

5. LICENSE RESTRICTIONS. Customer shall not, directly or indirectly, do any of the following: (i) reverse engineer, decompile, disassemble or otherwise attempt to discover the source code or underlying ideas or algorithms of the Services; (ii) modify or create derivative works (as defined under U.S. Copyright laws) based on the Services or any related documentation; (iii) rent, lease, distribute, sell, resell, assign, or otherwise transfer its rights to use the Services; (iv) use the Services for the benefit of any third party; (v) remove any proprietary notices from the Services or any other Guardian materials furnished or made available hereunder; (vi) publish or disclose to third parties any evaluation of the Services without Guardian's prior written consent; (vii) use the Services to develop a database, online or similar database service, or other information resource of any kind (print, electronic or otherwise) for sale to, distribution to, display to or use by others or otherwise create or attempt to create a substitute or similar service or product through use of or access to any of the Services or proprietary information related thereto; (viii) store in a retrieval system accessible to the public, transfer, publish, distribute, display to others, broadcast, sell or sublicense the Services, or any portion thereof; or (ix) pre-fetch, "crawl," "spider," or in any non-transitory manner store or cache any information obtain from the Services (including results or any part or copy or derivative thereof), except that Customer may store data provided by the Services for internal use so long as such storage is done in compliance with all applicable security requirements pertinent to Customer.

6. SECURITY.

6.1 Customer Account. Customer is entirely responsible for all activities that occur under Customer's account and all charges incurred from use of the Services accessed with Customer's login information. Customer agrees to immediately notify Guardian of any unauthorized use of Customer's account or any other breach of security known to Customer.

Guardian shall have no liability for any loss or damage arising from Customer's failure to comply with these requirements.

6.2 Security. Guardian agrees, pursuant to the FBI Criminal Justice Information Services Security Addendum, as set forth in Exhibit C hereto, to maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB). Customer acknowledges that, notwithstanding such security precautions, use of, or connection to, the Internet provides the opportunity for unauthorized third parties to circumvent such precautions and illegally gain access to the Services and Customer Data. Accordingly, Guardian cannot and does not guarantee the privacy, security, integrity or authenticity of any information so transmitted over or stored in any system connected to the Internet or that any such security precautions will be adequate or sufficient.

7. CUSTOMER SUPPORT. Except as expressly stated on Exhibit A, the Fees include the provision to Customer of Guardian's then-current standard telephone and e-mail support.

8. OWNERSHIP. Customer acknowledges that, as between Guardian and Customer, all right, title and interest in the Services, the results of the Services and all other Guardian materials furnished or made available hereunder, and all derivatives, modifications and enhancements thereof, including all rights under copyright and patent and other intellectual property rights, belong to and are retained solely by Guardian or Guardian's licensors and providers, as applicable. There are no implied rights. All rights not expressly granted by Guardian to Customer are reserved by Guardian. Guardian hereby grants Customer a perpetual, irrevocable license to use the deliverables of Services for its business purposes.

9. CUSTOMER OBLIGATIONS.

9.1 Hardware. As between the parties, Customer is responsible for obtaining and maintaining all computer hardware, software and communications equipment needed to access and use the Services, and for paying all third-party fees and access charges (e.g., ISP, telecommunications, bandwidth, hosting, etc.) incurred while using the Services.

9.2 Customer Data. Customer represents and warrants that it is and will continue to be in compliance with all applicable privacy and data protection laws and regulations with respect to any Customer Data. Customer shall be solely responsible for (i) the accuracy and completeness of all records, databases, data and information provided, submitted or uploaded by Customer or its authorized end users in connection with this Agreement or use of the Services.

9.3 Conduct. Customer is solely responsible for its actions and the actions of its employees using the Services. Customer acknowledges and agrees that (1) Customer is responsible for selecting appropriate remediation for, and resolving, any issues found on Customer's network or in Customer's web traffic through the Services; and (2) Guardian is not liable for, or responsible to, remediate any issues found on Customer's network or in Customer's web traffic through the Services. Customer agrees: (a) to abide by all local, state, national, and international laws and regulations applicable to Customer's use of the Services; (b) not to send or store data on or to the Services which violates the rights of any individual or entity established in any jurisdiction; (c) not to use the Services for illegal, fraudulent, unethical or inappropriate purposes; (d) not to interfere or disrupt networks connected to the Services or interfere with other ability to access or use the Services; and (e) not to transmit or post any material that encourages conduct that could constitute a criminal offense or give rise to civil liability; Customer acknowledges and agrees that Guardian neither endorses the contents of

any Customer communications or Customer Data or other Customer content nor assumes any responsibility for any infringement of third party intellectual property rights arising therefrom or any crime facilitated thereby.

9.4 Acceptable Use. Customer shall not: (i) provide system passwords or other log-in information for the Services to any third party except those specifically authorized to access the Services in this Agreement; (ii) share non-public Guardian system features or content with any third party; (iii) access the Services in order to build, assist, or facilitate the assembly of a competitive product or service, to build a product using similar ideas, features, functions or graphics of the Services, or to copy any ideas, features, functions or graphics of the Services; (iv) reverse engineer, decompile, disassemble or otherwise attempt to discover or directly access the source code or any underlying ideas or algorithms of any portions of the Services or any underlying software or component thereof; or (v) modify, create derivative works from, distribute, publicly display, publicly perform, or sublicense the Services except as expressly permitted by this Agreement. In the event that Guardian suspects any breach of the requirements provided in this Section 2(c), including by way of users of Customer's system, Guardian may suspend Customer's access to the Services for the reasonable time required to confirm or deny suspicion, in addition to other lawful remedies as required.

10. FEES AND TAXES; PAYMENT

10.1 Fees and Payment. Customer agrees to pay the fees set forth on Exhibit A ("**Fees**"). The Fees are quoted and payable in United States dollars. The Fees are non-refundable.

10.2 Payments. Customer shall pay all sums due under this Agreement in accordance with agreed payment terms. If Customer fails to pay a license or other fee within thirty (30) days of the due date, Guardian may suspend or terminate Customer's access to the Services and this Agreement immediately upon written notice, in addition to pursuing any other legal remedies available under this Agreement, at law or in equity.

11. TERM. This Agreement commences on the Effective Date and, unless terminated sooner in accordance with this Agreement, continues for the period set forth on Exhibit A. Customer is responsible for all Fees for the applicable term in which termination occurs. Guardian will not issue any refunds except in the case of termination pursuant to Section 12.1 or 12.2 herein. In the event that Guardian terminates this Agreement under Section 12.1 or 12.2 herein, Guardian shall provide Customer with a refund of the fees paid for any unexpired portion of the contract Term.

12. TERMINATION.

12.1 Breach. A party may terminate this Agreement upon written notice if the other party materially breaches this Agreement and does not cure the breach within 30 days of receipt of notice from the non-breaching party specifying the breach, except that the cure period for non-payment is ten days.

12.2 Convenience. (Reserved)

12.3 Failure to Pay/Customer Conduct. Guardian may suspend or terminate access to the Services, at its sole option, with or without notice to Customer if: (i) any payment is delinquent by more than thirty (30) days, or (ii) Customer breaches Section 9.2 or 9.3 of this Agreement.

12.4 Effect of Termination. Guardian will not be liable to Customer or any third party for suspension or termination of Customer's access to, or right to use, the Services under this Agreement. If Customer or Guardian terminates this Agreement, Customer will be obligated to pay the balance due for the Services, if any. Upon the effective date of expiration or termination of this Agreement for any reason, whether by Customer or Guardian, Customer's right to use the Services will immediately cease. Upon the expiration or termination of this Agreement, Customer access to the Services will terminate and Customer shall cease accessing and using the Services immediately. The definitions, rights, duties and obligation of the parties that by their nature continue and survive, including, without limitation, the payment, confidentiality and indemnity obligations and warranty disclaimer, and the ownership terms and the limitations on liability and consequential damages waiver and the license to the Customer Data, will survive its expiration or termination for any reason. Guardian will retain Customer Data for a period of at least 30 days after expiration or termination of this Agreement. Customer may request that Guardian conduct a mass export of Customer's Customer Data files and the database, and Guardian agrees to conduct the requested mass export at no cost to Customer. After 30 days, Guardian may delete and destroy all of Customer Data without notice or any liability to Customer.

12.5 Non-exclusive Remedy. Termination or expiration of this Agreement, in part or in whole, shall not limit either party from pursuing other remedies available to it, nor shall either party be relieved of its obligation to pay all fees that are due and owing under this Agreement through the effective date of termination. Neither party shall be liable to the other for any damages resulting solely from termination as permitted herein.

13. CONFIDENTIALITY.

13.1 Obligations. Each of the parties agrees to maintain in confidence any non-public information of the other party, whether written or otherwise, disclosed by the other party in the course of performance of this Agreement that a party knows or reasonably should know is considered confidential by the disclosing party ("**Confidential Information**"). The Confidential Information disclosed by a party constitutes the confidential and proprietary information of the disclosing party and the receiving party agrees to treat all Confidential Information of the other in the same manner as it treats its own similar proprietary information, but in no case will the degree of care be less than reasonable care. The receiving party shall use Confidential Information of the disclosing party only in performing under this Agreement and shall retain the Confidential Information in confidence and not disclose to any third party (except as authorized under this Agreement) without the disclosing party's express written consent. The receiving party shall disclose the disclosing party's Confidential Information only to those employees and contractors of the receiving party who have a need to know such information for the purposes of this Agreement, and those employees and contractors must have entered into written agreements with the receiving party containing confidentiality provisions covering the Confidential Information with terms and conditions at least as restrictive as those set forth herein.

13.2 Exclusions and Exceptions. Notwithstanding the foregoing, each party's confidentiality obligations hereunder do not apply to information that: (i) is already known to the receiving party prior to disclosure by the disclosing party; (ii) becomes publicly available without fault of the receiving party; (iii) is rightfully obtained by the receiving party from a third party

without restriction as to disclosure; (iv) is approved for release by written authorization of the disclosing party; or (v) is developed independently by the receiving party without use of, or reference to, the disclosing party's Confidential Information. The receiving party may disclose the disclosing party's Confidential Information pursuant to the requirements of a governmental agency or by operation of law, on condition that it gives the disclosing party reasonable prior written notice sufficient to permit the disclosing party to contest such disclosure and reasonably cooperates with the disclosing party in preventing or limiting the disclosure.

13.3 Terms of Agreement. (Reserved)

13.4 Destruction or Return of Confidential Information. Upon expiration or termination of this Agreement for any reason, each party shall promptly return to the other party, or destroy, as the parties agree, all copies of the other party's Confidential Information. All copies, notes or other derivative material relating to the Confidential Information shall be promptly retrieved or destroyed, as agreed, and no such material shall be retained or used by the receiving party in any form or for any reason.

14. WARRANTY.

14.1 Limited Warranty. Guardian warrants to Customer that the Services will perform substantially in accordance with the Service Level Agreement set forth on Exhibit B under normal use and circumstances. Customer's sole remedy, and entire liability of Guardian, for breach of the foregoing limited warranty is the remedy on Exhibit B. This limited warranty does not apply to any Services, or portion thereof, that is modified by any party other than Guardian, its agents or as authorized by Guardian in writing or that has been subjected to commercially unreasonable stress or conditions. Both parties understand that software and the Internet have inherent limitations. Customer has sole responsibility for the adequate protection and maintenance of hardware equipment used with the Services.

14.2 Warranty Disclaimer. EXCEPT AS EXPRESSLY WARRANTED IN SECTION 14.1, THERE ARE NO WARRANTIES OR CONDITIONS (WHETHER EXPRESS, STATUTORY, IMPLIED OR OTHERWISE ARISING IN LAW OR FROM A COURSE OF DEALING OR USAGE OF TRADE) FOR THE SERVICES OR SUPPORT. GUARDIAN EXPRESSLY DISCLAIMS AND EXCLUDES ALL WARRANTIES AND CONDITIONS, WHETHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY, MERCHANTABLE QUALITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OF THIRD PARTY RIGHTS. GUARDIAN DOES NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE SERVICES WILL MEET CUSTOMER'S NEEDS OR REQUIREMENTS OR THAT THE OPERATION OF THE SERVICES WILL BE UNINTERRUPTED OR ERROR-FREE OR THAT THE SERVICES WILL BE ALWAYS AVAILABLE OR AVAILABLE AT ANY PARTICULAR TIME OR THAT THE SERVICES WILL IDENTIFY ALL VIRUSES OR MALWARE OR THAT THE SERVICES WILL NOT OCCASIONALLY MAKE AN ERRONEOUS REPORT.

15. INDEMNIFICATION.

15.1 By Guardian. In addition to its indemnification obligations set forth in Appendix B, Guardian shall indemnify, defend or, at its option, settle any third-party claim, suit or proceeding against Customer to the extent based on a claim that the Services (excluding any Third Party Software) infringes any United States patent, copyright, trademark or trade secret and Guardian shall pay any final judgment entered against Customer in any claim, suit or proceeding or agreed to in settlement. Customer will notify Guardian in writing of the claim, suit or proceeding and give all information and assistance reasonably requested by Guardian or its designee. If use of the Services is enjoined, Guardian may, at its option, do one or more of the

following: (i) procure for Customer the right to use the Services, (ii) replace the Services with other suitable services or products, or (iii) refund the unearned prepaid portion of the Fees paid by Customer for the Services or the affected part thereof. Guardian will have no liability under this Section 15.1 to the extent a claim or suit is based upon (a) use of the Services in combination with software or hardware not provided by Guardian if infringement would have been avoided in the absence of the combination, (b) modifications to the Services not made by Guardian, if infringement would have been avoided by the absence of the modifications, or (c) use of any version other than a current release of the Services, if infringement would have been avoided by use of a current release. THIS SECTION 15.1 STATES GUARDIAN'S ENTIRE LIABILITY AND CUSTOMER'S SOLE AND EXCLUSIVE REMEDY FOR INTELLECTUAL PROPERTY INFRINGEMENT OR MISAPPROPRIATION CLAIMS.

16. LIMITATION OF LIABILITY.

16.1 Limitation on Direct Damages. EXCEPT AS SET FORTH IN APPENDIX B, IN NO EVENT SHALL GUARDIAN'S AGGREGATE LIABILITY, IF ANY, ARISING OUT OF OR IN ANY WAY RELATED TO THIS AGREEMENT EXCEED THE AMOUNTS PAID TO Guardian UNDER THIS AGREEMENT, WITHOUT REGARD TO WHETHER SUCH CLAIM IS BASED IN CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY OR OTHERWISE AND NOTWITHSTANDING ANY FAILURE OF THE ESSENTIAL PURPOSE OF THIS AGREEMENT OR ANY LIMITED REMEDY HEREUNDER. IN NO EVENT WILL GUARDIAN'S AFFILIATES, LICENSORS OR PROVIDERS BE LIABLE FOR ANY DIRECT DAMAGES OF ANY KIND.

16.2 Waiver of Consequential Damages. EXCEPT AS SET FORTH IN APPENDIX B, IN NO EVENT SHALL GUARDIAN OR ITS AFFILIATES, LICENSORS OR SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, PUNITIVE OR CONSEQUENTIAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOSS OF DATA OR LOSS OF PROFITS, WITHOUT REGARD TO WHETHER SUCH CLAIM IS BASED IN CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY OR OTHERWISE, EVEN IF GUARDIAN HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES AND NOTWITHSTANDING ANY FAILURE OF THE ESSENTIAL PURPOSE OF THIS AGREEMENT OR ANY LIMITED REMEDY HEREUNDER.

16.3 Essential Purpose. The essential purpose of this Section 16 is to limit the potential liability of the parties arising under this Agreement. The parties acknowledge that the limitations set forth in this Section 16 are integral to the amount of consideration levied in connection with the license of the Services and that, were Guardian to assume any further liability, such consideration would out of necessity, been set much higher.

17. NOTICES. All notices to a party shall be in writing and sent to the addresses specified above or such other address as a party notifies the other party, and shall be deemed to have been duly given when received, if personally delivered; when receipt is electronically confirmed, if transmitted by email; the day after it is sent, if sent for next day delivery by recognized overnight delivery service; and upon receipt, if sent by certified or registered mail, return receipt requested.

18. INDEPENDENT CONTRACTORS. Customer and Guardian are independent contractors and neither party is the legal representative, agent, joint venturer, partner, franchisor, franchisee or employee of the other party for any purpose whatsoever. Neither party has any right or authority to assume or create any obligations of any kind or to make any representation or warranty on behalf of the other party, whether express or implied, or to bind the other party in any respect whatsoever.

19. REFERENCES. All indices, titles, subject headings, section titles and similar items contained in this Agreement are provided for the purpose of reference and convenience only and are not intended to be inclusive, definitive or to affect the meaning, content or scope of this Agreement.

20. COUNTERPARTS. This Agreement may be executed in any number of counterparts, and each executed counterpart shall have the same force and effect as an original instrument.

21. ASSIGNMENT. Neither party shall assign its rights under this Agreement nor delegate any performance (other than the right to receive payments) without the other party's prior written consent, except that a party may, without the other party's consent, assign this Agreement to an affiliate or pursuant to a corporate reorganization, merger, acquisition or sale of all or substantially all of its assets to which this Agreement relates. Any attempted assignment or delegation in violation of the foregoing is void. Subject to the foregoing, this Agreement will bind and inure to the benefit of the parties and their respective successors and permitted assigns.

22. JURISDICTION. (Reserved

23. REASONABLE CONTROL. Except with respect to payment obligations, neither party is liable for any failure of performance or equipment due to causes beyond its reasonable control, including, but not limited to, the following: (i) acts of God, fire, flood, earthquake, tsunami, storm, or other catastrophes; (ii) any law, order, regulation, direction, action, or request of any governmental entity or agency, or any civil or military authority; (iii) national emergencies, insurrections, riots, wars or acts of terrorism; (iv) unavailability of rights-of-way or materials; or (v) strikes, lock-outs, work stoppages, or other labor difficulties.

24. WAIVER. The parties may waive this Agreement only by a writing executed by the party or parties against whom the waiver is sought to be enforced. No failure or delay (a) in exercising any right or remedy, or (b) in requiring the satisfaction of any condition, (c) under this Agreement, and no act, omission or course of dealing between the parties, operates as a waiver or estoppel of any right, remedy or condition. A waiver made in writing on one occasion is effective only in that instance and only for the purpose stated. A waiver once given is not to be construed as a waiver on any future occasion or against any other person.

25. COMPLIANCE. Customer shall comply with all applicable United States, foreign and local laws and regulations, including, without limitation, export control laws and regulations of the U.S. Export Administration.

26. AMENDMENT. The parties may amend this Agreement only by a written agreement of the parties that identifies itself as an amendment to this Agreement. If any part of this Agreement is found invalid or unenforceable that part will be enforced to the maximum extent permitted by law and the remainder of this Agreement will remain in full force.

27. CONSTRUCTION. This Agreement reflects the wording negotiated and accepted by the parties and no rule of construction shall apply against either party.

28. LANGUAGE. This Agreement is proposed and executed in the English language only and any translation of this Agreement into any other language shall have no effect. All proceedings related to this Agreement will be conducted in the English language.

29. ENTIRE AGREEMENT. This Agreement (including the Contract, additional Appendices, and Schedules hereto) constitutes the entire agreement between the parties with respect to the subject matter hereof. All earlier and contemporaneous negotiations and agreements between the parties on the matters contained in this Agreement, if any, are expressly merged into and superseded by this Agreement.

MARKETING. Guardian may use Customer's name as part of a general list of customers and may refer to Customer as a user of the Services in its, general advertising and marketing materials.

END OF EXHIBIT A