DAVE YOST
OHIO ATTORNEY GENERAL

Information Technology Services
150 E. Gay St. 20th Floor
Columbus, OH 43215

Request for Quotations (RFQ)

RFQ #AGOITS22005

IBM Content Manager and OpenText Captiva Services

Overview: The Ohio Attorney General's Office ("AGO") is seeking quote submissions in response to this Request for Quotations ("RFQ") to secure goods and/or services as defined below.

Ohio Attorney General Dave Yost is an elected official who is the Chief Law Officer for the State of Ohio and its agencies, boards and commissions. The office consists of about 1600 employees in nearly 30 distinct sections that advocate for consumers and victims of crime, assists the criminal justice community, provide legal counsel for state offices and agencies, and enforce certain state laws.

Purpose: The AGO is soliciting responses for the selection of a vendor to provide on-going, on-demand support of the IBM Content Manager and OpenText Captiva products being used by various applications within the AGO environment. These will be time and materials support services such as, but not limited to, break/fix, remote troubleshooting, installation of updates, other types or proactive and reactive services and basic usability assistance by a vendor/consultant with specific Content Manager and OpenText Captiva experience.

Terms and Conditions: The selected vendor may not report to the AGO or ship any equipment to the AGO, and no work may commence until an AGO contract as well as all other applicable agreements, including end user license agreements (EULA), subscription, and/or other license agreements have been fully executed, background checks are completed and approved for all vendor employees, and a purchase order is issued to the vendor. Note that the contracting, background check, and purchase order processes may take up to six to ten weeks in total to complete.

The work shall be performed within the United States or otherwise only where the vendor has received prior authorization from the AGO and is defined in the scope of work. No information or data provided by or belonging to the AGO shall be stored, accessed from, or transmitted to outside of the United States.

Additionally, the selected vendor(s) may be required to sign various AGO forms and/or agree to comply with certain requirements prior to commencement of work, including the following:

- AGO Non-Employee Computer Usage, Network Access, Internet Usage and Social Media Policy, Acknowledgement form. This is an AGO nondisclosure statement. Attachment A.
- IRS Publication 1075. This is guidance for US government agencies and their agents that access federal tax information (FTI) to ensure that they use policies, practices, and controls to protect its confidentiality. Attachment B.

- Federal Bureau of Investigation, Criminal Justice Information Services Security Addendum and Certification. This is a uniform agreement approved by the US Attorney General that helps ensure the security and confidentiality of CJI required by the Security Policy. Attachment C.
- Ohio Attorney General Products and Services Standards of Conduct Policy User Acknowledgement. This is an agreement to ensure that any individual accessing products and services of the AGO, including network services and data on AGO electronic networks become familiar with and acknowledge awareness of this Standards of Conduct Policy (the "Policy") when connecting to the AGO network from any host to utilize AGO Products and Services. Attachment D.

Once the selected vendor(s) reports to the AGO, all work will be conducted in accordance with AGO policies, procedures, coding standards, and best practices as instructed by the AGO.

The AGO is subject to the requirements of the Ohio Public Records Act, located at Ohio Revised Code Section 149.43. Accordingly, vendors must understand that information and other materials submitted in response to this RFQ or in connection with any contract as a result of this RFQ is subject to disclosure as a public record. Accordingly, responses should not include any confidential or trade secret information.

During the term of any contract resulting from this RFQ, the vendor shall be engaged by the AGO solely on an independent contractor basis, and the vendor shall therefore be responsible for all the vendor's business expenses, including, but not limited to, employees' wages and salaries, insurance of every type and description, and all business and personal taxes, including income and Social Security taxes and contributions for Workers' Compensation and Unemployment Compensation coverage, if any.

Vendor Quote Content: All responses to this RFQ must include the information listed below to ensure the quote submission is considered for this opportunity. Any material deviation from the format or information below may result in rejection of a response.

1. A Quote Cover Letter on company letterhead that includes at a minimum:
    - AGO Request for Quote number.
    - Contact Person, who has the authority to answer questions regarding the quote, including their Name, Title, Address, Phone Number, and E-mail Address.
    - DAS State Term Schedule (STS) Number, if applicable.
    - List price and discounted price for AGO.
    - Quote date expiration (at least 60 days from deadline date).
    - Acknowledgement of the project scope and duration.
    - Name, Title and Signature of an individual authorized to legally bind the company.
2. Proposed Personnel/Candidate, Experience and Resumes.
3. Total cost and cost breakdown, including DAS contract price list line item description, if applicable.
4. Attachments A and D, completed and returned for the proposed personal/candidate as part of the quote content.

Quote Submission: All responses must be submitted no later than **March 19 at 1:00 PM** Eastern Time via email to: Procurement@OhioAttorneyGeneral.gov, referencing the RFQ title: RFQ #AGOITS22005 **IBM Content Manager and OpenText Captiva Services**. Any quotation received after the required time and date specified for receipt shall be considered late and non-responsive. Any late quotations will not be evaluated for award.

The AGO has the discretion to select a vendor and to reject responses that are not in the best interest of the AGO, or to rescind this RFQ. The AGO may waive minor defects and/or request clarifications in the responses that do not materially deviate from the specifications or otherwise create an unfair competitive advantage. Any response, revision or amendment to a response received after the date and time specified or improperly marked or submitted may be disqualified.

The AGO will not be liable for any costs incurred by a vendor in responding to this RFQ, regardless of whether the AGO awards any contract(s) through this process, decides to cancel this RFQ for any reason, or issues another RFQ if it is deemed to be in the best interest of the AGO to do so.

The AGO reserves the right to negotiate all terms associated with this RFQ, including price. It is entirely within the discretion of the AGO to permit negotiations. A vendor must not submit a response assuming that there will be an opportunity to negotiate any aspect of the response. The AGO is free to limit the negotiations to particular aspects of any response. Vendors should not base their pricing on the assumption of long-term financing by the AGO that extends beyond the current biennium, which ends June 30, 2023.

The contract will be awarded to the vendor that offers the best value, based on a combination of qualifications and price. The contract will not necessarily be awarded to the lowest price proposal.

Calendar of Events:

- RFQ issued date: March 1, 2021
- Quote due date: March 19, 2021, 1:00 PM
- Estimated selection date: April 30, 2021
- Estimated initial contract execution date: July 1, 2021

Communication and Inquiries: Unless the AGO advises differently, any contact is to be in writing using the State of Ohio Procurement website. If an inquiry period is opened, all inquiries and responses will be posted to the same website. The due date for any inquiry within the intent and scope of this request will be listed on the website. Any reference materials related to this RFQ will be also available on the website. The State of Ohio Procurement website address is linked from: https://www.ohioattorneygeneral.gov/Business/Services-for-Business/RFQ.

Work Locations: Work performed under a contract awarded pursuant to this RFQ may be conducted at the AGO location provided. If onsite work is requested, the vendor shall not be reimbursed for travel, lodging or any other expenses incurred in the performance of the work under the contract.

AGO Request for Services – Responsibilities of the Vendor:

1. Provide time and material support services as described on IBM Content Manager and OpenText Captiva as requested by the AGO's office.
2. Project Management:
    - Submit monthly report of billable services provided.
    - Provide timely alerts when hours are tracking to exceed estimated hours on tasks for any given month.
    - Provide Project Change Request (PCR) for any hours required beyond 80 in a given month. PCR will document and be approved by the AGO for work requiring additional hours before work is performed.
    - Manage resources assigned and scheduling of support services.

AGO Assumptions:

1. AGO will assign a main point of contact with authority to authorize and prioritize services requested by AGO.
2. AGO can request services verbally, via email to the vendor, or through other means which assure request will be received in a timely manner. Verbal requests for services will be documented in writing.
3. The AGO will only be charged for the actual work authorized by the AGO.
4. AGO will apply a severity level to the requests. The levels are as follows:
    a) Level 1 – The vendor will provide a call back within 2 hours and start working on the task within 8 hours. These include critical "work stoppage" issues that prevent completion of critical business functions.
    b) Level 2 - The vendor will provide an email/call back within 24 hours and will respond with an issue resolution plan within 48 hours. These include high priority issues that slow or prevent completion of some business functions. A work around is in place or the process can be delayed for a period until the issue is resolved.
    c) Level 3 - The vendor will provide an email/call back within 2 days and will respond with an issue resolution plan within 5 days. These include low priority issues, questions, or research items.
5. All requests for after hours or holiday work need to be approved by the AGO in writing.
6. Remote access to servers needed to diagnose issues remotely can be provided if necessary.
7. The total hours for this service shall not exceed 1000 hours. The AGO will only be charged for the actual work authorized by the AGO.

DAVE YOST
OHIO ATTORNEY GENERAL

Information Technology Services
Office of the Chief Information Officer
Office 614-466-5272
Fax 614-644-2055

150 East Gay Street, 20th Floor
Columbus, Ohio 43215
www.OhioAttorneyGeneral.gov

Form ITSSEC02 Rev. 01-15-2019

Ohio Attorney General Non-Employee Computer Usage, Network Access, Internet Usage, and Social Media Policy
Contractor Employee Acknowledgement

This Ohio Attorney General ("AGO") Non-Employee Computer Usage, Network Access, Internet Usage, and Social Media Policy Contractor Employee Acknowledgement (the "Acknowledgement") sets forth the policies and procedures for proper computer, network, Internet, and social media use by all non-AGO personnel performing work for the AGO (the "User"). This Computer Usage, Network Access, Internet Usage, and Social Media Policy (the "Policy") applies to all independent contractors and/or any other consultant performing work for any contractor or consultant doing business with the AGO and their employees. Any violation of this Policy may result in, among other penalties and liabilities, immediate removal of User access to all AGO systems and notification to the User's employer of the violation. The AGO may temporarily suspend or block a User's access to an account when it appears reasonably necessary to do so to protect the security of the AGO network or to protect the AGO from liability. **All Users will be held personally responsible and liable, to the fullest extent of the law, for actions in violation of this Policy.**

I. COMPUTER USAGE AND NETWORK ACCESS POLICY

In order to comply with Ohio law and to ensure the security and integrity of AGO network resources (e.g. routers, switches, servers, workstations, printers, etc.), the User shall:

- Acknowledge he/she has been provided with and will comply with the provisions of this Policy;
- Utilize the AGO's network resources and any information/data provided therefrom for authorized use only;
- Use all computer resources, including, but not limited to, equipment, hardware, software, documentation, and data solely for AGO business;
- Immediately notify the AGO of any proven or suspected unauthorized disclosure or exposure of any AGO data or of information or identity theft;
- Immediately notify the AGO if a Security Event has occurred or if suspicion of a Security Event has been identified. A Security Event includes, but is not limited to:
    - Any abnormality in the environment that could lead to a compromise of the system integrity or result in disclosure of data,
    - Hack attempts,
    - Malware,
    - Changes in security infrastructure,
    - System failures,
    - Compromised user accounts, and
    - Lost/stolen laptop or media.

- Promptly notify the AGO of the date of separation if User leaves the employer or if access to AGO networks, applications, systems, and/or AGO data is no longer required. Access to the AGO network may be rescinded for failure to provide such notice;
- Take all reasonable precautions to prevent the dissemination of User's credentials by any means, including, but not limited to, not sharing the User's username and password, not writing down the username and password, etc.;
- Create a password in compliance with the AGO password criteria set forth below. The AGO reserves the right to change the password criteria from time to time. Compliance with the AGO password criteria will be enforced via automated password authentication or public/private keys with strong pass-phrases. The AGO password criteria are as follows:
    - Minimum 12 characters,
    - Must include 3 of the 4: a-z, A-Z, 0-9, and special characters,
    - Passwords will require being reset based on level of access at the AGO's discretion,
    - Passwords must be kept securely by the account owner, and never be shared,
    - Passwords must not contain sequences 01, 123, abc, etc.,
    - Passwords must not contain properly spelled dictionary words, and
    - Passwords must not be directly identifiable to the user (e.g. social security number, date of birth, spouse's name, username, etc.).

  Password history will be retained for 24 changes to ensure unique passwords. Inactive accounts will be disabled at 90 days, and removed at 120 days. Users of accounts that reach 120 days of inactivity must reapply for an account.
- Comply with all applicable network or operating system restrictions, whether or not they are built into the operating system or network, and whether or not they can be circumvented by technical means;
- Comply with all federal, Ohio, and any other applicable law, including, but not limited to: Internal Revenue Service Publication 1075 which is based on United States Code Title 26, Section 6103; Ohio Revised Code Chapter 1347; the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and the associated omnibus rule to modify the HIPAA Privacy, Security and Enforcement Rules; and the Health information Technology for Economic and Clinical Health ("HITECH") Act; and
- Comply with all applicable contracts and licenses.

User shall not:

- Move, alter, delete, copy, or otherwise change any information/data stored or contained on AGO networks or computers without express, written authorization by the AGO (e.g. a written agreement, scope of work, or approved vendor quotation).
- Leave a computer unattended for any period of time unless it is secured in such a way that the computer cannot be used by any other individual (e.g. sign-off procedure, password protected screen saver, etc.);
- Make paper, electronic, or any other copies or reproductions of any AGO information/data or licensed materials, regardless of how the information/data or materials were obtained, without prior authorization from the AGO;
- Use an e-mail account, username, or signature line other than the User's own;

- Attempt to represent himself or herself as any individual other than him/herself. This specifically includes, but is not limited to, use of the Internet, e-mail, online service account, or signature line; and
- Share any information/data gained through use of AGO networks with anyone outside the AGO without prior authorization from the AGO.

II. INTERNET USAGE POLICY

Improper use of the AGO's Internet and Internet services can waste time and resources, violate AGO policies, and create legal liability and embarrassment for both the AGO and the User. The AGO's Internet services include, but are not limited to, e-mail, file transfer protocol, and access to the World Wide Web. This Policy applies to use of the AGO's Internet and Internet services (collectively the "Internet") accessed using AGO network resources or paid Internet access methods, and used in a manner that identifies the User with the AGO.

User's authorized Internet access will be provided by the AGO through vendors approved by the Information Technology Services Section of the AGO ("ITS"). All other access methods to the Internet are prohibited.

All activities that require use of the AGO's Internet must be pre-approved by the AGO. Certain activities that require use of the AGO's Internet are strictly prohibited. Therefore, the User shall not use the AGO's Internet in connection with any of the following activities:

- Engaging in illegal, fraudulent, or malicious conduct;
- Engaging in conduct that is beyond the scope of the contract or retention agreement, if applicable, for which User access is granted;
- Transmitting, downloading, retrieving, or storing offensive, obscene, defamatory, or otherwise prohibited material (including, but not limited to, pornographic, X-rated, religious, political, threatening, or racial or sexual harassing content);
- Harassment of any kind;
- Monitoring or intercepting the files or electronic communications of AGO employees or third parties;
- Attempting to test, circumvent, or defeat the security systems of the AGO or any other organization, or accessing or attempting to access the AGO's or any other organizations' systems without prior authorization from the AGO;
- Providing access to anyone other than the User to the AGO Internet and/or network resources without prior authorization from the AGO;
- Providing anyone access to or disseminating any AGO information/data, regardless of whether or not it is considered confidential or public, and regardless of how the information/data was obtained;
- Using or accessing social media;
- Participating in chat rooms, open forum discussions, interactive or instant messaging unless such participation is for business purposes and pre-approved by ITS;
- Operating a business for personal gain, sending chain letters, or soliciting money in any way for religious, political, charitable, personal, or business purposes while acting within the scope of User's work and using AGO Internet services;
- Transmitting, collecting, and/or receiving incendiary statements which might incite violence or describe or promote the use of weapons or devices associated with terrorist activities;

- Distributing frivolous, non-business related material such as jokes and or cartoons; and
- Participating in any other unauthorized activity that may bring damage, discredit upon, or create liability to the AGO.

III. SOCIAL MEDIA POLICY

Social media and social networking sites are not private and the User shall use good professional judgment regarding any references to the AGO, this Acknowledgement, any applicable contract or memorandum of understanding, clients of the AGO, or services provided by the AGO. All Users shall abide by and be aware of the following:

- Personal blogs shall contain clear disclaimers that the views expressed by the author in the blog are the author's alone and do not represent the views of the AGO;
- User shall refrain from discussions regarding employees and clients of the AGO on any social media or networking site;
- Social media activities shall not be conducted on AGO networks or while using the AGO's Internet;
- User's online presence may be linked to this Acknowledgement, any applicable related contract or memorandum of understanding, and the AGO. Be aware that the User's actions captured through images, posts, or comments should not include illegal, harassing, or other content that violates the law and/or the User's employer's or the AGO's policies or ethical requirements. Such conduct may lead to termination of the User's employment relationship with the AGO;
- AGO logos and templates shall not be used on personal blogs or for personal postings on social network sites; and
- Users engaging in chat rooms, blogging, tweeting, or other social media during non-working hours shall not reference or discuss information from the AGO or represent themselves as employees of, or spokespersons for, the Attorney General or the AGO.

IV. USER'S UNDERSTANDINGS

- User understands that any User who engages in electronic communications with people or entities in other states or countries, or on other systems or networks, are on notice that they may also be subject to the laws of those other states and countries and the rules and policies of those other systems and networks. User is responsible for obtaining, understanding, and complying with the laws, rules, policies, contracts, and licenses applicable to their particular uses.
- User understands that the confidentiality and privileged nature of AGO files and information/data must be respected and protected. User understands that the AGO retains the right, and has the capability, among other security measures, to review, audit, or monitor the User's directories, files, e-mails (both sent and received), as well as Internet usage to ensure maintenance of information/data integrity. User also understands that the AGO has the right to remove or destroy unauthorized materials found on AGO networks and to terminate User's employment relationship with the AGO for breach of this Policy.
- User understands that, among other security measures, the AGO makes backup copies and stores User information. User activities are therefore not private and User content is potentially stored on AGO servers. User also understands that the AGO is subject to public records disclosure and to discovery requests and that the User's activities and information may be released pursuant to a public records or discovery request.

- User understands that web browsers leave "footprints" that provide a record of all site visits. Access to, and use of, the Internet is not confidential and may be a public record.
- User understands that all Users and their employers will be held responsible and liable to the fullest extent of the law for actions while using the AGO's network resources, computers, and Internet.

User Acknowledgement

By signing below, you, as a User, acknowledge that you have read and understand this Policy, and you, the User, agree to comply with the terms of this Policy.

Printed Name of User: _____ Title: _____

User's Employer: _____ Contract End Date: _____

User's Phone Number: _____ User's E-mail: _____

Requested Period of Access:
From: _____ To:_____

Application or resources requested:

(VPN, AGO Domain Account, systems support, etc.)

_____

_____

Public IP: _____

User's Signature: _____ Date: _____

Account Identity Control Information (1):_____(mother's maiden name, etc.)

Account Identity Control Information (2):_____(first car owned, etc.)

The above Account Identity Control Information will be used to identify you in the event that you have lost or do not remember your account ID or password. The User must provide two unique pieces of information as a shared secret with the AGO to verify your identity when account resets and other services that require identity verification are needed. It is the User's obligation to provide and secure these shared secrets in the same manner that is required for account credentials.

Employer Acknowledgement

By signing below, you, as the User's employer, acknowledge that you are a duly authorized representative of the User's employer able to bind the employer to the terms of this Acknowledgement. By signing below, you, as the User's employer, also agree that access by the employer may be rescinded at the discretion of the AGO, with prior notice, if the employer fails to take reasonable precautions, as defined above, to avoid a breach of this Policy and/or to ensure that the employer's Users do not breach this Policy.

Printed Name: _____ Title: _____

Employer's Signature: _____ Date: _____

Employer's Phone Number: _____

Employer's E-mail: _____

Official AGO Use Only:

AGO Contract #:_____

AGO ITS Work Order Number: _____

AGO issued username: _____

AGO issued rights: _____

_____

_____

AGO Chief Information Officer, Chief Information Security Officer, or their designee

Name: _____ Title: _____

Signature: _____ Date: _____

Comments: _____

_____

_____

_____

_____

_____

_____

ATTACHMENT
IRS Publication 1075

1075 CONTRACT LANGUAGE FOR TECHNOLOGY SERVICES

I. PERFORMANCE

In performance of this Agreement, Contractor agrees to comply with and assume responsibility for compliance by his or her employees with the following requirements:

(1) All work will be done under the supervision of Contractor or Contractor's employees.

(2) Contractor and Contractor's employees with access to or who use Federal Tax Information ("FTI") must meet the background check requirements defined in IRS Publication 1075.

(3) Any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this Agreement. Information contained in such material will be treated as confidential and will not be divulged or made known in any manner to any person except as may be necessary in the performance of this Agreement. Disclosure to anyone other than an officer or employee of Contractor will be prohibited.

(4) All returns and return information will be accounted for upon receipt and properly stored before, during, and after processing. In addition, all related output will be given the same level of protection as required for the source material.

(5) Contractor certifies that the data processed during the performance of this Agreement will be completely purged from all data storage components of his or her computer facility, and no output will be retained by Contractor at the time the work is completed. If immediate purging of all data storage components is not possible, Contractor certifies that any IRS data remaining in any storage component will be safeguarded to prevent unauthorized disclosures.

(6) Any spoilage or any intermediate hard copy printout that may result during the processing of IRS data will be given to the agency or his or her designee. When this is not possible, Contractor will be responsible for the destruction of the spoilage or any intermediate hard copy printouts, and will provide the agency or his or her designee with a statement containing the date of destruction, description of material destroyed, and the method used.

(7) All computer systems receiving, processing, storing or transmitting FTI must meet the requirements defined in IRS Publication 1075. To meet functional and assurance requirements, the security features of the environment must provide for the managerial, operational, and technical controls. All security features must be available and activated to protect against unauthorized use of and access to Federal Tax Information.

(8) No work involving Federal Tax Information furnished under this Agreement will be subcontracted without prior written approval of the IRS.

(9) Contractor will maintain a list of employees authorized access. Such list will be provided to the agency and, upon request, to the IRS reviewing office.

(10) The agency will have the right to void the Agreement if the contractor fails to provide the safeguards described above.

(11) Audit and accountability policy and procedures must be developed, documented, disseminated, and updated as necessary to facilitate implementing audit and accountability security controls.

a. To support the audit of activities, all agencies must ensure that audit information is archived for seven years.

b. The information system must protect audit information and audit tools from unauthorized access, modification, and deletion.

(12) IRS Publication 1075 compliance is mandatory. The aforementioned compliance items are a small selection of key elements contained within the requirements defined in IRS publication 1075. The State reserves the right to impose additional and more stringent requirements as deemed necessary to protect FTI (Federal Tax Information).

II. CRIMINAL/CIVIL SANCTIONS

(1) Each officer or employee of any person to whom returns or return information is or may be disclosed will be notified in writing by such person that returns or return information disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any such returns or return information for a purpose or to an extent unauthorized herein constitutes a felony punishable upon conviction by a fine of as much as $5,000 or imprisonment for as long as 5 years, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized further disclosure of returns or return information may also result in an award of civil damages against the officer or employee in an amount not less than $1,000 with respect to each instance of unauthorized disclosure. These penalties are prescribed by IRCs 7213 and 7431 and set forth at 26 CFR 301.6103(n)-1.

(2) Each officer or employee of any person to whom returns or return information is or may be disclosed shall be notified in writing by such person that any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this Agreement. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of the Agreement. Inspection by or disclosure to anyone without an official need-to-know constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as $1,000 or imprisonment for as long as 1 year, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized inspection or disclosure of returns or return information may also result in an award of civil damages against the officer or employee [United States for Federal employees] in an amount equal to the sum of the greater of $1,000 for each act of unauthorized inspection or disclosure with respect to which such defendant is found liable or the sum of the actual damages sustained by the plaintiff as a result of such unauthorized inspection or disclosure plus in the case of a willful inspection or disclosure which is the result of gross negligence, punitive damages, plus the costs of the action. These penalties are prescribed by IRC 7213A and 7431 and set forth at 26 CFR 301.6103(n)-1.

(3) Additionally, it is incumbent upon Contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a(i)(1), which is made applicable to contractors by 5 U.S.C. 552a(m)(1), provides that any officer or employee of a contractor, who by virtue of his/her employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material

is prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.

(4) Granting a contractor access to FTI must be preceded by certifying that each individual understands the agency's security policy and procedures for safeguarding IRS information. Contractors must maintain their authorization to access FTI through annual recertification. The initial certification and recertification must be documented and placed in the agency's files for review. As part of the certification and at least annually afterwards, contractors must be advised of the provisions of IRCs 7431, 7213, and 7213A (see Exhibit 4 of Publication 1075, Sanctions for Unauthorized Disclosure, and Exhibit 5 of Publication 1075, Civil Damages for Unauthorized Disclosure). The training provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches (See Section 10 of Publication 1075). For both the initial certification and the annual certification, Contractor must sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.

III. INSPECTION

The IRS and the Agency, with 24 hour notice, shall have the right to send its inspectors into the offices and plants of Contractor to inspect facilities and operations performing any work with FTI under this Agreement for compliance with requirements defined in IRS Publication 1075. The IRS' right of inspection shall include the use of manual and/or automated scanning tools to perform compliance and vulnerability assessments of information technology (IT) assets that access, store, process or transmit FTI. On the basis of such inspection, corrective actions may be required in cases where Contractor is found to be noncompliant with Agreement safeguards.

FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM

Legal Authority for and Purpose and Genesis of the Security Addendum

Traditionally, law enforcement and other criminal justice agencies have been responsible for the confidentiality of their information. Accordingly, until mid-1999, the Code of Federal Regulations Title 28, Part 20, subpart C, and the National Crime Information Center (NCIC) policy paper approved December 6, 1982, required that the management and exchange of criminal justice information be performed by a criminal justice agency or, in certain circumstances, by a noncriminal justice agency under the management control of a criminal justice agency.

In light of the increasing desire of governmental agencies to contract with private entities to perform administration of criminal justice functions, the FBI sought and obtained approval from the United States Department of Justice (DOJ) to permit such privatization of traditional law enforcement functions under certain controlled circumstances. In the Federal Register of May 10, 1999, the FBI published a Notice of Proposed Rulemaking, announcing as follows:

> 1. Access to CHRI [Criminal History Record Information] and Related Information, Subject to Appropriate Controls, by a Private Contractor Pursuant to a Specific Agreement with an Authorized Governmental Agency To Perform an Administration of Criminal Justice Function (Privatization). Section 534 of title 28 of the United States Code authorizes the Attorney General to exchange identification, criminal identification, crime, and other records for the official use of authorized officials of the federal government, the states, cities, and penal and other institutions. This statute also provides, however, that such exchanges are subject to cancellation if dissemination is made outside the receiving departments or related agencies. Agencies authorized access to CHRI traditionally have been hesitant to disclose that information, even in furtherance of authorized criminal justice functions, to anyone other than actual agency employees lest such disclosure be viewed as unauthorized. In recent years, however, governmental agencies seeking greater efficiency and economy have become increasingly interested in obtaining support services for the administration of criminal justice from the private sector. With the concurrence of the FBI's Criminal Justice Information Services (CJIS) Advisory Policy Board, the DOJ has concluded that disclosures to private persons and entities providing support services for criminal justice agencies may, when subject to appropriate controls, properly be viewed as permissible disclosures for purposes of compliance with 28 U.S.C. 534.
>
> We are therefore proposing to revise 28 CFR 20.33(a)(7) to provide express authority for such arrangements. The proposed authority is similar to the authority that already exists in 28 CFR 20.21(b)(3) for state and local CHRI systems. Provision of CHRI under this authority would only be permitted pursuant to a specific agreement with an authorized governmental agency for the purpose of providing services for the administration of criminal justice. The agreement would be required to incorporate a security addendum approved by the Director of the FBI (acting for the Attorney General). The security

addendum would specifically authorize access to CHRI, limit the use of the information to the specific purposes for which it is being provided, ensure the security and confidentiality of the information consistent with applicable laws and regulations, provide for sanctions, and contain such other provisions as the Director of the FBI (acting for the Attorney General) may require. The security addendum, buttressed by ongoing audit programs of both the FBI and the sponsoring governmental agency, will provide an appropriate balance between the benefits of privatization, protection of individual privacy interests, and preservation of the security of the FBI's CHRI systems.

The FBI will develop a security addendum to be made available to interested governmental agencies. We anticipate that the security addendum will include physical and personnel security constraints historically required by NCIC security practices and other programmatic requirements, together with personal integrity and electronic security provisions comparable to those in NCIC User Agreements between the FBI and criminal justice agencies, and in existing Management Control Agreements between criminal justice agencies and noncriminal justice governmental entities. The security addendum will make clear that access to CHRI will be limited to those officers and employees of the private contractor or its subcontractor who require the information to properly perform services for the sponsoring governmental agency, and that the service provider may not access, modify, use, or disseminate such information for inconsistent or unauthorized purposes.

Consistent with such intent, Title 28 of the Code of Federal Regulations (C.F.R.) was amended to read:

§ 20.33 Dissemination of criminal history record information.

a) Criminal history record information contained in the Interstate Identification Index (III) System and the Fingerprint Identification Records System (FIRS) may be made available:

1) To criminal justice agencies for criminal justice purposes, which purposes include the screening of employees or applicants for employment hired by criminal justice agencies.

2) To noncriminal justice governmental agencies performing criminal justice dispatching functions or data processing/information services for criminal justice agencies; and

3) To private contractors pursuant to a specific agreement with an agency identified in paragraphs (a)(1) or (a)(6) of this section and for the purpose of providing services for the administration of criminal justice pursuant to that agreement. The agreement must incorporate a security addendum approved by the Attorney General of the United States, which shall specifically authorize access to criminal history record information, limit the use of the information to the purposes for which it is provided, ensure the security and confidentiality of the information consistent with these regulations, provide for sanctions, and contain such other provisions as the Attorney General may require. The power

and authority of the Attorney General hereunder shall be exercised by the FBI Director (or the Director's designee).

This Security Addendum, appended to and incorporated by reference in a government-private sector contract entered into for such purpose, is intended to insure that the benefits of privatization are not attained with any accompanying degradation in the security of the national system of criminal records accessed by the contracting private party. This Security Addendum addresses both concerns for personal integrity and electronic security which have been addressed in previously executed user agreements and management control agreements.

A government agency may privatize functions traditionally performed by criminal justice agencies (or noncriminal justice agencies acting under a management control agreement), subject to the terms of this Security Addendum. If privatized, access by a private contractor's personnel to NCIC data and other CJIS information is restricted to only that necessary to perform the privatized tasks consistent with the government agency's function and the focus of the contract. If privatized the contractor may not access, modify, use or disseminate such data in any manner not expressly authorized by the government agency in consultation with the FBI.

FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM

The goal of this document is to augment the CJIS Security Policy to ensure adequate security is provided for criminal justice systems while (1) under the control or management of a private entity or (2) connectivity to FBI CJIS Systems has been provided to a private entity (contractor). Adequate security is defined in Office of Management and Budget Circular A-130 as "security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information."

The intent of this Security Addendum is to require that the Contractor 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).

This Security Addendum identifies the duties and responsibilities with respect to the installation and maintenance of adequate internal controls within the contractual relationship so that the security and integrity of the FBI's information resources are not compromised. The security program shall include consideration of personnel security, site security, system security, and data security, and technical security.

The provisions of this Security Addendum apply to all personnel, systems, networks and support facilities supporting and/or acting on behalf of the government agency.

1.00 Definitions

1.01 Contracting Government Agency (CGA) - the government agency, whether a Criminal Justice Agency or a Noncriminal Justice Agency, which enters into an agreement with a private contractor subject to this Security Addendum.

1.02 Contractor - a private business, organization or individual which has entered into an agreement for the administration of criminal justice with a Criminal Justice Agency or a Noncriminal Justice Agency.

2.00 Responsibilities of the Contracting Government Agency.

2.01 The CGA will ensure that each Contractor employee receives a copy of the Security Addendum and the CJIS Security Policy and executes an acknowledgment of such receipt and the contents of the Security Addendum. The signed acknowledgments shall remain in the possession of the CGA and available for audit purposes. The acknowledgement may be signed by hand or via digital signature (see glossary for definition of digital signature).

3.00 Responsibilities of the Contractor.

3.01 The Contractor will 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 and all subsequent versions), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

4.00 Security Violations.

4.01 The CGA must report security violations to the CJIS Systems Officer (CSO) and the Director, FBI, along with indications of actions taken by the CGA and Contractor.

4.02 Security violations can justify termination of the appended agreement.

4.03 Upon notification, the FBI reserves the right to:

a. Investigate or decline to investigate any report of unauthorized use;

b. Suspend or terminate access and services, including telecommunications links. The FBI will provide the CSO with timely written notice of the suspension. Access and services will be reinstated only after satisfactory assurances have been provided to the FBI by the CGA and Contractor. Upon termination, the Contractor's records containing CHRI must be deleted or returned to the CGA.

5.00 Audit

5.01 The FBI is authorized to perform a final audit of the Contractor's systems after termination of the Security Addendum.

6.00 Scope and Authority

6.01 This Security Addendum does not confer, grant, or authorize any rights, privileges, or obligations on any persons other than the Contractor, CGA, CJA (where applicable), CSA, and FBI.

6.02 The following documents are incorporated by reference and made part of this agreement: (1) the Security Addendum; (2) the NCIC 2000 Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20. The parties are also subject to applicable federal and state laws and regulations.

6.03 The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they augment the provisions of the CJIS Security Policy to provide a minimum basis for the security of the system and contained information and it is understood that there may be terms and conditions of the appended Agreement which impose more stringent requirements upon the Contractor.

6.04 This Security Addendum may only be modified by the FBI, and may not be modified by the parties to the appended Agreement without the consent of the FBI.

6.05 All notices and correspondence shall be forwarded by First Class mail to:

Information Security Officer

Criminal Justice Information Services Division, FBI

1000 Custer Hollow Road

Clarksburg, West Virginia 26306

FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM

CERTIFICATION

I hereby certify that I am familiar with the contents of (1) the Security Addendum, including its legal authority and purpose; (2) the NCIC Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20, and agree to be bound by their provisions.

I recognize that criminal history record information and related data, by its very nature, is sensitive and has potential for great harm if misused. I acknowledge that access to criminal history record information and related data is therefore limited to the purpose(s) for which a government agency has entered into the contract incorporating this Security Addendum. I understand that misuse of the system by, among other things: accessing it without authorization; accessing it by exceeding authorization; accessing it for an improper purpose; using, disseminating or re-disseminating information received as a result of this contract for a purpose other than that envisioned by the contract, may subject me to administrative and criminal penalties. I understand that accessing the system for an appropriate purpose and then using, disseminating or re-disseminating the information received for another purpose other than execution of the contract also constitutes misuse. I further understand that the occurrence of misuse does not depend upon whether or not I receive additional compensation for such authorized activity. Such exposure for misuse includes, but is not limited to, suspension or loss of employment and prosecution for state and federal crimes.

_____ _____

Printed Name/Signature of Contractor Employee Date

_____ _____

Printed Name/Signature of Contractor Representative Date

_____

Organization and Title of Contractor Representative

DAVE YOST
OHIO ATTORNEY GENERAL

Information Technology Services
Office of the Chief Information Officer
Office 614-466-5272
Fax 614-644-2055

150 East Gay Street, 20th Floor
Columbus, Ohio 43215
www.OhioAttorneyGeneral.gov

Form ITSSEC01 Rev. 01-15-2019

Ohio Attorney General Products and Services Standards of Conduct Policy
User Acknowledgement

The purpose of this Acknowledgement is to ensure that any individual (the "User") accessing products and services of the Ohio Attorney General ("AGO") (including all AGO network services and data which may include, but is not limited to, FTPS, e-mail, source data, database services, and user account management ("Products and Services")) on AGO electronic networks become familiar with and acknowledge awareness of this Standards of Conduct Policy (the "Policy") when connecting to the AGO network from any host to utilize AGO Products and Services. This Policy is designed to minimize the AGO and the State of Ohio's potential exposure to damages which may result from unauthorized use of AGO Products and Services. Such damages include, but are not limited to, the loss or dissemination of sensitive or confidential data, loss or dissemination of intellectual property, damage to public image, and damage to critical AGO internal systems. Any violation of this Policy may result in immediate termination of User access to any or all AGO Products and Services and notification of the violation to the User's employer signing this Policy in conjunction with the User. **All Users will be held personally responsible and liable, to the fullest extent of the law, for actions in violation of this Policy.**

This Standards of Conduct Policy must be followed at all times. Therefore, all Employers and Users shall:

- Utilize AGO's network resources, applications, systems and any information provided therefrom for authorized use only.
- Take reasonable precautions to ensure that the computer used to connect to AGO Products and Services is secure and free of malicious code. Examples of reasonable precautions include, but are not limited to:
    - Endpoint protection (e.g. anti-malware, user controls, etc.),
    - Perimeter protection (e.g. firewall, Host/Network Intrusion Detection System, Host/Network Intrusion Protection System, Demilitarized Zone, Universal Threat Management, etc.),
    - Audit logs,
    - Adequate physical security for data and systems,
    - System monitoring and auditing of the logs,
    - Incident response policy, and
    - Data safeguarding procedures appropriate for the type of data and access.
- Protect against improper access, use, loss alteration or destruction of any AGO data. Examples of this protection include, but are not limited to:
    - Never sharing an account,
    - Reporting if the User has more access than needed,
    - Lock or log out of workstations when not actively using them,
    - Ensure workspaces are set up to prevent passersby from viewing any information,
    - Only using data or access to the data for the express authorized purpose,
    - Preventing the introduction of malicious code,

- Ensuring data is backed up or replicated, and
- Ensuring data is not copied or does not leave the work environment.

- Promptly notify the AGO if a Security Event has occurred or if suspicion of a Security Event has been identified. A Security Event includes, but is not limited to:
  - Any abnormality in the environment that could lead to a compromise of the system integrity or result in disclosure of data,
  - Hack attempts,
  - Malware,
  - Changes in security infrastructure,
  - System failures,
  - Compromised user accounts, and
  - Lost/stolen laptop or media.
- Promptly notify the AGO of the date of separation if User leaves the employer or if access to AGO networks, applications, systems and/or AGO data is no longer required. Access to AGO Products and Services may be rescinded for failure to provide such notice.
- Create a password in compliance with the AGO password criteria set forth below. The AGO reserves the right to change the password criteria from time to time. Compliance with the AGO password criteria will be enforced via automated password authentication or public/private keys with strong pass-phrases. The AGO password criteria are as follows:
  - Minimum 12 characters,
  - Must include 3 of the 4: a-z, A-Z, 0-9, and special characters,
  - Passwords will require being reset based on level of access at the AGO's discretion,
  - Passwords must be kept securely by the account owner, and never be shared,
  - Passwords must not contain sequences 01, 123, abc, etc.,
  - Passwords must not contain properly spelled dictionary words, and
  - Passwords must not be directly identifiable to the user (e.g. social security number, date of birth, spouse's name, username, etc.).

  Password history will be retained for 24 changes to ensure unique passwords. Inactive accounts will be disabled at 90 days, and removed at 120 days. Users of accounts that reach 120 days of inactivity must reapply for an account.
- Comply with all federal, Ohio and any other applicable law, including, but not limited to: Internal Revenue Service Publication 1075 which is based on United States Code Title 26, Section 6103; Ohio Revised Code Chapter 1347; the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and the associated omnibus rule to modify the HIPAA Privacy, Security and Enforcement Rules; and the Health information Technology for Economic and Clinical Health ("HITECH") Act.
- Comply with all applicable contracts and licenses.

USER'S UNDERSTANDINGS:

- User understands that any Users who engage in electronic communications with people or entities in other states or countries, or on other systems or networks, are on notice that they may also be subject to the laws of those other states and countries and the rules and policies of those other systems and networks. Users are responsible for obtaining, understanding, and complying with the laws, rules, policies, contracts, and licenses applicable to their particular uses.
- User understands that the AGO retains the right, and has the capability, among other security measures, to review, audit or monitor the User's directories, files, e-mails (both sent and received), as well as Internet usage to ensure maintenance of system integrity. User also understands that User's access to the Products and Services is subject to termination for breach of this Policy at any point.
- User understands that, among other security measures, the AGO makes backup copies and stores User information. User activities are therefore not private and User content is potentially stored on AGO servers. User also understands that the AGO is subject to public records disclosure and to discovery requests and that User's activities and information may be released pursuant to a public records or discovery request.

PROHIBITED ACTIVITIES:

- Users shall not engage in illegal, fraudulent, or malicious conduct on or while accessing any AGO Product or Service.
- Users shall not provide an AGO Product or Service login or password to any person or entity for any reason.
- Users shall not leave a computer unattended that is connected to AGO Products or Services for any period of time unless it is secured in such a way that the computer cannot be accessed by any other individual (e.g. sign-off procedure, password protected screen saver, etc.).
- Users shall not engage in conduct on or while accessing any AGO Product or Service that is beyond the scope of the User's AGO authorized access, including access governed by a Memorandum of Understanding, contract or retention agreement, if applicable, for which AGO access is granted.
- Users shall not monitor or intercept the files or electronic communications of AGO employees or any other third parties.
- Users shall not attempt to test, circumvent, or defeat the security systems of the AGO or any other organization, or access or attempt to access the AGO's or any other organizations' systems without prior authorization from the AGO.
- Users shall not provide anyone access to AGO Products and Services.
- Users shall not provide anyone access to or disseminate any AGO information, regardless of whether or not it is considered confidential or public, and regardless of how the information was obtained, without prior authorization from the AGO.
- Users shall not make paper, electronic, or any other copies of any AGO information, regardless of how the information was obtained, without prior authorization from the AGO.

User Acknowledgement

By signing below, you, as a User, acknowledge that you have read and understand this Policy, and you, the User, agree to comply with the terms of this Policy.

Printed Name of User: _____ Title: _____

User's Employer: _____ Contract End Date: _____

User's Phone Number: _____ User's E-mail: _____

Requested Period of Access:
From: _____ To:_____

Application or resources requested:

(FTPS, Edisp, Livescan, etc.): _____

_____

Public IP: _____

User's Signature: _____ Date: _____

Account Identity Control Information (1): _____ (mother's maiden name, etc.)

Account Identity Control Information (2): _____ (first car owned, etc.)

The above Account Identity Control Information will be used to identify you in the event that you have lost or do not remember your account ID or password. The User must provide two unique pieces of information as a shared secret with the AGO to verify your identity when account resets and other services that require identity verification are needed. It is the User's obligation to provide and secure these shared secrets in the same manner that is required for account credentials.

Employer Acknowledgement

By signing below, you, as the User's employer, acknowledge that you are a duly authorized representative of the User's employer able to bind the employer to the terms of this Acknowledgement. By signing below, you, as the User's employer, also agree that access by the employer may be rescinded at the discretion of the AGO, with prior notice, if the employer fails to take reasonable precautions, as defined above, to avoid a breach of this Policy and/or to ensure that the employer's Users do not breach this Policy.

Printed Name: _____ Title: _____

Employer's Signature: _____ Date: _____

Employer's Phone Number: _____

Employer's E-mail: _____

Official AGO Use Only:

AGO ITS Work Order Number: _____

AGO issued username: _____

AGO issued rights: _____

_____

AGO Chief Information Officer, Chief Information Security Officer, or their designee

Printed Name:_____ Title: _____

Signature: _____ Date: _____

Comments: _____

_____

_____

_____

_____

_____

_____