RESOLUTION NO. 466

ADOPTING THE RENSSELAER COUNTY BUSINESS ANALYSIS AND RISK ASSESSMENT FOR ACCEPTING ELECTRONIC SIGNATURES ON CONTRACTS, AMENDMENTS AND MEMORANDUMS OF UNDERSTANDING

Introduced: 8/12/24
By Law Committee:

WHEREAS, The County Executive has requested authorization to adopt Rensselaer County's Business Analysis and Risk Assessment for Accepting Electronic Signatures on Contracts, Amendments and Memorandums of Understanding in order to allow Albany County to execute contracts with electronic signatures, and

WHEREAS, 9 NYCRR § 540.4(c) allows a governmental entity to elect to adopt an existing business analysis and risk assessment completed and documented by another governmental entity when selecting an electronic signature for use or acceptance in the same type of electronic transaction to which the existing business analysis and risk assessment applies, now, therefore, be it

RESOLVED, By the Albany County Legislature that the Rensselaer County Business Analysis and Risk Assessment for Accepting Electronic Signatures on Contracts, Amendments and Memorandums of Understanding is hereby adopted in order to authorize the use and acceptance of electronic signatures and electronic records in the contact of executing contracts; give e-signatures and e-records the same force and effect as ink/wet signatures and paper records; authorize e-delivery of contract records to vendors; and authorize and recognize e-records as original and official contract records, and, be it further

RESOLVED, That the Clerk of the County Legislature is directed to forward certified copies of this resolution to the appropriate County Officials.

October 14, 2016

ELECTRONIC SIGNATURES AND ELECTRONIC RECORDS

Business Analysis and Risk Assessment For Accepting Electronic Signatures on Contracts, Amendments and Memorandums of Understanding (MOUs)

Rensselaer County

Human Services Cabinet

October, 2016

October 14, 2016

A. GENERAL INFORMATION

This document presents an analysis and risk assessment for the acceptance and use of an electronic signature (e-signature) and electronic record (e-record) solution for contracts let by the Human Services Cabinet (HSC) departments which include, Aging, Employment and Training, Health, Mental Health, Probation, Social Services and the Youth Bureau. These departments contract with outside vendors to provide a wide range of human services throughout Rensselaer County. The previous contract execution process used involved the manual routing of contracts for review, approval and collection of signatures. To streamline this process, reduce duplications and improve efficiencies, in 2015 the County invested in software designed to automate the entire contract creation and execution process. The contract management software includes an e-signature solution. The HSC is seeking approval to accept e-signatures and maintain e-records of all activities associated with contracts created in the Contract Management System (CMS). Pursuant to New York State's Electronic Signatures and Records Act (ESRA) guidelines, the Human Services Cabinet has completed its analysis of the manual contract creation and execution process, and evaluated the potential risks of using e-signatures and maintaining electronic files as official contract records. The findings of the analysis and risk assessment are set forth below.

Since 2015, over 615 contracts and amendments have been set up and routed through CMS.

B. PURPOSE

The business units of Rensselaer County government contract with non-profits organizations, and public and private sector entities to provide a wide range of human and professional services to address the needs of Rensselaer County residents. The purpose of this project is to determine whether signatures are required for executing contracts and to determine whether the recommended e-signature approach is sufficient for the specific business function--contract execution. Ultimately, this document provides sound business reasons for implementing e-signatures and e-records and for giving e- signatures and e-records retained in the CMS, the same validity and effect as handwritten signatures and paper records.

1. Analysis of Legal and Business Requirement: In New York State, the execution of a contract is governed by State and Municipal Law. Rensselaer County requires a written signature on contracts and agreements. Under the previous manual contract execution process, original handwritten signatures were required for contracts to be legally binding and enforceable. Signatures, on paper contracts, document authentication and approval, demonstrate intent, protects against fraud, and repudiation. The New York State ESRA Act and the Federal Electronic Signatures in Global and National Commerce Act (E-SIGN) make e-signatures legally binding, with the same legal force and validity as handwritten signatures.

Prior to the launch of CMS, contracts activities were largely manual, requiring original signatures on two contract paper copies. Under the manual process, once the required steps for executing a contract are completed, original signature copies are transmitted to the Auditor and the vendor for record retention. Pursuant to existing County and State statues or regulations, transitioning the manual contract functions to an electronic process requires an e-signature and e-record solution. Analysis for determining whether an e-signature is required for executing contracts electronically is summarized in the Table A.

Assessment of Whether E-Signature is Required

Table 1

Situation/Context	Signature Required by Law or Regulation Governing Transaction	Signature NOT Required by Law or Regulation
There is a need for emphasizing the significance of the transaction.	Electronic Signature Required	Electronic Signature Required
There is a need to bind a party to a specific intent or transaction.	Electronic Signature Required	Electronic Signature Required
There is a need for the parties to attest to the accuracy of the information, agree to certain conditions, and /or that they read and understood the related documents.	Electronic Signature Required	Electronic Signature Required
Notarization is Required	Wet/Print Signature Required	Original Print Signature Required
All Other Transactions	Electronic Signature Required	Electronic Signature Optional or Not Needed

As Table 1 shows, an e-signature is required to emphasize the importance and formal nature of contracts, and gives the signing parties a signal that they are entering into a legally binding transaction. It is important that all parties to the contract understand the nature and importance of the transaction.

The contract execution transaction involves an intent element (contract, agreement, acknowledgement approval, receipt, etc.), therefore, a signature is useful and helps formally bind a party by signing and approving the document, and makes the document enforceable. By entering a Username and password, and clicking the "I Accept" button, authorized signees acknowledge reading and understanding the content of the Electronic Submission Notice, located on the login screen. Therefore users understand that an electronic document has the same legal weight as a paper document and the authorized signee fully understands intent when clicking the "I Accept" icon. *Finally predefined tasks are generated through an Approval Routing Modular. When authorized signees log into CMS to approve/sign a contract, the user will see a highlighted banner with his/her name and the task that must be completed. This control prevents authorized users from denying that the electronic transaction ever took place. It also safeguards against users denying awareness that they were signing a contract. Authorized signees login to CMS with contracts waiting for their signature will see a banner instructing them to approve and sign contract. This is another control that ensures intent and vendors are aware they are signing a legal document. An audit trail documents, time and date stamp every action.

2. **Analysis of Those Who Will Use Electronically Signed Records:** User friendly and easy to navigate, a username and password are required to access CMS. Access is through an Internet browser. Once online, users can easily access CMS from anywhere, and create, review, approve, monitor and execute contracts 24-hours a day.

During 2015 and 2016, the County rolled out CMS automating the contract execution process, and requesting vendors contracting with HSC departments to generate and execute contracts electronically. To date, both print and the electronic versions are retained; the print copy is transmitted to and stored by the Auditor. **Once the Legislature passes a resolution recognizing e-signatures and e-records as legally binding and equivalent to handwritten signatures and paper copies,** the goal will be to transition to only electronically signed contracts. E-contract records will be available and accessible any time to individuals registered and set up as authorized CMS users. Once fully transitioned to an electronic solution, original signed contracts will no longer be required for the Auditor's Office; the executed contract e-record will be stored in CMS as the official record, accessible to internal and external CMS users 24/7.

Pursuant to ESRA and E-Sign, the use of e-signatures must be voluntary and never mandatory or required in order to obtain a service from the Local Government Unit (LGU), conduct a business transaction and/or enter into a legal agreement or contract. Vendors wishing to opt out of using CMS may submit paper copies of contracts with original signatures. Written notice is required from the vendor, which is uploaded under the vendor's profile. The County will upload and route the contract in CMS for internal review, approval and execution. A paper copy of the fully executed contract will be returned to the vendor by mail and the executed contract e-record will be retained in CMS.

3. **Determination of Interoperability & Intrusion:** The e-signature solution is compatible and interoperable with Rensselaer County's existing technology systems. From the onset of this project, the County's Bureau of Research and Information Services (BRIS) was integrated into the RFP team and played a critical role defining the County's system network specifications in the RFP. Also BRIS reviewed the subsequent Proposal submitted by the consultant to avoid network system issues once the CMS software was launched and reviewed and provided advisement on the consultant's contract and deliverables. BRIS and project manager collaborated with the consultant on system requirements, security protocol, including technical requirements to provide assurances that the CMS software satisfied the County's network requirements. CMS application is web-based

therefore, internet access is required. County users must log into the County's network to access the internet. CMS is a hosted database managed offsite, with the ability to be accessed from remote locations and facilitate the use of many simultaneous users. Both the County and the software consultant provide strict cyber-security protocols. Both have strong security practices in place. BRIS reviewed the consultant's proposal and concurred with steps taken to guarantee the system-to-user interface would be designed in a way that provide ease of system navigation among system users. Furthermore, the CMS software program incorporates the use of Software as a Service (SaaS) e-signature authentication model. This model allows users to automate, send, sign and return contract documents inside one program.

The consultant provides onsite monitoring of CMS 24/7/365 to ensure business continuity and to make certain the entire website is always available to users and operating properly. **With these checks in place, the probability of intrusion by outside parties is low.**

C. PROJECT SCOPE

Functionality would be the creation and maintenance of the e-signature and e-contract record, storage of e-contract records, and e-delivery to vendors/users of e-contract records. The scope of this analysis and risk assessment is limited to contract records under the departments and offices composing the Human Services Cabinet.

Overview of Business Process

1. Pre-CMS Contract Execution Business Process: The County solicits contract proposals by sending out budget call letters to nonprofits, private consultants for the provision of a wide range of human and professional consultant services. Processing timely and accurate vendor contracts manually has been challenging. The lack of uniform standards, consistency in boilerplates, performance measurement and output data and transparency across the departments was common. Contracts for each agency differ in language and format. While some of these issues may be dictated by funding sources, some are copyediting and formatting issues. CMS offers an opportunity to clean up and copyedit contracts and boilerplates for grammar and typos. Also, it presents an opportunity to professionalize the look of our contracts and boilerplates by copyediting for typos and grammar and standardizing format to provide consistency. Prior to 2015, each department maintained its own contract database, which was accessible to limited users within the department. As each office retains its own paper or scanned copies of contracts, transparency and accessibility to documents and specific information about contractual commitments and work scope were generally limited within each separate department, rather than across the various functional units comprising the human services departments.

2. Post-CMS Implementation: HSC set out to implement changes to meet challenges by introducing technology to the contract creation and execution function. Since its implementation in 2015, CMS has improved efficiencies with the administrative and support tasks associated with creating and executing contracts. As of October 2016, over 530 users and 15 county departments and offices have been set up in CMS, including the Office of the Auditor, Budget, BRIS, the County Attorney, and Purchasing/Central Services. Since its 2015 implementation, over 600 contract records and 518 unduplicated vendor records have been created in CMS. In 2015, 298 contracts were processed through CMS (14 were 2014 contract documents): in 2016, that number increased to 308 contracts. Nearly 500 contracts were created routed and successfully executed in CMS since 2015!

There are multiple benefits to implementing an electronic contract execution solution. Currently, CMS permits transparency across the department heads, and the inter-departmental collaboration of the HSC contracts. Through CMS, users have a **secure,** computer-generated, time and date stamped audit trail that documents independently the date and time of users entries, including specific contract activities to develop, review, track, retrieve and renew contracts online, in real time, in a singular digital portal at http://rensco-contracts.com/login.

The e-signature feature in CMS is subjected to two layers of security controls. Once at the site, users click on the Electronic Submission Notice link. This notice clearly spells out intent. It also directs authorized users to read and agree to abide by the provisions of documents, which became part of the resulting contract record. By entering a User ID and a personal password, CMS users acknowledge reading and understanding the Electronic Submission Notice by clicking the "I Accept" button. In addition, contracts are set up with tasks identified in the Approval Routing Modular that show intent. Once activated, a notification is generated to each person associated with the contract describing the task that must be completed. For example, the Authorized Signatory of record receives a notice that a contract is waiting for approval. Once logged into the system, the individual will view a banner describing the task that must be completed. The banner description also clarifies intent. Secondly, a Click Through feature enables users to approve the contract document. **Every transaction, process step and e-mail communication is time-stamped, tracked and linked to the contract record. Vendors review, approve and move contracts to the next routing step in the Approval Routing Modular.**

3. Cost of Implementing E-Signatures and E-Records: In terms of the fiscal impact of transitioning from a paper to electronic environment for creating, routing and executing contracts under the purview of the HSC departments, and offices, the current and future cost is minimal. In December 2013, pursuant to Resolution Number G/626/13, the County Legislature authorized the County Executive to enter into a contract for the installation of contract management software purchase the CMS software application. The resolution included the e- signature feature as part of the contract scope. To date, the vendor has received the total contract amount of $39,500 for installation, training and rollout of CMS. The Resolution also authorized a total of $15,000 payable annually for three years for annual software maintenance and the availability of Help Desk assistance. So far, the vendor has been paid a total of $10,000--$5,000 for 2015 and 2016. The balance of $5,000 will be invoiced and paid in January 2017. At this time, with the exception of the cost of personnel required for performing contract execution related tasks, there is very little future costs involved in executing e- signatures on contracts. Conversely, the savings for implementing E-signatures are outlined under the heading, Benefits of E-Signatures and E-Records.

D. PROJECT REQUIREMENTS

A legislative resolution is required to give e- signatures and e- records the same legal validity and force as traditional paper-based handwritten signatures. Plans are underway to prepare a resolution for the October 11 Legislative Meeting Agenda. To meet this timeframe, the legislative resolution and fiscal impact statement must be prepared and submitted to the County Attorney's Office and Budget before but no later than September 20.

Specifically, the resolution language shall: a) authorize the use and acceptance of electronic signatures and electronic records in the context of executing contracts; b) give e-signatures and e-records the same force and effect as ink/wet signatures and paper records; c) authorize e-delivery of contract records to vendors, and d) authorize and recognize e-records as original and official contract records. The resolution will be limited in scope to the use of e-signatures and e-records

on contracts under the purview of the Human Services Cabinet departments and offices. However, if approved, this risk assessment and business analysis may be considered for contracts under other County departments, or similar types of transactions requiring handwritten signature.

E. BENEFITS OF E-SIGNATURES

The use of e-signatures and e-records can significantly speed up cycle/transaction time for executing contracts. Furthermore, it improves productivity, reduces costs for paper and for office equipment to file records, simplifies transactions and overall, enhances customer satisfaction. Recent Federal and State laws encourage and allow government agencies the authorization to use and accept e-signatures to authenticate e-records. Until the Rensselaer County Legislature enacts the use of e-signatures, vendors and users operating within the CMS environment are required to use a dual electronic and print/original signature contract approval process and retain an electronic copy and one paper copy of the contract.

Instead of reducing county staff and vendors staffing resources spent executing contracts, speeding up the cycle/transaction time, and reducing cost associated with executing and filing paper contracts, the required dual electronic and manual contract process is inefficient, cumbersome, and has produced the exact opposite effect of an e-signature solution of slowing down the entire contract execution process and generating paper.

F. TRANSACTION RISK FACTORS TO E-SIGNATURE, E-RECORD BUSINESS SOLUTION

With respect to each challenge to the enforceability of an e-signature, the risk assessment conducted followed steps in the NYS IT Guidelines for the ESER Act.

Risk Determinations

Three determinations were made for each process during the risk analysis:

- The importance of knowing the identity of the person who holds the ability to sign
- The importance of assuring that the individual who signed/approved the contract, was in fact the holder of the authorized signature set up in CMS
- The importance that the document was unchanged since it was signed

The following provides rationale and justification of how CMS meets each of these requirements.

1. <u>User Name and Password Required</u>: To access CMS, users must be registered and set up in CMS. A user name and password are required to login to CMS. Once registered, the Help Desk generates a username and temporary password to the user's e-mail address, along with the hyperlink to CMS' login screen. The username and password are both required, and are under the sole control of the person using them. Both the user name and password are linked to the contract record. CMS has the ability to identity users through their username and password and Determine whether the individual approving a contract is the authorized signee of record in CMS. Authorized signees are set up under the vendor profile screen. A written memo or email is required from vendors wishing to add other authorized signees. This correspondence is uploaded and stored in CMS under the vendor's profile.

2. <u>CMS Creates an Audit Trail</u>: Throughout a contract's lifecycle, every activity, document, communication of transmission and process steps are time stamped and an audit trail captures the date of user entries, including actions that create, modify or delete e-records, and messages. The

audit trail is retained for a period at least as long as that required for the paper record and may be made available, as needed upon request.

Process steps are clearly defined for each person with a role in the contract's approval. Each step has a desired action or result. Controls are set up in CMS make it impossible for an e-signature to be applied to a document without the signer having been informed that a signature is being applied. Upon logging in to CMS, the authorized signee will see a banner with instructions such as "Sign and Approve Contract and Return Print Copy to the Attorney's Office." This language demonstrates intent. The signee is asked to click a button to demonstrate intent or agreement to the contents of a document. This security method is called Click Through or Click Wrap. CMS allows the signer's intent to be expressed as part of the record and linked to the signed contract record. CMS records the date, time and fact that the signer indicated his or her intent.

The business transaction involves the acceptance, approval and signing of contract documents. In that a contract is a legal document, it is important that the signature is indisputably linked to the originally authorized signee on record in CMS. In addition, after contract negotiations are concluded, it is important to ensure that the final and signed contract is not altered. Steps to mitigate these concerns are discussed below.

3. **Likelihood of a Challenge to the Signature is Low:** Generally speaking, vendors and HSC departments' have long-term, ongoing contractual business relationships with County public services departments and are in good standing with these agencies. Contracts with vendor agencies are typically renewed annually. One department must amend vendor contracts each year due to the different timeframes of the State and County budget cycles. The initial contract amounts are usually based on the previous year. Once the State budget is enacted, if there is an increase in vendor appropriations, the contracts are amended to reflect the increase. This is part of the process and vendors have a clear understanding of contract procedures and processes.

A vendor would have very little to gain from forging a signature on contract. If this occurred, there would be two entities affected--the vendor organization and citizens who services may be affected until the situation is investigated. The likelihood and risk of someone forging the signature is relatively low. The names of authorized signee(s) on contracts are included under the vendor's profile screen. There is no financial gain to an individual as vendor claims are payable to the organization and checks are mailed to the address on file.

The likelihood of a legal challenge to a contract is low. In that vendors are required to identify the authorized signee for contracts, which is documented in the vendor profile e-record, the likelihood of forgery and the level of harm that would be caused if a forger were to e-sign the contract is low. If the person who approves and e-signs the contract differs from the authorized signee listed in CMS, this would raise a red flag and the department contract liaison would be responsible for reaching out to the agency. Vendors may add others as signees, but must submit a written request through CMS or via e-mail, which is uploaded to the vendor's profile e-record.

Further, controls in CMS show the identity and location of active users in the system. This includes an identifier traceable to a particular individual such as a user ID and password and proof that the submitting or approving individual is the person registered in CMS, as the organization's authorized signee. Moreover, the system can identify the source of transmissions--e.g., mail server id, e-mail account name, time-date stamped, and Internet Protocol address.

4. Risk of Unauthorized Alteration or Other Compromise to E-Record: The likelihood of challenges to the enforceability of an e-signature on contract documents due to a security intrusion or breach to the transaction or stored record is low. Typically, the content of contract documents are worked out before uploaded in CMS. When the County is the vendor the other party to the contract is responsible for preparing and submitting a draft the contract to the designated department contract liaison for review and approval by the County Attorney. Once negotiations are concluded and the contract finalized, it is uploaded in CMS and routed for approvals.

Mitigating Controls

First, to mitigate the risk of a person attempting to repudiate an e-record bearing that individual's e-signature, the system establishes an audit trail of all actions associated with the contract record, any alterations to the contract record, the date, time they were made, the identity of who made the alteration, and the location where the change were made. In addition, vendors must provide written documentation identifying persons authorized to sign on behalf of vendor and bind the agency contractually. These signees are identified in CMS. The vendor may authorize more than one person to sign on behalf of the agency. This information is captured in the Vendor profile screen.

Secondly, the e-signature is linked to the respective contract e-record throughout its lifecycle and retained according to the records retention schedule, which is generally, six (6) to nine (9) years. Once a contract is signed by the vendor and approved to form by the County Attorney, the contract is locked, prohibiting any further modifications. Once the contract completes the approval and execution process, the County Attorney's Office e-delivers a PDF e-record of the contract to all persons connected to the document.

A third mitigating control is the restriction of user access to certain information screens in CMS and entry of data such as contract amounts and terms is limited to County HSC contract employees. This information cannot be changed by users with limited access. The Bureau of the Budget and the County Attorney reviews and verifies information in CMS including the contract amount, budget and funding codes, insurance certifications and legislative resolution authorizing the contract and funds. **These multiple review and approval levels in the contract execution process increase the integrity of the information and data. These controls tend to make deception more difficult to initiate and sustain.**

In Rensselaer County signatures are legally required from the parties to the contract. The contract cannot be executed until all signatures are collected. In the case where a signature is legally required, without the signature of all parties to the contract, the enforceability is greater.

5. Electronic Delivery (E-Delivery): ESRA and ESIGN recognize that Local Government Units (LGUs) may satisfy the delivery legal requirements by providing e- records but the required sequence of steps must still be met. This is achieved by setting up the sequential steps necessary for reviewing, approving and executing a contract in the Approval Routing Modular. The contract may be e-delivered to the vendor and returned electronically. The audit trail captures all actions and information associated with the document transmission.

6. Access to E-Records & Management & Retention of E-Records: E-records created in the transaction of public business are public records and subject to the Public Records Law and need to be retained according to a records retention and disposition schedule. The shift to e-signatures on contracts will have the effect of creating a higher volume of e-records to maintain and

store, as automating the contract management and execution process transfers previously paper generated contracts, MOUS and agreements, to e-records. These e-records are actually original official documents subjected to the Freedom of Information Act.

Therefore, E-records are preserved in a format that makes the information easily accessible and useable to all persons who are entitled by law to access such records. For this reason, in CMS, E-records are capable of being easily retrieved in a timely manner. Towards that end, contracts e-records may be searched by a number of attributes including by year, vendor name, and contract name. The e-signature is part of the e-record and linked to it throughout the e-record's lifecycle including storage after the execution has been completed. The e-signature remains associated with the e-record for as long as the document must be retained according to the retention schedule. The e-record typically includes the contract document, and all attachments or exhibits, agency forms, questions and responses, messages, certifications and instructions--all permanently linked to the contract e-record. An audit trail captures every activity of the sender and receiver of the e-record, showing all alternations, the date and time they were made, and identification of who made them.

Registered users may access contract records anytime by logging in to CMS, print them and store the e-record. The County will comply with all laws applicable to traditional paper government records--at the county, state and federal levels that require e-records that must be signed by electronic means, including public records and records retention laws.

Included in this analysis and assessment is information on the type of data that will be collected and stored in CMS. **Table 2, Risk Assessment and Mitigation Steps,** captures and summaries information on risk, risk level and controls in place to mitigate risk**. Table 3, Privacy Impact Assessment,** describes the type of data that will be collected and stored in CMS, identifies third party sources that information will be collected from, type of information collected from individual users in CMS, and information on records retention schedules and disposition. **Table 3, Access to CMS Data**, answers questions about who will have access to data and describes different user levels and restrictions, and disclosure under FOIA. This assessment was completed to show that personal identification information is generally, not collected or stored in CMS. The collection and storage of personal information is limited in CMS to only independent consultant contracts. Typically, the consultant's personal e-mail address, mobile and land phone numbers, and home address are entered and stored in CMS. However, this applies to a very small number of contracts. While Employer Identification Numbers (EINs) of vendor agencies are entered in CMS, social security numbers of independent consultants are not.

G. SUMMARY AND CONCLUSION

Based upon the above analysis, it is concluded that the County HSC should proceed with developing a legislative resolution and fiscal impact statement for submission to the County Legislature to accept e-signatures and e-records in the contract creation, review and execution function.

It is important to ensure our users that CMS will not introduce dramatic changes into the current work practice process, as the software application is designed to mirror the manual contract approval and execution process but perform contract management tasks more efficiently. Before transitioning to the electronic process, vendors had to provide a handwritten signature on paper copies of contracts. With CMS, vendors are required to approve contracts in the CMS platform environment, **and** manually sign a paper/print copy of the signature page, which is then returned to the County Attorney's Office to complete the contract approval and execution steps.

If the act of signing a contract becomes a more complicated process, it is assumed that the heads of vendor agencies, who generally are authorized signees, would be less willing to use the system themselves and may engage their assistants in the process of signature collection. The acceptance of e-signatures would eliminate this concern, as the contract e-record would be e-delivered to the authorized signee with the process step clearly identified and highlighted in a banner format. Almost instantaneously, a vendor can approve, sign and move a contract to the next process step in CMS.

In that the likelihood of identifiable risks occurring is low, the potential impacts from such risks are equally low. CMS is a secure, computer generated software application that is accessed through an Internet browser over the County server. We are confident that sufficient and adequate controls are in place to safeguard the system from threats and which also address any potential vulnerabilities. The processes set up in CMS for creating and executing contracts also have strong controls in place that provide a high level of assurance of the integrity of the e-signed record and controls aimed at detecting unintentional or malicious alteration to e-records.

The identified management risks are equal for electronic or paper contract solutions. Users must be registered to access CMS and a user ID and password is required to login to the system. When users go to the login screen they will see information about the contract management system process. Users are prompted to read and acknowledge the Electronic Submission Notice. By entering their username and password and clicking the "I Accept" button, users acknowledge reading and understanding the content of the Electronic Submission Notice on the login screen.

Users understand that an electronic document has the same legal weight as a paper document and the authorized signee fully understands intent when clicking the "I Accept" icon. This control prevents authorized users from denying that the electronic transaction ever took place. It also safeguards against users denying awareness that they were signing a contract. Authorized signees login to CMS with contracts waiting for their signature will see a banner instructing them to approve and sign contract. This is another control that ensures vendors are aware they are signing a legal document. Below is the signature attestation included in the Electronic Notice located on CMS login screen:

"By submitting a contract and related documents electronically through the Purchasing Contract Management System, it is unnecessary to forward any materials to the office of Purchasing and Central Services. However, by submitting electronically, the applicant agrees that:

- The application is made with the full knowledge and consent of the official authorized to enter into contracts on behalf of the municipality or agency (vendor).
- Upon receiving a contract electronically, the vendor shall comply with all applicable federal, state, and local statutes, rules and regulations.
- The contract will be developed based upon the information gathered in the contract building process and contained within the final contract. The fully executed contract and related documents are the only documents binding on the parties.

Before any contract is entered into by a municipality or agency (vendor), the authorized signing official should read and agree to abide by provisions of the following documents, which become a part of resulting contracts."

Vendors are responsible for self-identifying authorized signees in writing, which become part of the vendor profile e-record. These individuals are set up as system users and identified in

CMS as authorized signees. Any user generating contracts under the vendor will have access to information and all documents uploaded to the vendor screen.

As the Risk Assessment states, an audit trail captures every activity, document, communication of transmission of documents, messages, the date and time of users' entries including actions that create, modify or delete electronic files. It captures the entire contract approval routing, who reviewed and actions taken, all date and time stamped.

Both the County and the Consultant C&C follows strict cyber-security guidelines, has proper firewalls and multiple security practices in place. The C&C Security Plan involves as strict 5 Tier Approach to data and information security. Their disaster recovery plan utilized two geographically different remote locations where the servers reside.

Many of the businesses that contract with HSC departments and offices have had ongoing, long-term contractual business relations. Generally, contracts are typically renewed each year and contract amounts are contingent typically on State funding sources. Vendors are very aware of the contract processes and procedures. Many have already registered as CMS users. There is very little to gain from a vendor forging a signature on a contract or denying e-signing the contract e-record. The likelihood of both is very low as doing so would significantly delay payment to a vendor and in some instances, have a damaging effect of the organization's cash flow. Additionally, in that vendors must identify authorized signees on contracts, it is fairly easy to discern whether the signee is authorized to bind the agency contractually.

Risk Assessment
Table 2

The following risks of using e-signatures and e-records in the contract creation, delivery, review, and execution are listed below and the steps to mitigate the identified risks are also listed

RISK	RISK LEVEL & MITIGATION STEPS
SIGNER AUTHENTICATION RISK: The process and procedures used to authenticate the signer and thereby, establish a link or association between the signer and the information and method used to sign. The process established confidence in user identities and assurance that the document truly comes from the signer.	**Risk Level: LOW Controls in place to assure that the asserted identity is accurate.** *Mitigating Steps* **1.** Generally, most vendors have long-term contractual relationships with HSC departments and are in good standing with the County. They understand the contract procedures and processes. A vendor has little to gain from forging an e-signature on a contract and much to lose including loss of grant funds, therefore, the likelihood of this occurring is low. **2.** CMS is a secure, computer software application that is accessed via the Internet. Only registered users can access CMS. A user id and password are required. **Vendors are required to designate the person(s) authorized to sign contracts on their behalf.** Authorized to signees are set up in the Routing steps. Once logged in the CMS, the users will see a banner message with instructions of the task that must be completed, for example, "Sign and approve contract." Once the signee completes this task, the contract moves to the next step in the approval routing process. **3.** Controls in CMS show the identity and location of active users in the system. This includes an identifier traceable to a particular individual such as a user ID and password; and proof that the submitting or approving individual is the person registered in CMS as such. As well, the system can identify the source of the transmission -- mail server id, e-mail account name, time-stamped Internet Protocol address. **4.** An audit trail captures every activity, document, and communication of transmission of documents, messages, the date and time of users' entries including actions that create, modify or delete electronic files. The e-signature is linked to the respective contract's e-record throughout its lifecycle and retained according to the records retention and disposition schedule.

Table 2 Risk Assessment - Continued RISK	RISK LEVEL & MITIGATION STEPS
REPUDIATION: This is the method used to ensure the signed record is in the original form, without modification, as signed by the signee. Repudiation addresses the level of assurance regarding the integrity of the signed record. Used to escape accountability. Signer claims "I didn't sign the document."	**Risk Level: LOW -- Level of Assurance is High Controls are in place to detect unintentional or malicious alteration to e-contract. Agency might expend staff efforts to resolve.** *Mitigating Steps* **1.** The Secure Hash Algorithm--SHA-256 is a **high** level encryption certification used in CMA. SHA-256 is used to verify data integrity. Designed by the National Security Agency SHA-256 is the industry's standard and is a secure hashing algorithm certificate. It provides high assurance, by comparing hashing functions, it determines data integrity and show if downloaded data has been modified or tampered with. The Security Plan involves a strict 4-tier approach to data and information security. **2.** An audit trail captures the entire contract creation, review, approval, and execution process. Only persons registered and set up in CMS can access the system. E-mail addresses are provided by the vendor agencies. Once a contract is signed by the vendor and approved to form by the County Attorney, the contract is locked, prohibiting any further modifications. Once the contract completes the approval and execution process, the County Attorney's Office e-delivers a PDF e-record of the contract to all persons connected to the contract. **3.** Another control is the restriction of users' access to certain information screens and inability to enter data reduces the likelihood of information being altered and tampered with. For example, certain information may only be entered by HSC contract staff and the System's Administrator. The e-signature is linked to the respective contract e-record throughout its lifecycle. **4.** The multiple review and approval levels in the contract process increase data integrity. Contract amounts, funding and budget codes and legislature resolution authorizing funding are reviewed and verified by the Bureau of the Budget and Legal. A review of insurance certificates is completed also by Legal staff to ensure that the insurance coverage requirements are met. **These multiple reviews tend to make deception more difficult to initiate and sustain.**

Table 2 Risk Assessment - Continued RISK	RISK LEVEL & MITIGATION STEPS
System Unavailability and Access to CMS **Threat Source: Power Failure,** Network Failure, Software Failure, Capacity Constraint, Internet Unavailable, Act of God. **Category of Harm:** Inconvenience, would affect productivity as users will not be able to access the system to process to perform contract related tasks. **Impact of Harm:** Low	**Risk: Low to Moderate as some risk factors are unpredictable and out of our control.** 1. Both the County and C&C follow strict cyber-security guidelines and have controls in place to guard against intrusion and system unavailability due to outside parties. Both have proper firewalls and strong security practices in place. In that CMS is accessible via the Internet, users on the County servers may have a higher likelihood of system unavailability due to network issues than individuals on the State servers. However, BRIS has been implementing steps that may adequately address system disruptions. **2.** CMS is a SaaS approach. The servers are located in two geographic different areas of the U.S. and backed up to another remote location. Technicians are physically available 24/7/365 to handle application specific issues. Bandwidth is monitored daily. Redundant power supplies and network infrastructure ensure Internet traffic is never interrupted. Finally, as part of the maintenance scope, controls are in place for monitoring the software traffic, servers are scanned daily for malicious software/worms and allows for security and operating system fixes and patches. **3.** Once signatures are collected and contracts executed, CMS generates notification that the contract is executed and the e-record is available. Vendors have access to the e-record anytime by simply logging in to CMS. E-records are retained according to the records retention/disposition schedule. The servers are perpetually backed up. After the contract retention period expires, the contract would be deleted but the process used by the consultant for backing up files, involves encrypting and storing the files in an off-site **location for one additional year beyond the records disposition schedule. Essentially, C&C's backup policy is the retention of all active data indefinitely but once data is deleted, it is removed from the archives after 1 year.**

Privacy Impact Assessment
Data in CMS

Table 3

Question	Response
Describe all information to be included in the system, including personal data.	CMS is used to process contractual information and execute contracts. Information retained in CMS includes: vendor names and contact information including :vendor address, names of authorized signees, and all users email addresses, Employer ID Number, phone numbers, and insurance certifications . This same information is collected from individuals with professional services contracts. Typically, the home address and personal mobile numbers and emails are collected and stored as part of the contract record on professional services contracts. **Social Security Numbers are never collected and stored in CMS, although EINs are entered in the system.** Department, employee name, and contact information. Account and Budget Fund Codes, Resolution Numbers, Resolutions, Contracts and associated contract documents. Annual Budget and Funding Application Forms. Messages sent through CMS.
What stage of the life cycle is the system currently in?	Operational/Maintenance
What are the sources of the information in the system?	Data available in CMS is provided by Rensselaer County employees involved in any aspect of performing contract creation, approval and execution functions. Other information is provided by vendors who have contracts in CMS and have chosen to use the electronic services provided by CMS to execute contracts. Vendors provide username, email address and access the system by entering a password and username. On occasion, outside auditors are set up users to review vendor contract records.
What State and local agencies are providing data for use in the system?	Youth Bureau uploads NYS OCFS Annual Resource Allocation Plan and NYS Education Department Summer Food Program Agreement. However, this information is provided by the County agency.
What Federal agencies are providing data for use in the system?	None.
What other third party sources is the data collected from?	None, other than vendors that consist of private and public sector organizations, independent consultants, Non-profits including local community based service providers, school district and behavioral health providers.
What information will be collected from the individual whose record is in the system?	Information is collected from vendor agencies. The following information is collected: User names, contact information, email addresses, insurance certifications, EIN #, e-signatures, contracts & related documents, memos and e-generated messages.

Access to CMS Data
Table 4

Question	Response
Who will have access to data in CMS?	Only users that are registered in CMS will have access to the data. Access to certain information is limited to the user's assigned role and task. Specific users include County Executive, County Attorney, Director of the Bureau of Budget and staff, the Auditor and staff, department heads and their employees responsible for overseeing the contract creation, review, delivery and execution process. Finally, registered vendors and designated employees responsible for contracts. Upon request auditors of vendor programs that received public funding may have temporary access to data but access would be restricted to the vendor's contracts.
Is any of the data subject to exclusion from disclosure under the Freedom of Information Act (FOIA)?	Contract information is subject to disclosure under the FOIA. E-mail addresses are excluded from disclosure under FOIA.
Will users have access to all data in the system or will the user's access be restricted? Explain	No. A user's access to data in CMS is restricted to access level to assure that only authorized users have access to certain information. Depending on their role, users may view, approve, or modify information. Some users have the ability to reject contracts. CMS has a variety of levels of system access including rights as a contributor, monitor (view-only). Users have specific role assignments, set up in the Approval Routing Modular.
What controls are in place to prevent the misuse of data or to prevent altering information in the system?	There are multiple controls in place to prevent altering information maintained in CMS. The CMS application shows an audit trail of information about who accesses the computer; every action is documented, time and date stamped, showing who completed the action and type of action. SH-256 is a high level certificate used in CMS that can show whether records have been altered or tampered with.
Do other systems share data or have access to data in this system?	No, not at this time.
How will the data be disposed of when the record retention date expires and the record is no longer needed?	Retention and disposition of page contract records is the same for e-records, which is seven to ten years. We are working with the consultant to prepare solution for capturing the records disposition date and sending a notification to everyone on the account when nearing the date. Compliance to records retention schedule will be satisfied.