Nth Generation Computing, Inc.'s Response to

DATA BACKUP AND RECOVERY SOLUTION

Request for Proposal (RFP) for:
City of Beaumont

Submittal Deadline: 2/19/2021 @ 10:00am

Table of Contents

Confidentiality Notice

This Nth Generation Proposal and all associated documents and attachments contained and included herewith, includes proprietary and confidential data that shall not be disclosed outside of Client Companies and Nth Generation Computing, Inc. and shall not be duplicated, used, or disclosed in whole or in part for any purpose other than to evaluate this proposal. This restriction does not limit any right to use information contained in this proposal if it is obtained from another source without restriction.

Nth GENERATION

Cover Letter

February 19, 2021

Attention:
City of Beaumont
Edgar Trenado
Information Technology Manager
etrenado@beaumontca.gov

RE: Nth Generation Computing, Inc.’s Proposal to City of Beaumont RFP for Back Up and Disaster Recovery Solution

Dear Mr. Trenado,

Nth Generation Computing, Inc. (“Nth”) is pleased to present herein our proposal in response to City of Beaumont’s (“City” or “Client”) RFP for Back Up and Disaster Recovery Solution.

Nth is proposing a Rubrik solution to meet the City’s needs. The Rubrik CDM software solution that Nth is proposing is an all-inclusive converged package requiring no additional footprint such as master and media servers, proxy servers, a reporting server, etc. outside of the on-premise Rubrik clusters. The included Features Table in section 8 details how our solution provides the City’s desired features and functionality.

The required information for both Nth and Rubrik is provided herein.

Thank you in advance for your anticipated professional courtesy and consideration. Should you have any questions or concerns, please do not hesitate to contact me.

Sincerely,

Joyce Russell

Joyce Russell
EVP/CFO
Nth Generation Computing, Inc.
17055 Camino San Bernardo
San Diego, CA 92127
858-451-2383
888-674-4684 (fax)
joyce.russell@nth.com

Katherine Hayes

Katherine Hayes
Enterprise Account Manager
Nth Generation Computing, Inc.
17055 Camino San Bernardo
San Diego, CA 92127
858-451-2383
888-674-4684 (fax)
katherine.hayes@nth.com

1. Company Information

1.1 Company Name:

Nth Generation Computing, Inc. (Partner/Manufacturer: Rubrik, Inc.)

1.2 Company address:

Nth: 17055 Camino San Bernardo, San Diego, CA 92127

Rubrik, Inc.: US Headquarters: 1001 Page Mill Road, Bldg 2 Palo Alto, CA

1.3 Company phone number:

Nth: 858-451-2383
Rubrik, Inc.: Telephone: 1-844-4RUBRIK

1.4 How long has your company or division been providing on-premises and cloud backup and recovery solutions?

Rubrik has been providing on-premises and cloud backup and recovery solutions since 2014.

1.5 Do you install the equipment or use subcontractors?

Nth's partner, Rubrik, will install the equipment and employs their own professional services delivery teams.

1.6 Do you install the equipment or use subcontractors?

Nth's partner, Rubrik, has hardware on-hand and usually ships to customers sites within 10 business days.

1.7 How many employees do you have?

Nth employs approximately 70 employees and Rubrik employs 1,600 employees.

1.8 How many Microsoft, Fortinet, HP, and Cisco certified engineers do you have and what level?

Nth holds the HPE Platinum Service One/Service Now partnership and associated certifications for engineering and sales. Due to our partnership level and certifications Nth is able to deliver services on behalf of HPE.

Rubrik has expertise with Rubrik platform and integrating into Microsoft on-premises applications and Azure/M365. Rubrik networking is very straightforward and easy to configure and have a well-documented port guide for access applications both on-premises and cloud. Rubrik also produces a quarterly security hardening guide to keep up with the latest cyber-security threats.

1.9 How many Microsoft, Fortinet, HP, and Cisco certified engineers do you have and what level?

Rubrik will follow the city's COVID recommendations. Rubrik can be on-site if request or can perform all installation/configuration functions remotely.

2. Vendor References

Customer Organization	Reference Contact
City of Manhattan Beach	Phat (pronounced Pat) Tran 310-802-558 1400 Highland Ave Manhattan Beach, CA 90266
Monterey County Office of Education	Francisco Garcia 831-755-0323 901 Blanco Cir Salinas, CA 93901
Yuba County	Joseph Oates 530-749-5626 915 8th St Marysville, CA 95901
City of Chandler	Andy Sandoval 480-748-5463 215 E. Buffalo St, Chandler, AZ 85225
Maricopa County Sheriff's Office	Robert Brooks 480-280-0860 550 W Jackson St, Phoenix, AZ 85003

3. Product Requirements

3.1 Rubrik Product Proposal for City of Beaumont

3.1.1 Product description

3.1.1.1 Rubrik R6404 (2) appliance with 30TB of usable capacity

3.1.1.2 3 years of hardware & software support (8am – 8pm M-F)

3.1.1.3 Rubrik Cloud Data Management (RCDM) for the data center (Rubrik's turnkey appliances) – Core software (unlimited on-prem applications integration and replication) with one of the industries only built-in data immutability, cannot be turned off or compromised by ransomware

3.1.1.4 Rubrik CloudOut (long-term archiving)

3.1.1.5 Rubrik Continuous Data Protection (Built in near-zero data loss technology for critical tier 0/1 VMWare workloads at no additional cost)

3.1.1.6 Rubrik GPS – Central management for all Rubrik workloads

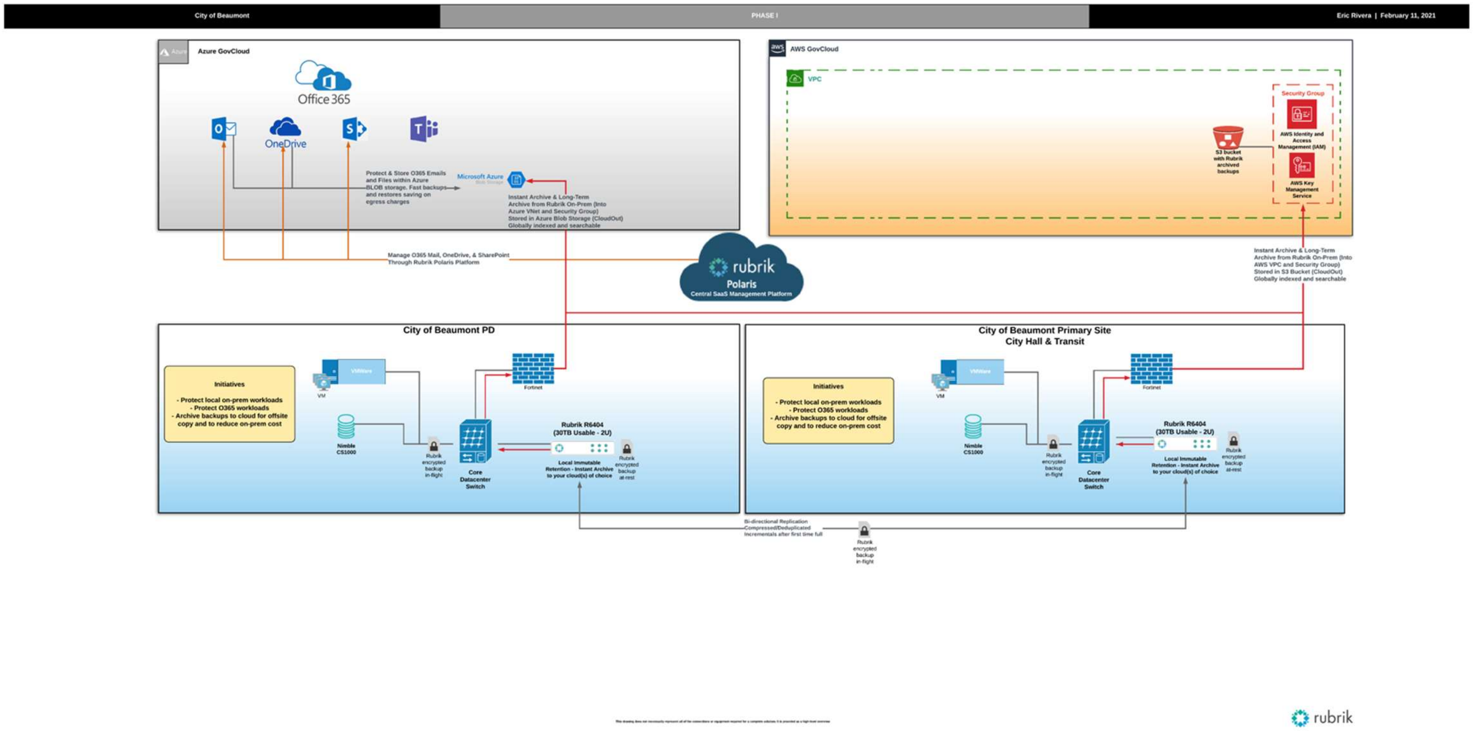
3.1.1.7 Rubrik Office 365 Backup – Subscription for M365 application protection

3.1.1.8 Rubrik Polaris Radar – Analyze backup data to find anomalies to pinpoint files that have been affected by ransomware and have a precise remediation

3.1.1.9 Cloud native instances – 100 instances can be protected for AWS EC2, Azure, or GCP cloud workloads

3.1.2 Describe Rubrik's Solution for this Proposal

High level design overview with on-premises and cloud data flow



City of Beaumont | PHASE I | Eric Rivera | February 11, 2021

Protect & Store O365 Emails and Files within Azure BLOB storage. Fast backups and restores saving on egress charges

Instant Archive & Long-Term Archive from Rubrik On-Prem (Into Azure VNet and Security Group) Stored in Azure Blob Storage (CloudOut) Globally indexed and searchable

Manage O365 Mail, OneDrive, & SharePoint Through Rubrik Polaris Platform

Instant Archive & Long-Term Archive from Rubrik On-Prem (Into AWS VPC and Security Group) Stored in S3 Bucket (CloudOut) Globally indexed and searchable

Initiatives

- Protect local on-prem workloads
- Protect O365 workloads
- Archive backups to cloud for offsite copy and to reduce on-prem cost

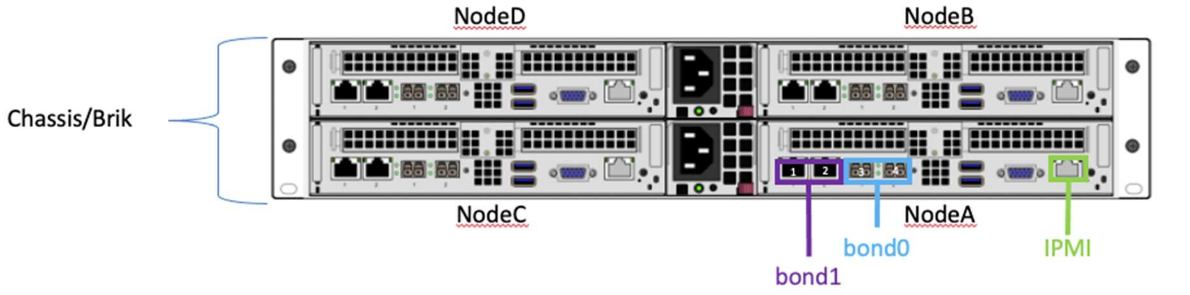
Local Immutable Retention - Instant Archive to your cloud(s) of choice

Bi-directional Replication Compressed/Deduplicated Incrementals after first time full

3.1.3 Desired Features spreadsheet included with the packet. Digital copy is on thumb drive

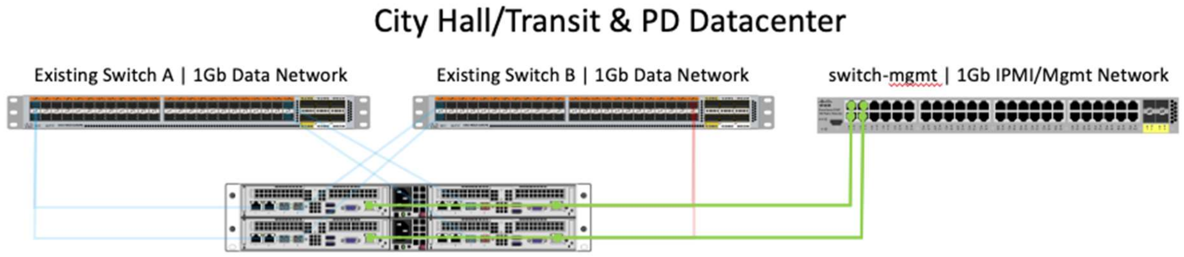
3.1.4 IT Network Requirements

3.1.4.1 Node port breakdown. Bond0 will be default data/management data flow. IPMI is 1GB for hardware troubleshooting



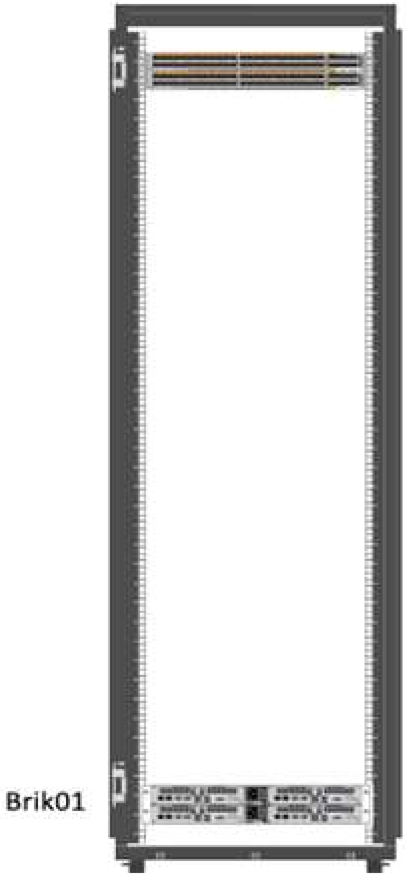
1. 10GBaseT port eth0, bond1
2. 10GBaseT port eht1, bond1
3. 10GbE/25GbE port eth2, bond0
4. 10GbE/25GbE port eth3, bond0

3.1.4.2 Cabling diagram


City Hall/Transit & PD Datacenter
Existing Switch A | 1Gb Data Network
Existing Switch B | 1Gb Data Network
switch-mgmt | 1Gb IPMI/Mgmt Network

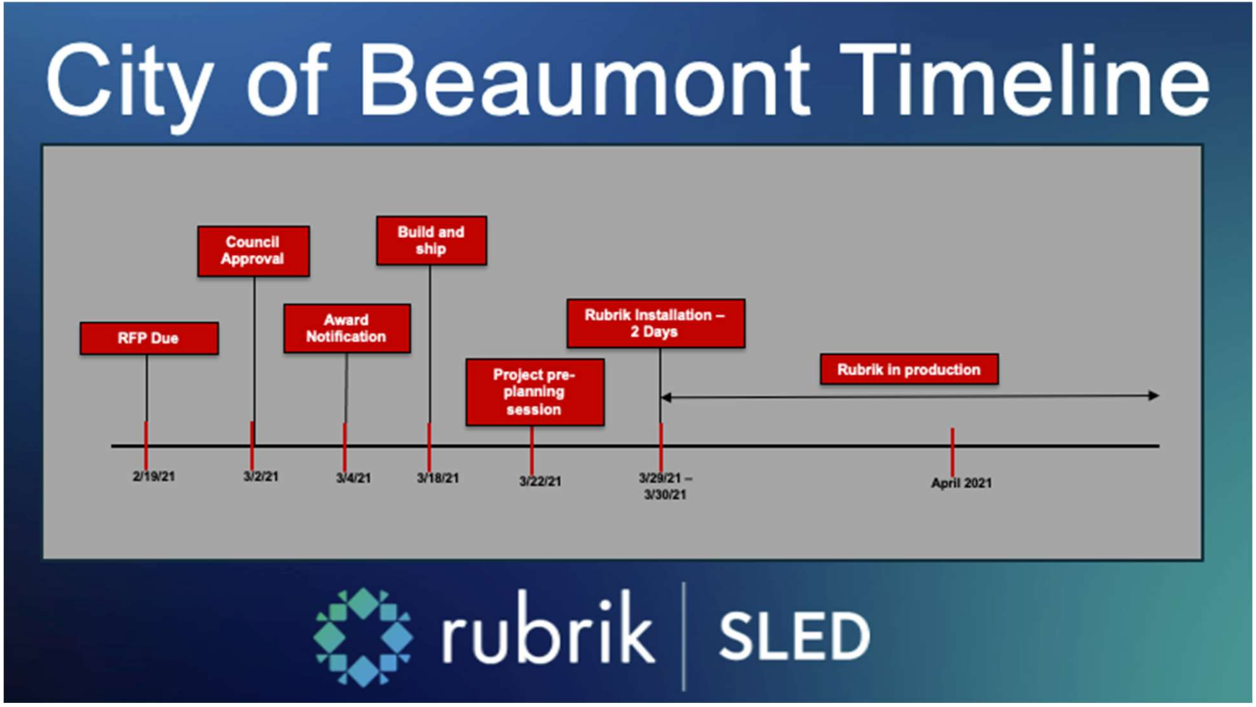
3.1.4.3 Rack Diagram. Each Rubrik appliance is 2U, weight 86lbs, Max Power Consumption 1023 Watts, and 3490 BTU/hour

City Hall/Transit & PD Datacenter



4. Rubrik Installation Service and Maintenance

4.1 Rubrik Project Timeline



City of Beaumont Timeline

RFP Due – 2/19/21

Council Approval – 3/2/21

Award Notification – 3/4/21

Build and ship – 3/18/21

Project pre-planning session – 3/22/21

Rubrik Installation – 2 Days – 3/29/21 – 3/30/21

Rubrik in production – April 2021

rubrik | SLED

4.2 As part of Rubrik's professional services deployment, the sales team and professional services team will collect all environmental information, physical power and network, as well as new cluster names, DNS, gateway, assigned IP addresses for the cluster and application info to make the deployment of the solution go a smooth as possible on date of installation

4.3 Please see our End User License Agreement at this link: https://www.rubrik.com/wp-content/uploads/2018/06/Rubrik-EULA.pdf

4.4 Please see our Support Services Policy at this link: https://www.rubrik.com/wp-content/uploads/2018/03/Rubrik-Support-Services-Policy.pdf

4.5 Rubrik upgrades are performed by customer support. Simply open a case and support will take care of the rest and coordination

4.6 All technical issues will be handled by customer support. You can either open a case online or via email.

4.7 As a part of post installation services, Nth will add Cloud (City's existing AWS or Azure) as a target for backups.

- Add the City's existing public cloud (AWS or Azure) target into the backup software as a defined "library" with the proper creds and secret keys.
- Add the library as a target to an existing backup repository or storage policy with retention parameters.
- Using a new or existing policy, run some test backups and make sure the backup job data gets copied to the cloud library with validation.
- Attempt to restore sample data from the cloud library to ensure it works both ways and make any final changes needed for customer policies.
- Any scope in addition to the initial setup and configuration or any additional licenses or subscriptions are not included and will require a scoping discussion and involve Nth's Change Control process.

5. Disaster Recovery

5.1 **Malfunctioning equipment (failover)** – Rubrik operates in a scale-out cluster model with erasure coding. Each of our solutions have four nodes for built-in non-disruptive failover scenarios

5.2 **Loss of one site** – Rubrik will be able to provide live mount capability for your applications to run directly off Rubrik storage to secondary VMWare environment. This will provide the city the ability to get services back online very quickly

5.3 **Ransomware** – Rubrik's filesystem is natively immune to ransomware. It is a write-once read many append only file system so if the city is hit with Ransomware, the city will be able to recover from your last backup taken. Rubrik is also going to provide the city with our advanced anomaly detection, not only to have immutable backups, but to pinpoint exactly which files or machines were affected by Ransomware to further reduce any downtime but preserve good data in the environment

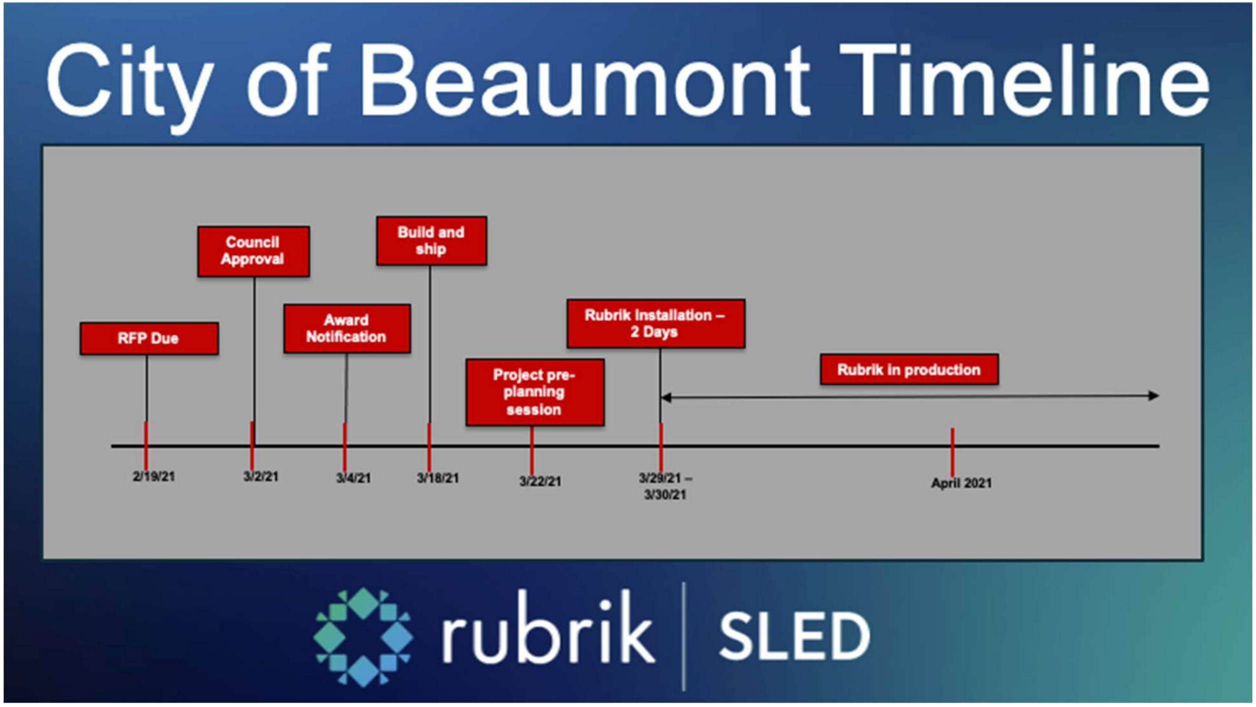
5.4 **Loss of power** – Rubrik appliances have dual power supplies and recommend splitting power between two different PDU's and circuits

5.5 **Loss of access to the building** – Rubrik has capabilities to be managed by any web browser that has access to the network it is residing on. City IT can VPN and have access to Rubrik UI

5.6 **Destruction of data** – Rubrik provides a destruction process for equipment that is traded in or swapped out by support

6. Project Plan

6.1 Rubrik Project Time



City of Beaumont Timeline

6.2 Based on RFP timeframe and key dates, equipment should be built and shipped to city's site on 3/18/2021. There will be a project pre-planning session with the sales team, professional services (PM and Install Engineer), and City IT to discuss all the necessary information needed to bootstrap and configure the Rubrik appliances

6.3 Knowledge transfer and documentation will be provided during the installation from the install engineer

6.4 Install engineer will provide all testing and acceptance from City IT and will send out daily updates with completed and outstanding items

6.5 On-site post support assistance will be provided for hardware related issues. All software post support issues will be handled by our central customer service time with 24x7x365 support.

6.6 Wasabi will connect Rubrik to cloud repository.

7. Pricing

7.1 One time cost for hardware, installation, and configuration services

7.2 One time cost for software and training

7.3 Ongoing cost, including a list of all licenses, annual maintenance costs and ongoing support

7.4 Hourly rates for out of contract work

7.5 Any other fees

7.6 Provide 5-year pricing for support on all equipment and licensing

7.7 Include part and model numbers for all proposed equipment

7.8 All cost associated with responding to this RFP are the sole responsibility of the responding vendor.

Please see Nth's solution pricing in the table below:

Part #	Qty	Description	Price (per unit)	Extended Price
		Rubrik Backup & DR Solution 5 Years		
RBK-R6404S-HW-01	2	r6404s Appliance, 4-node, 48TB raw HDD, 1.6TB SSD, SFP+ NIC	$14,218.07	$28,436.14
RBK-CMPLT-R6404	2	One (1) month of Rubrik Complete Edition for r6404, incl. RCDM, Polaris GPS, CloudOut, 100 instances/VMs of cloud native protection and Basic Support, subscription prepay, limit 1 per customer, M-F 8am-8pm support	$46,702.00	$93,404.00
RBK-SVC-BASIC-HW	2	60 Months Basic Support for hardware, prepay, M-F 8am-8pm support	$7,928.00	$15,856.00
RBK-F3M-CBL-01	2	Fiber Optic OM3 LC/LC Cable, 3M, pack of 4	$241.00	$482.00
RBK-SFP-TSR-01	4	10G/1G Dual Rate SFP+ Transceiver, pack of 4	$1,661.00	$6,644.00

RBK-SVC-CMPLT-RMOT	1	Rubrik Remote Consulting for Complete edition, must be used within 6 months of purchase, prepay	$1,445.00	$1,445.00
RBK-POL-RADAR	30	One (1) month of Polaris Radar, incl. Premium Support, per FETB per month, subscription prepay	$574.19	$17,225.90
		Wasabi Cloud 5 Years		
RCS-45TB-5Y	1	Reserved Capacity Storage 45TB 5Years	$16,157.00	$16,157.00
WS-PS	1	Wasabi Premium Support	$1,123.00	$1,123.00
			Sub total	**$180,773.04**
			Taxes	$2,756.06
			Solution Total	**$183,529.10**

Resource Pricing (out of contract work)

For additional services outside of this project scope, Nth charges daily resource costs for custom development, on-site implementation or engineering support and training as follows:

- **On-site implementation engineer (Rubrik Skill Set)***: $350.00 per hour, minimum 1 day (8 hours)

*Project Manager is included for the duration of On-site implementation.

For Rubrik add-on support programs, you can download the document at this link: https://www.rubrik.com/wp-content/uploads/2018/03/DATA-SHEET-Rubrik-Proactive-Add-On-Support-Program.pdf

8. Features Table

Desired Feature	**Nth/Rubrik Response**
Maintain an in-house backup solution, hardware, and software, for general operations (disk-to-disk)	Rubrik CDM software is an all-inclusive converged package requiring no additional footprint such as master and media servers, proxy servers, a reporting server, etc. outside of the on-premise Rubrik clusters.
Utilize a hosted environment for remote backup, backup replication/archiving, and extended retention schedules. (disk-to-cloud)	Rubrik has a very simple methodology of integrating with cloud providers to enable remote backup and backup replication/archiving to meet your extended retention schedules. Rubrik is cloud agnostic and can tie in with all the major cloud providers including on-premise NFS or Object storage if the city wants to keep sensitive data on-premise
Ability to access the hosted environment backups in the event of an infrastructure collapse to mimic virtualized datacenter environment for DR purposes	Rubrik has technology called CloudOn to convert on-premise VMs to either AWS EC2 instances or Azure VHD instances for cloud DR or migration services. For this RFP, we are proposing Wasabi as the Cloud provider of choice.
Features and Functionality	**Nth/Rubrik Response**
Easy/intuitive secure interface and management	Rubrik's HTML5 web UI is very intuitive to learn and use. Most of our customers learning curves are less than a week. Rubrik also provides a robust REST API library to help City IT automate repetitive restore operations, for example, refreshing test/dev servers after the backups complete with no human interaction
Easy to manage - backups, restores, policies, archiving, etc.	Rubrik has many customer success stories where organizations were spending a lot of time managing legacy backup products but was able to cut that time significantly down and focus on other projects that drove the business

Reporting on backup errors or anomalies (e.g., High change rates)	Rubrik has built a SaaS solution (no additional on-premise infrastructure needed) that is AI-ML driven to analyze backup data to find anomalies like high change rates and high levels of encryption from backup to backup. This will alert City IT and a detailed analysis will be provided on what files were affected. This solution won best security product at VMWorld and Rubrik is not a security company
Default auto protect of new VMs	Rubrik can apply our SLA domain at different level of your VMware architecture, Cluster/Host, folder, or VM level. If SLA domain is set a Cluster/host or folder level, any new VM associated at those levels will automatically inherit the SLA domain and be auto protected
Must be capable of VM level backups and restores of whole VMs	This feature is one of the many VM restore options within Rubrik
Must be capable of native database level SQL backups and restores	Rubrik supports native SQL backup and restores and also provides live mount option to spin database instances off of the Rubrik appliance to SQL servers for test/dev functions or for critical situations
Fast recovery times	Rubrik has won many awards for our backup and recovery speeds. With our latest software release we add another 5x performance boost for VMWare and 2x performance boost for SQL
'Instant' restore - spin up a VM on the backup system to quickly get it back running while it is being live migrated back to the production system	Rubrik's "instant" restore functionality is called live mount. Rubrik supports this for VMWare, SQL, and Oracle. Rubrik presents data directly from Rubrik appliance to the application via secure NFS or CIFS and automatically mounts to the application. Once a VM is live mounted off Rubrik City IT can vMotion back to production SAN
Intraday snapshots	Yes, this is supported within Rubrik SLA domain. Rubrik also has built-in continuous data protection so you can have near-zero data loss up to 4 hours on your critical VMWare servers
Out of the box reporting for auditing, capacity planning, and forecasting	Rubrik has many built-in reports for auditing, capacity, and forecasting. Also, as part of the call home feature, your sales engineer will have access to your cluster

	statistics and analytics for capacity and forecast trending
Capable of fine granularity (file level, point in time, etc.)	Rubrik can restore down to the file level at any point that a backup was perform. Files can easily be searched and sorted from latest copy to oldest
The system must provide logs of backup/restore activity	Rubrik logs all activities done by all users. Rubrik has Active Directory and Multifactor authentication ability as well as role-based access for tighter controls in Rubrik.
Able to spin up a VM quickly and easily from a backup copy in isolation to retrieve data, test a patch	Rubrik's City IT would VM live mount. Rubrik presents data directly from Rubrik appliance to the application via secure NFS and automatically mounts to the vCenter with the option to disable network interface. Once a VM is live mounted City IT can test patches or updates against the newly created VM. Once the testing/patching is completed, dismount from Rubrik and the VM will be cleaned from vCenter
Ability to quickly restore a deleted file/folder or restore an older version of a file	Rubrik's robust search engine can search entire backup data and quickly locate file/folders that need to be restored. The search goes against all backups on-premise and cloud storage
Ability to quickly restore a virtual server	Rubrik has many quick restore options for VMWare, live mounting, live mounting drives only, and instant restore (running production VM on Rubrik storage)
Ability to restore a physical server to a replacement physical server or Capacity to support existing storage size and easily scale to increase capacity in a cost-effective manner without substantially increasing the backup window	Rubrik does support BMR with matching processor families
Ability to recover from Ransomware	Rubrik's Atlas filesystem in natively immutable to ransomware. Rubrik has several customer success stories where they were hit by ransomware and were able to recover all their data from Rubrik and avoid paying any ransom
Ability to backup machines with different operating systems (Current environment is Windows only)	Rubrik supports all currently supported Windows Server operating systems. If City IT has older Windows versions, we can still

	backup at the VM level and perform restores
Restore files/folders based on search criteria (file/folder names, location, and attributes) across multiple backup copies. Geodiversity of replication hardware	Rubrik's robust search engine can search entire backup data and quickly locate file/folders that need to be restored. The search goes against all backups on-premise and cloud storage
Restore entire VM Hosts to bare-metal	This feature is one of the many VM restore options within Rubrik
Restore VMs as new VM not original	This feature is one of the many VM restore options within Rubrik
Provide continued functionality in the event of a power loss from outside the network	Rubrik will continue to function if on UPS and has network access to hosts it is protecting
Provide continued functionality in the event of a disaster that limits access to the building for a short or extended time	Rubrik will continue to function if on UPS and has network access to hosts it is protecting. If outgoing internet connection is down archiving will be queued until the link is back online
Flexible, Hardware-Agnostic replication	Rubrik can replicate to another Rubrik appliance or Rubrik software and agnostic to any archive location
Electronic transmission of city data must be encrypted	Rubrik provides in-flight and at-rest encryption for all data that is being protected
Service Level Agreement specifying Recovery Time Objectives and Recovery Point Objective and Ability to support long term data archival to	Rubrik's SLA domain engine simplifies backup policies by simply telling it how often to take the backup, for how long to keep it, and where to store the data (either local appliance or cloud storage)
Third party local storage	Rubrik would configure your local third-party storage as an archive target to Rubrik then we can configure our simple and power SLA domain engine to direct long-term data to move at a specific age in the lifecycle
Proprietary cloud - native to the platform and support granular file level recovery (to minimize cloud read and egress costs) or Third-party cloud (Example: AWS and Azure)	Rubrik would assist to configure your cloud storage bucket as an archive target to Rubrik then we can configure our simple and power SLA domain engine to direct long-term data to move at a specific age in the lifecycle. We support tiering within cloud tiers or you can directly archive to cold storage reducing your cloud spend. Rubrik also sends compressed/dedupe data

	so there is no need to rehydrate the data just to get it to the cloud
System Solution	**Nth/Rubrik Response**
Detailed documentation of required steps for proper backup and recovery	This documentation will be provided by install engineer as the environment is being installed, configured, and tested
Ability to meet HIPAA (Health Insurance Portability and Accountability Act)	Rubrik meets HIPAA standards and has many healthcare customers and data leveraging the Rubrik solution
Ability to meet CJIS (Criminal Justice Information Services) requirements	Rubrik meets CJIS standards and has many law enforcement customers and data leveraging the Rubrik solution. Rubrik can provide compliancy statement if needed
Ability to meet CIS (Center for Internet Security) standards	Rubrik uses the CIS benchmarks inputs for what we define for hardening standards and good practices at Rubrik
Follow NIST (National Institute of Standards in Technology)	Rubrik has directly obtained the NIST validated cryptographic module certificate (https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Certificate/2658)
Ability to perform searches on archived files in the event of a legal requirement	Every file that is protected with Rubrik is searchable with our global search features no matter if the data lives on-premise on Rubrik appliance or archived into cloud storage. Also, specific backups and be placed on legal hold if necessary
System Requirements	**Nth/Rubrik Response**
Retaining backup - the City requires the following:	
~ Once per 4 hours, retain for 2 days	This retention can be easily achieved with Rubrik SLA domain
~ Once per day, retain for 30 days	This retention can be easily achieved with Rubrik SLA domain
~ Once per month, retain for 12 months	This retention can be easily achieved with Rubrik SLA domain
~ Once per year, retain for 5 years	This retention can be easily achieved with Rubrik SLA domain

*The more granular the backups can be kept with little storage impact, the better.	There is very little storage impact for having more restore points
**"Infinite Cloud" advertised by some vendors is strongly preferred.	Rubrik maintains storage efficiencies in cloud storage to keep data storage cost to a minimum
Ability to do automated restore testing including service start verification of VMs	This can be achieved through Rubrik REST API automation. We have several customers leveraging this functionality to automate testing daily backups
Separate backup definitions and retention schedules for different VMs/Machines	This would be achieved creating two or more SLA domains and assigned to different folders/VMs
Must do backups with minimal performance impact to the production servers and to the network during normal business hours 6am – 6pm M-F	Rubrik performs a first time and incremental forever backup going forward so all additional backups are very efficient and minimal performance impact
The solution must provide its own local storage hardware for primary backup	Rubrik appliance comes with its own local immutable storage, compute, and networking that can easily scale-out
Ability to export backups to external drives	Yes, as long as server is registered to Rubrik and has valid drive letter
Must have an effective method to restore from local/cloud storage when the backup appliance is not available (Example: Backup appliance gets destroyed in a fire)	Rubrik can recover from a replicated appliance or mount cloud backups from replacement appliance or virtual instance to recover data

wasabi®

Ensuring CJIS Security Policy Compliance with Wasabi

Table of Contents

Executive Overview

Wasabi is an affordable and fast cloud storage service. Law enforcement agencies can use Wasabi for a variety of purposes including primary storage, secondary storage for backup or disaster recovery, and cold storage for data archival. Wasabi is ideal for maintaining and storing a wide variety of law enforcement application data and digital content including criminal justice information (CJI).

CRIMINAL JUSTICE INFORMATION SERVICES
CJIS
COMPLIANT

The U.S. Criminal Justice Information Services (CJIS) Security Policy has established minimum security requirements and controls to protect criminal justice information such as biometric data, digital evidence and electronic criminal records. The Federal Government does not provide a formal CJIS Security Policy assessment or certification process. Instead, individual law enforcement agencies are responsible for ensuring their IT systems and practices comply with the Security Policy.

Law enforcement agencies can use Wasabi to store and maintain CJI in accordance with the CJIS Security Policy statute. Wasabi uses security best practices and technologies to ensure the physical security of its facilities and to maintain the privacy, security and integrity of electronic data and digital records. In addition, following a thorough audit, the Wasabi service was awarded the official CJIS ACE Compliance Seal by Diverse Computing, a trusted third-party law enforcement agency solution provider with deep CJIS audit and compliance expertise.

This white paper provides an overview of the Criminal Justice Information Services Security Policy and explains how Wasabi helps law enforcement agencies comply with CJIS guidelines for safeguarding the privacy of criminal justice information.

Introduction – CJIS Security Policy Overview

The Criminal Justice Information Services Division of the FBI gives federal, state and local law enforcement and criminal justice agencies controlled access to a wide range of criminal justice information such as digital fingerprint records, arrest and stolen property reports, criminal records, and digital evidence such as dashboard and body-worn camera video.

A wide variety of agencies, external organizations and individuals may need to access CJI. To that end, the CJIS has established a Security Policy defining the minimum set of security controls required for interacting with CJI. The CJIS Security Policy applies to every individual—contractor, private entity, non-criminal justice agency representative, or member of a criminal justice entity—with access to, or who administers criminal justice services and information including private contractors such as cloud service providers. All private contractors who process CJI must sign the CJIS Security Addendum, a uniform agreement that ensures the contractor's IT systems and practices are consistent with the CJIS Security Policy.

While the CJIS provides uniform information security requirements, guidelines, and agreements, the Security Policy is left to the individual states and local jurisdictions to interpret. Specific administrative, technical and contractual requirements vary from state to state, and from locality to locality.

CJIS Security Policy Data Privacy and Security Implications

The CJIS Security Policy specifies 13 Policy Areas for safeguarding CJI, including provisions for maintaining data security and privacy. Law enforcement agencies must ensure digital information, electronic records, and personally identifiable information (PII) are not deleted improperly, corrupted, tampered with, or disclosed to unauthorized individuals. Agencies must put strong security systems and practices in place to protect access to confidential data and to safeguard the integrity of electronic records throughout their lifecycle. The rules apply to data and records maintained on-premises, in a hosted facility (colocation center), or in the cloud.

The CJIS does not offer a formal Security Policy accreditation process. The onus is on the individual agency to ensure its IT systems and practices comply with state and local CJIS data privacy and security requirements.

Wasabi engaged Diverse Computing, a respected third-party law enforcement agency solution provider to evaluate Wasabi's security architecture, systems and practices for CJIS Security Policy compliance. Diverse Computing solutions are used by of 1,600 agencies across the U.S. and the company is a recognized authority in CJIS audit and compliance. After a thorough review, the company awarded Wasabi its official CJIS ACE Compliance Seal.

Wasabi Hot Storage Overview

Wasabi hot storage is affordable, fast and reliable cloud object storage—for any purpose. Unlike legacy cloud storage services with confusing storage tiers and complex pricing schemes, Wasabi hot storage is easy to understand and implement, and cost-effective to scale. One product, with predictable and straightforward pricing, supports virtually every cloud storage application.

Law enforcement agencies can use Wasabi for:

- Low-cost primary storage for on-premises or cloud-based applications
- Economical secondary storage for backup, disaster recovery in the cloud, or data migration initiatives
- Affordable and reliable archival storage for long-term data retention

Wasabi hot storage is ideal for a wide variety of law enforcement agency applications including:

- Electronic records storage and retention
- Digital evidence preservation
- Body, dashboard and surveillance camera video retention
- Electronic imaging and biometric data storage

Ensuring CJIS Security Policy Compliance with Wasabi Hot Storage

Law enforcement agencies can use Wasabi to store and maintain CJI in accordance with CJIS security regulations. The Wasabi cloud storage service is engineered to ensure the protection, privacy and integrity of customer data. The service is built and managed according to security best practices and standards, with CJIS security guidelines in mind, and has received the CJIS ACE Compliance Seal from Diverse Computing.

Wasabi takes a "defense-in-depth" approach, employing multiple layers of security to address relevant CJIS Security Policy Areas. Wasabi ensures the physical security of its data centers; institutes strong authentication and authorization controls for all its cloud compute, storage and networking infrastructure; and encrypts data at rest and in transit to safeguard CJI.

Physical Security

The Wasabi service is hosted in premier Tier IV data center facilities that are highly secure, fully redundant, and certified for SOC-2 and ISO 27001 compliance. Each site is staffed 24/7/365 with on-site security personnel to protect against unauthorized entry. Security cameras continuously monitor the entire facility—both indoors and outdoors. Biometric readers and two-factor or greater authentication mechanisms secure access to the building. Each facility is unmarked so as not to draw attention from the outside.

Secure Network Architecture

Wasabi employs advanced network security elements, including firewalls and other boundary protection devices to monitor and control communications at internal and external network borders. These border security devices segregate customers and regulate the flow of communications between networks to prevent unauthorized access to Wasabi infrastructure and services.

Data Privacy and Security

Wasabi supports a comprehensive set of data privacy and security capabilities to prevent unauthorized disclosure of CJI. Strong user authentication features tightly control access to stored data. Access control lists (ACLs) and administratively defined policies selectively grant read/write and administrative permissions to users, groups of users, and roles.

Wasabi encrypts data at rest and data in transit to prevent leakage and ensure privacy. All data stored on Wasabi is encrypted by default to protect data at rest. And all communications with Wasabi are transmitted using HTTPS to protect data in transit.

Data Durability and Protection

Wasabi hot storage is engineered for extreme data durability and integrity. Wasabi provides eleven 9s object durability, protecting data against hardware failures and media errors. In addition, Wasabi supports an optional data immutability capability that protects data against administrative mishaps or malicious attacks.

An immutable object cannot be deleted or modified by anyone—including Wasabi. Wasabi data immutability protects the integrity of CJI, mitigating the most common causes of data loss and tampering including accidental file deletions, viruses and ransomware.

Customer Responsibilities

Wasabi customers typically interface with the Wasabi service using third-party file management applications and backup tools. To ensure CJIS Security Policy compliance, IT personnel must ensure the storage management tools and applications they use are configured to take advantage of Wasabi security features. For example, HTTPS must be enabled to encrypt data in transit. In addition, customers must encrypt all content and data (with the exception of surveillance, bodycam and dashboard cam video) prior to uploading it to Wasabi. Additionally, Wasabi gives you the option of where you store your data, so law enforcement agencies can select a U.S.-based data center of their choosing.

Law enforcement IT organizations must also ensure they have strong security systems and practices in place to safeguard other elements of their on-premises and cloud-based infrastructure. The Wasabi storage service is typically employed as part of a larger public or hybrid cloud IT implementation that includes multiple compute, storage and networking components.

CJIS Security Addendums

All private contractors (including cloud service providers) who process CJI must sign the CJIS Security Addendum. Wasabi will sign CJIS Security Addendums as required by state or local law.

Conclusion

The CJIS Security Policy introduces stringent data privacy and security requirements for law enforcement agencies. The CJIS does not provide formal Security Policy certification mechanisms, so the onus is on every law enforcement agency to ensure its IT systems and practices comply with state and local statutes.

Wasabi's cloud storage service ensures the protection, privacy, and integrity of criminal justice information, helping agencies comply with the CJIS Security Policy. Wasabi ensures the physical security of its data centers, employs strong authentication and authorization controls to safeguard infrastructure and services, and encrypts data at rest and in transit to prevent unauthorized information disclosure.

Wasabi is typically used in conjunction with other compute, storage and networking platforms and services. Law enforcement agencies must implement strong security systems and practices across all on-premises and cloud-based infrastructure to fully protect CJI and comply with the CJIS Security Policy requirements.

Additional Information

For additional information about CJIS and Wasabi consult the following resources:

- FBI CJIS website
- CJIS Security Policy resource center

About Wasabi

Wasabi provides simple, predictable and affordable hot cloud storage for businesses all over the world. It enables organizations to store and instantly access an infinite amount of data at 1/5th the price of the competition with no complex tiers or unpredictable egress fees. Trusted by customers worldwide, Wasabi has been recognized as one of technology's fastest growing and most visionary companies. Created by Carbonite co-founders and cloud storage pioneers David Friend and Jeff Flowers, Wasabi has secured $110 million in funding to date and is a privately held company based in Boston.

Tel 1-844-WASABI-1
Email info@wasabi.com

wasabi
hot cloud storage
www.wasabi.com