Proposal for O365 Extended Contractual Support

Prepared for

Fulton County Government

Presented
9/16/2023

B2B TECHNOLOGIES

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Over the past two years, B2B Technologies has been working with the Fulton County Government to migrate legacy Microsoft systems to Microsoft 365. Following the successful completion of the project, Fulton County Information Technology (FCIT) submitted a request for extended support. We provided a response to that request for consideration. FCIT has provided feedback to allow us to right size the proposed services. The purpose of this proposal is to address the needs identified through this process.

We have organized this document to align with the FCIT Divisions. The document consists of the following main sections:

- Endpoints Division
- Service Desk
- Systems Division
- Web Team
- Security Consulting
- Systems Engineering Consulting
- Pricing and Assumptions

B2B is looking forward to our continued partnership with Fulton County. We appreciate the opportunity to submit this proposal. If you have any questions, please contact one of the following:

Frank Fuerst
ffuerst@b2btech.com
(404) 271-4791

Tonya Smith
tsmith@b2btech.com
(770) 630-7200

ENDPOINTS DIVISION

In keeping with FCIT's most recent request, we are proposing the following services for the Endpoints Division:

- Tier 3 Support
- County Device Co-Management Consulting Services

Tier 3 Support

B2B offers general support contracts to allow you to extend your IT team on an ad-hoc basis. We are including a standard 100 hour support contract for the Endpoints Division. The hours may be used for ad hoc support or for scheduled Office Hours.

Scheduling Support
Ad hoc support may be requested by directly contacting one of the following people at B2B:

- Practice Manager for the area responsible for supporting the application/system associated with the issue.
- Account Executive for Fulton County

Contact may be made via email or phone. All requests will contain:

- FCIT Contact name, email address and direct phone number
- Description of the issue and history of resolution attempts
- OPTIONAL: End-user name, email address and direct phone number (if applicable)

Alternatively, FCIT may assign (escalation) work orders to a centralized B2B account which will forward an email to an assigned B2B resource.

Office hours
Office hours are open support sessions where users can join a call and request assistance with issues or simply ask questions about the best way to perform a task. One or more senior consultants from B2B are on these calls to answer questions and/or remediate issues.

FCIT may utilize support hours for "Office Hours" as desired. We will work with you to define the schedule for Office Hours. It is the responsibility of FCIT to communicate Office Hours schedules to users.

Tracking/Reporting
B2B will assign a resource to provide a Consumption Report at the beginning of each month noting the number of hours expended in the previous month. The report will show:

- The number of hours consumed during the month broken down by department.
- The number of hours consumed broken down by department from the beginning of the contract to the present.

- The total number of hours consumed.
- The number of remaining hours.

B2B's consultants will track utilization at a detail level in the event additional information is required. Details will be entered into B2B's time tracking system.

County Device Co-Management Consulting

Fulton County and B2B have successfully implemented co-management with Configuration Manager and Intune. In our prior collaboration, B2B provided valuable assistance to Fulton County in the co-management of a select group of "pilot" devices, sourced from the IT Department. Documentation and streamlined processes were furnished to guide the addition of further devices for co-management, which Fulton County has been diligently adhering to as the need arises.

Currently, Fulton County aims to expedite the co-management process for additional devices and seeks further consulting services pertaining to application deployment, device compliance and security, process refinement, and ongoing support.

SERVICE DESK

In keeping with FCIT's most recent request, we are proposing the following services for the Service Desk Division:

- Tier 3 Support
- Intune Dashboard Consulting Services

Tier 3 Support

B2B offers general support contracts to allow you to extend your IT team on an ad-hoc basis. We are including a standard 100 hour support contract for the Service Desk. The hours may be used for ad hoc support or for scheduled Office Hours.

Scheduling Support, Office Hours and Tracking/Reporting were described above in the Endpoints Division section. These processes/procedures prevail for all divisions.

Service Desk - Consulting

In our consultations with Fulton County, a significant portion of the Service Desk consulting focus revolves around the Mobile Device Management (MDM) area of Intune. In addition to the support currently provided for mobile device enrollment and management, B2B is proposing the implementation of further training for the support desk, with a particular emphasis on Mobile Devices. The recommended training encompasses, but is not limited to, the following areas:

- General Use of Intune with Mobile Devices: Comprehensive instruction on leveraging Intune's functionalities and features for optimal mobile device management.
- Troubleshooting Common Issues during Enrollment: Equipping the support desk with troubleshooting skills to address typical challenges encountered during device enrollment. This includes troubleshooting application deployment, configuration policy issues, and compliance report auditing.
- Dashboard and Reporting for Enrollment Issues: Training on effectively utilizing Intune's dashboard and reporting capabilities to identify and address enrollment-related issues efficiently.

By imparting this specialized training to the support desk, Fulton County can enhance its overall mobile device management capabilities, ensuring smoother operations and improved end-user experiences.

SYSTEMS DIVISION

In keeping with FCIT's most recent request, we are proposing the following services for the Systems Division:

- Tier 3 Support
- Exchange Public Folder Migration
- Decommission Legacy Exchange
- Decommission Airwatch
- Decommission Enterprise Vault
- eDiscovery Self-Service Configuration and Training

Tier 3 Support

B2B offers general support contracts to allow you to extend your IT team on an ad-hoc basis. We are including a standard 100 hour support contract for the Systems Division. The hours may be used for ad hoc support or for scheduled Office Hours.

Scheduling Support, Office Hours and Tracking/Reporting were described above in the Endpoints Division section. These processes/procedures prevail for all divisions.

Exchange Public Folder Migration

Fulton County currently has a large number of Public Folders in the Exchange 2013 on-premises staging environment. Exchange 2013 was at end-of-life as of April 11, 2023. There is no support available, and no security patching being provided for this system. While public folders will continue to work in the current environment, upgrading to Exchange 2016 or higher may require additional processes to allow them to continue to work properly.

B2B recommends converting Public Folders to modern systems within Microsoft 365. As discussed with the team previously, we will analyze Public Folders with each user department/area and determine the best replacement. These destinations can be:

- Resource Mailboxes such as Room or Equipment
- Shared Mailboxes
- Microsoft 365 Groups
- SharePoint Site Collection
- Teams

Once the destination is determined for each PF, we will move the data and/or functionality and provide user training.

Decommissioning of Exchange 2007

Given the architecture of legacy Exchange, it is imperative to undertake a proper decommissioning process from the domain to preempt any potential issues with integrated systems, including Active Directory. We acknowledge the progress made thus far, as mentioned during our recent discussion, wherein Fulton County confirmed the removal of the last Exchange 2007 server.

In the event of further assistance required for this critical task, B2B is well-prepared to scope and execute a small project to ensure seamless and efficient decommissioning. Our team of experts possesses the necessary knowledge and expertise to carry out this essential work, safeguarding the integrity and functionality of your integrated systems.

Decommissioning of Exchange 2013

As of the present, Exchange 2013 has reached its end-of-life status. Within the organization, three departments are presently utilizing this environment. Regarding the migration strategy, the decision has been made not to migrate Registration and Elections due to licensing constraints. Concurrently, the Board of Health is either in the process of self-migrating to a distinct email system/Microsoft 365 Tenant or may potentially be migrated as part of a separate initiative outlined elsewhere in this proposal.

In parallel, the CJIS teams are currently leveraging Exchange 2013 for their Zoom Rooms. Once the relocation of Public Folders and mail for these three departments is successfully accomplished, specific segments of the on-premises Exchange environment should be decommissioned, barring the exceptional case of retaining one hybrid server for attribute synchronization.

It is imperative that the hybrid endpoint is smoothly migrated to a supported platform, ensuring seamless operations and compatibility with future upgrades. By adhering to these steps, your organization can navigate the transition from Exchange 2013 effectively, mitigating potential risks and aligning with the latest supported technologies. Our team at B2B is fully equipped to provide comprehensive assistance throughout this migration process, ensuring a seamless and secure transition to a supported platform.

Given the architecture of legacy Exchange, it is imperative to undertake a proper decommissioning process from the domain to preempt any potential issues with integrated systems, including Active Directory.

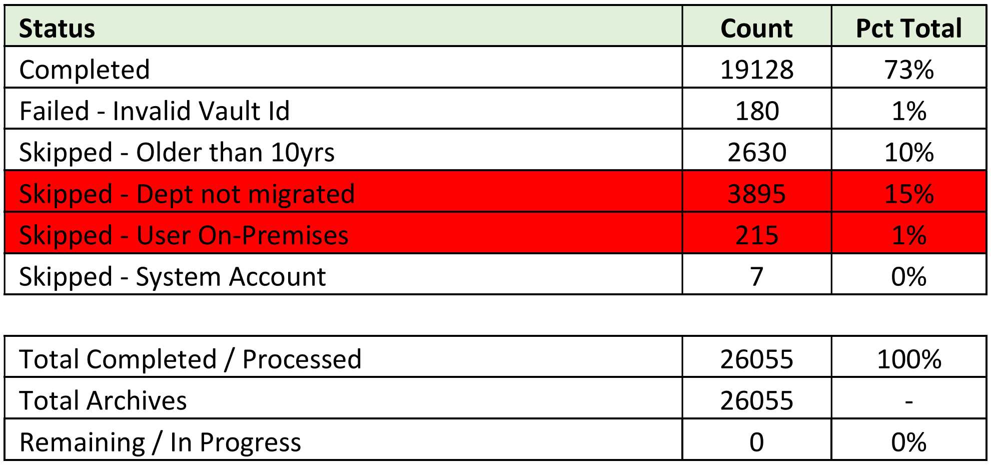
AirWatch Decommissioning

Fulton County presently holds licenses for AirWatch/Workspace One, but these licenses are nearing their renewal period. Subsequently, the migration of devices from AirWatch/Workspace One to Intune will ensue, and the consequent decommissioning of the server, along with associated components such as Secure Mail Gateway, will follow suit. It is crucial to ensure the migration of all devices to Intune, as failure to do so will render the management of devices unfeasible. In order to circumvent any potential disruption, B2B strongly recommends enrolling/migrating all users to Intune before proceeding with the decommissioning of AirWatch/Workspace One and the removal of any dependent components.

B2B is proficient in facilitating server decommissioning and adeptly identifying components that warrant attention before the decommissioning process takes place.

Enterprise Vault Decommissioning

After the completion of the previous migration initiative, a considerable number of vaulted mailboxes were successfully migrated to Exchange Online, either to the respective user's mailbox or to a shared mailbox, depending on the Active Directory account status. However, certain departments within Fulton County, such as Registration and Elections and the Board of Health, were not included in the scope of the prior migration effort and thus continue to be housed in the Enterprise Vault. Below are statistics detailing the count of vaulted mailboxes that were migrated and those that remain on-premises (highlighted in red):



Status	Count	Pct Total
Completed	19128	73%
Failed - Invalid Vault Id	180	1%
Skipped - Older than 10yrs	2630	10%
Skipped - Dept not migrated	3895	15%
Skipped - User On-Premises	215	1%
Skipped - System Account	7	0%

Total Completed / Processed	26055	100%
Total Archives	26055	-
Remaining / In Progress	0	0%

B2B will collaborate with Fulton County to determine the conclusive status of the remaining archives, and subsequently, orchestrate their migration as per the County's requirements. Following the successful migration of the vaulted mailboxes, the decommissioning process for the Enterprise Vault servers can be initiated.

Exchange 2019 Management Server

Following the completion of the previous mailbox migration project, Fulton County retained Microsoft Exchange 2013 servers on-premises to accommodate the remaining user mailboxes and serve as the Hybrid Endpoint for mail-flow. As a result of utilizing hybrid identities, the presence of an on-premises Exchange Server is necessary to manage Active Directory attributes concerning Exchange/Email. However, it is imperative to note that Exchange 2013 reached its end of life in April 2023.

To address this situation, B2B is prepared to collaborate with Fulton County in migrating any lingering resources to a unified and consolidated Exchange 2019 server. Additionally, we will undertake the reconfiguration of the hybrid setup to direct cross-premises mail-flow and enable synchronization of Exchange-related attributes with Azure AD/Exchange Online through the Exchange 2019 servers. This approach ensures compliance with the latest software and facilitates a seamless and efficient exchange environment for Fulton County.

eDiscovery Self-Service Configuration and Training

Previously, the management of e-Discovery requests within Fulton County was solely undertaken by the IT Team, utilizing the on-premises infrastructure. However, with the adoption of Microsoft 365, there is now an opportunity to expand access to the e-Discovery interface, enabling additional groups of users to avail themselves of self-service capabilities. It is essential to exercise prudence in granting such access, limiting it exclusively to users with a genuine need for these privileges.

B2B is well-prepared to oversee the configuration of appropriate roles that facilitate self-servicing of e-Discovery requests. Our team will diligently ensure that the access permissions are accurately tailored to meet specific user requirements. Furthermore, we are committed to providing comprehensive training to the designated team responsible for handling e-Discovery requests, empowering them to efficiently navigate the interface and execute these tasks proficiently.

By empowering select users with self-service capabilities and equipping them with the necessary training, Fulton County can streamline the e-Discovery process, reduce the workload on the IT Team, and promote a more efficient and responsive approach to handling legal requests within the organization.

WEB TEAM

In keeping with FCIT's most recent request, we are proposing the following services for the Web Team:

- Tier 3 Support
- Naming Convention Clean-up and Management

Tier 3 Support

B2B offers general support contracts to allow you to extend your IT team on an ad-hoc basis. We are including a standard 100 hour support contract for the Web Team. The hours may be used for ad hoc support or for scheduled Office Hours.

Scheduling Support, Office Hours and Tracking/Reporting were described above in the Endpoints Division section. These processes/procedures prevail for all divisions.

Naming Convention Clean-up and Management

Microsoft Teams include special purpose SharePoint sites that may be accessed through Teams or directly through SharePoint Online. In order to better manage these Teams "sites" from within SharePoint, the Fulton County Web Team has requested assistance with enforcing a specific naming convention. This request consists of two parts:

- Retrofitting the naming convention to current Teams (i.e., sites); and
- Enforcing the naming convention for future Teams (i.e., sites).

Step one will be to implement a procedure and systems to enforce the naming convention for any new Teams. There are several ways to achieve this goal. Our recommendation (and pricing) is based on the following method:

- Limit the role(s) allowed to create new Microsoft Teams
- Create an online form to request creation of a team.
- Customize a workflow that forwards the request for approval.
- Automate the creation (and naming) of the team as a result of the approval.

In order to retrofit the naming convention, B2B will write a PowerShell script and run it against the SharePoint Online environment. The script will be run outside normal business hours as it will disable the each team for up to 15 minutes as the rename process is running. We will rely on FCIT to communicate the changes and provide support to end-users other than system errors.

SECURITY CONSULTING

FCIT has requested assistance with the various security workloads within Microsoft:

- Identity and Access Administration
- Data Loss Prevention Administration
- Security Configuration for Microsoft 365

B2B recommends our Microsoft Centric Security Program – Secure and Protect – to meet these needs. Secure and Protect is a tenant security hardening effort by B2B to improve the overall security posture of the Microsoft 365 and Azure Tenants. The following workloads are reviewed and hardened as part of this effort. A complete list of actions performed are outlined in Appendix B: Secure and Protect:

- Azure Active Directory
- Microsoft Purview (Compliance) and Security
- Defender for Cloud Apps
- Defender for Endpoints
- Exchange Online
- Intune (Mobile Application Policies for BYOD)
- OneDrive / SharePoint
- Teams

The initial review and security hardening protocol typically takes six to eight months for implementation. The Microsoft 365 Tenant Security monitoring effort will begin upon implementation of the first workload. As new workloads or functions are incorporated into Microsoft 365, we will incorporate them into the offering, always keeping your environment maximally protected. In addition, once the initial hardening effort is complete, we will begin the ongoing review cycle to ensure that your security posture continues to meet or exceed best practices over time. We will work with you to define the review schedule. An example review cycle is included here for demonstration purposes.

Quarter	Review
1	Data Loss Prevention Configuration/Settings
2	MDM/MFA Configuration and Policies
3	Purview Configuration and Policies
4	Defender for Cloud Apps Configuration and Policies

We will also provide monthly reports and will work with you to continually adjust the review process to ensure a maximal security posture across all Microsoft systems.

Secure and Protect Tasks

The following are an itemized tasks that are performed as part of the Secure and Protect effort. Additional items may be added depending on Microsoft Secure Score recommendations:

Tasks / Effort	***Platform***
Review Azure AD Reporting	Azure AD
Turn on User Risk Policies	Azure AD
Turn on User Sign-in Policies	Azure AD
Restrict user consent to applications	Azure AD
Do not allow users to grant consent to unmanaged applications	Azure AD
Restrict logins by IP / Geo-Location	Azure AD
Enable self-service password reset	Azure AD
Enforce MFA for Admins	Azure AD
Set up Azure AD Break Glass Accounts	Azure AD
Implement Privileged Identity Management for Just-in-time access	Azure AD
Remove dormant accounts from sensitive groups	Azure AD
Use limited administrative roles	Azure AD
Implement Custom Banned Passwords List and Lockout thresholds	Azure AD
Secure Applications Access using Conditional Access Rules	Azure AD
Ensure all users can complete multi-factor authentication for secure access	Azure AD
Configure Named Locations to allow bypass of conditional access policies	Azure AD
Block Legacy Authentication	Azure AD
Configure General Anti-Spam Policies	Compliance and Security
Configure Safe Links and Safe Attachments Delivery	Compliance and Security
Configure DLP (Data Loss Prevention) Rules and notifications	Compliance and Security
Configure Retention Policies	Compliance and Security
Configure General Anti-Phishing Policies	Compliance and Security
Configure General Anti-Malware Policies	Compliance and Security
Create customized DLP policies for personal data	Compliance and Security
Create DLP Policies for Company Sensitive Information	Compliance and Security
Create DLP Policies for Personally Identifiable Information	Compliance and Security
Configure Sensitivity Labels	Compliance and Security
Apply sensitivity labels to protect sensitive or critical data	Compliance and Security
Configure Microsoft Information Protection Scanner for on-premises file classifications	Compliance and Security
Review Security Recommendations for Azure and remediate	Compliance and Security
Configure supported app connectors	Defender for Cloud Apps
Configure Conditional Access App Controls for apps for session control	Defender for Cloud Apps
Integrate Azure for Identities with Cloud App Security	Defender for Cloud Apps
Enable Azure AD Identity Protection Integration	Defender for Cloud Apps

Enable Defender for Identities Integration	Defender for Cloud Apps
Configure Sanctioned Apps to block access using Defender for Endpoints	Defender for Cloud Apps
Discover Risky and Non-Compliant Shadow IT Applications	Defender for Cloud Apps
Detect anomalous behavior	Defender for Cloud Apps
Set automated notifications for new and trending cloud applications in organization	Defender for Cloud Apps
Notify upon Detection of New OAuth Application	Defender for Cloud Apps
Create a Custom Activity Policy to Discover Suspicious Usage Patterns	Defender for Cloud Apps
Install Defender for Endpoints on Servers	Defender for Endpoints
Implement Outbound Spam Policy	Exchange Online
Implement DMARC for outbound mail	Exchange Online
Enable Client Rules Forwarding Block	Exchange Online
Set up Sender Policy Framework to prevent spoofing	Exchange Online
Implement BIMI with logo	Exchange Online
Configure Message Records Management Tags and Policies (for archiving)	Exchange Online
Allow Mailbox Delegation Only When Authorized	Exchange Online
Do Not Override FROM Address Enforcement	Exchange Online
Implement connection filter	Exchange Online
Manage Calendar Details Sharing	Exchange Online
Use S/MIME	Exchange Online
Configure MAM policies for App Protection and Selective Wipe for BYOD	Intune
Review and Configure OneDrive and SharePoint Sharing configuration	OneDrive/SharePoint
Review Security configuration for OneDrive and SharePoint	OneDrive/SharePoint
Enable versioning for document libraries	OneDrive/SharePoint
Configure External Sharing Links to Expire	OneDrive/SharePoint
Azure AD Password Protection on on-premises domain controller	On-Premises
Configure Microsoft Defender for Identities (formerly Azure ATP)	On-Premises
Review ADFS environment for security	On-Premises
Configure secondary Azure AD Connect server in staging	On-Premises
Configure which users are allowed to present in Teams meetings	Teams
Require lobbies to be set up for Teams meetings	Teams
Restrict anonymous users from joining meetings	Teams
Limit external participants from having control in a Teams meeting	Teams
Restrict anonymous users from joining Teams meetings	Teams
Restrict dial-in users from bypassing a meeting lobby	Teams

SYSTEMS ENGINEERING CONSULTING

B2B collaborated with Fulton County to facilitate the migration of Exchange (Mail) and File Servers, encompassing user home drives and departmental shared folders, to the Microsoft 365 platform. Our dedicated team at B2B is well-versed in best practices and adept at troubleshooting, promptly addressing any reported or requested issues to ensure optimal performance.

Regarding Exchange, B2B assumes responsibility for email service support, including user account management, distribution groups, and resource mailboxes. We configure mail flow rules, administer security settings, and proactively monitor server health to swiftly address any email-related challenges.

Furthermore, in the context of SharePoint, B2B offers assistance in managing site collections, libraries, and lists. Our team is proficient in assigning permissions to users and groups, ensuring controlled access to sensitive documents while strictly adhering to governance policies to safeguard data integrity. We skillfully customize SharePoint settings, encompassing versioning, content types, and search options, to promote collaboration and knowledge sharing across the organization. Continual monitoring of SharePoint's performance and usage metrics empowers us to identify opportunities for enhancement and cater to the evolving needs of users with utmost efficiency.

PRICING AND ASSUMPTIONS

Support Hours

In keeping with FCIT's request, B2B is proposing a pre-paid support contract at a discounted rate to be used for ad hoc support needs. The following applies to the Support Hours proposed for each division.

1.1. Support Options: Prepaid

- Client purchases a prepaid block of hours at a discounted rate
- Hours can be used as needed
- When contacted, B2B Technologies will schedule a time, based on customer needs and B2B availability, to work on the specific issue and/or project.

1.2. Support work hours

- Support provided during normal working hours, M-F, 8:30 to 5:30pm
- Technicians will record time in no less than 15-minute increments
- Onsite support will be a minimum of 4 hours.

1.3. Schedule: Support services to begin upon contract execution. The first Consumption Report will be provided on or about the first of the following month and each month thereafter.

Pricing Options/Overview

Tier 3 Support is pre-paid. For other requests, B2B is providing a Fixed Cost quote. This quote is valid for 12 months or through the end of this agreement, whichever comes first.

Endpoints Division

Description	Cost
Tier 3 support (100 hours)	$18,500
County Device Co-Management Consulting	$18,655
TOTAL	**$37,155**

Service Desk

Description	Cost
Tier 3 support (100 hours)	$18,500
Service Desk Consulting (Intune, Dashboard)	$7,755
TOTAL	**$26,255**

Systems Division

Description	Cost
Tier 3 support (100 hours)	$18,500
Exchange Public Folder Migration	$16,810
Decommission Legacy Exchange	$19,475
Decommission Airwatch	$8,710
Decommission Enterprise Vault	$54,305
eDiscovery Self-Service Configuration and Training	$6,010
TOTAL	**$123,810**

Web Team

Description	Cost
Tier 3 support (100 hours)	$18,500
Naming Convention Clean-up and Mangement	$6,150
TOTAL	**$24,650**

Security Consulting

B2B recommends Secure and Protect to meet these requirements. Pricing is based on an annual commitment (invoiced monthly) with a discount for a three-year commitment.

Duration	Monthly	Annual
One-Year Commitment	$6,000	$72,000

Systems Engineering - Consulting

Actual costs will be determined by the actual number of hours worked. We are basing our costs on 20 hours per week. We will report on actual hours a minimum of monthly. We will work with you to address requirements that could potentially result in overages in advance.

Duration	Hrly Rate	Monthly	Total
One-Year Commitment/20 hours per week	$130	$11,700	$140,400

Summation of Pricing

	Cost
Endpoints Division	$37,155
Service Desk	$26,255
Systems Division	$123,810
Web Team	$24,650
Security Consulting	$72,000
Systems Engineering Consulting	$140,400
TOTAL	**$424,270**

Assumptions

General Assumptions:

- All Work will be performed remotely.
- All software is licensed and current by the County.

Client Responsibilities:

- Client will provide a single point of contact to coordinate access to systems and personnel as required to successfully complete the project in a timely manner.
- Client will provide administrator level access to any systems required to complete the project. Access will be granted at the time of or prior to the kick-off meeting. Specific permissions include but may not be limited to:
    - Configuration Manager: Full Administrator
    - Active Directory Domain: Domain Administrator
    - Azure Tenant: Owner
    - Microsoft 365 Tenant: Global Administrator
- Client will be responsible for coordinating the appropriate personnel for meetings.
- Client will be responsible for licensing all software required.

Out of Scope:

- Any task or deliverable not included or agreed upon in this statement of work