FIRST AMENDMENT
TO PROFESSIONAL SERVICES AGREEMENT WITH
DAKADESIGN, LLC

THIS FIRST AMENDMENT is made and entered into this 26th day of October, 2021, by and between the CITY OF FORT BRAGG, hereinafter referred to as "City," and DAKADESIGN, LLC, hereinafter referred to as "Consultant."

WHEREAS, the City and Consultant entered into a Professional Services Agreement ("Contract") on June 30, 2021 to utilize the services of Consultant for on-call backup IT services as needed; and

WHEREAS, the Contract states that Consultant will provide on-call backup IT services for a total contract amount not to exceed Ten Thousand Dollars ($10,000.00); and

WHEREAS, the parties desire to amend the contract to increase the scope of work to prioritize network security and safe network and application practices at the City of Fort Bragg, as outlined in **Exhibit A** attached hereto; and

WHEREAS, at this time, the City desires to increase the total compensation amount by $50,000 for a total amount not to exceed Sixty Thousand Dollars ($60,000.00) to cover some of the more immediate security and network needs as outlined in **Exhibit A**; and

WHEREAS, the legislative body of the City on October 25, 2021 by Resolution No. _____ authorized execution of this First Amendment on behalf of the City in accordance with Chapter 3.20 of the City Municipal Code;

NOW, THEREFORE, for the aforementioned reasons and other valuable consideration, the receipt and sufficiency of which is acknowledged, City and Consultant hereby agree that the Professional Services Agreement for IT services between the City and Consultant dated June 30, 2021, is hereby amended as follows:

1. **Scope of Work:**

   Paragraph 1.1 (Scope of Work) is hereby amended to include the additional work described in Exhibit A attached hereto and incorporated herein by reference, subject to project-by-project approval by the City Manager.

2. **Compensation:**

   Paragraph 2.1 (Compensation), is hereby amended to state, "Consultant's total compensation shall not exceed **Sixty Thousand Dollars ($60,000.00)**."

3. Except as expressly amended herein, the Professional Services Agreement between the City and Consultant dated June 30, 2021, is hereby reaffirmed.

IN WITNESS WHEREOF, the parties have executed this Amendment the day and year first above written.

CITY OF FORT BRAGG:

By:_____
Tabatha Miller
City Manager

ATTEST:

_____
June Lemos, CMC
City Clerk

CONSULTANT:

By:_____
Deborah Smith
Principal

APPROVED AS TO FORM:

_____
Keith F. Collins
City Attorney

EXHIBIT A

Key: P1 items in Red, **P2 in Blue**, P3 in Black.

City of Fort Bragg:

Prioritized Network & Network Security Items

It's a scary time to be responsible for network security. Endless headlines tell of yet more enterprises, hospitals, government entities, etc. being hit with ransomware, customer credit card data theft, and other serious (and expensive) breaches. Yes, *effective* network security is expensive...but it's far less expensive than the oh-so-painful impacts of not doing everything possible to protect enterprise and customer data!

For many years, my focus as a Network Architect was in creating high performing, highly available networks to give the best possible uptime and performance to support Voice over IP and all other critical enterprise traffic (both wired and WiFi). With the rise of ever more sophisticated malware in recent years, my primary focus areas have grown to encompass security: a network environment that is not as secure as possible *will* eventually be breached...if it has not been already! Without a multi-layered approach, network security (and, hence, availability) is a temporary illusion, at best.

However, it is *essential* to prioritize implementing the ***basics*** of network management and security! Without ensuring safe network and application practices at the most basic levels are addressed first, security holes large enough for a truck to drive through may remain in place without anyone knowing this is the case!

Goal 1: Provide overall direction and strategy for implementing industry recognized Best Practices

1.1 Assess which international or national processes and security standard it would be best for the City of Fort Bragg to follow (e.g., NIST, ISO 27001/2).
1.2 Work with M. Ortiz to assess CFB current position with respect to industry standards (e.g., ISO 27001/2 or other chosen standard).
1.3 Assess which areas of discovered weaknesses place the City at the highest risk levels, and adjust the prioritized lists in Goals 2 and 3 below as necessary.

[All of Goal 1: This is the most urgent set of items under consideration. We need to determine if there are as-yet-to-be-discovered, yet well-known in the industry, security holes.

Estimate: DDLLC: $5000, and 20 hours of M. Ortiz time.]

Goal 2: Improve Network Performance, Availability, and Manageability (in suggested order):

Key: P1 items in Red, **P2 in Blue**, P3 in Black.

2.1 Provide troubleshooting services as-needed on a continuing basis. [Already covered under separate contract.]

2.2 Begin creation of detailed physical and logical network infrastructure drawings and related documentation. [Estimate is listed on related item below.]

2.3 Implement new wireless or VPN link between Corporate Yard and Police Dept. [Already in process.]

2.4 Eliminate extra hop for City Hall outbound traffic caused by the default gateway being the Adtran router that connects to the Corporate Yard / Water Treatment plant. (The default gateway should be the Firewall.) [Note: Making this change first requires implementing routing on the City Hall main switch, which will occur after switch upgrades as in 2.10.]

2.5 Test UPS capability at PD and elsewhere, and modify as necessary for the hours of support deemed critical by City management. (Recent power glitch dropped power to the Firewall and to AD server.) [DDLLC: $1500.]

2.6 Upgrade current PD Comcast Internet circuit to one using Public IPs (/28) and BGP routing, or implement other backup method that will survive a Comcast outage. [Approach TBD]

2.7 Modify network design to incorporate a secondary Internet connection (with auto-failover).

2.8 Acquire new Internet circuit from a second provider (not Comcast), and that uses divergent/ separate provider infrastructure if possible. This secondary provider will need also to run BGP, and to agree to advertise the public IPs (/28) of the primary circuit.

2.9 Implement new wireless or VPN link for failover connection between City Hall and Police Dept. [Already in process.]

2.10 Replace all EOS and/or unmanaged / insecure network infrastructure equipment (i.e., entire switch infrastructure) with current models that support 10G where needed. [Estimate: Hardware $48k, DDLLC $5500 configuration and after-hours installation, $5500 / 3 yrs licensing and support.]

2.11 Complete detailed physical network infrastructure drawing. [DDLLC Estimate: $7500 - $10k]

2.12 Implement 10G connectivity for server connectivity to switches, and for internal PD switch connections.

2.13 Limit trunking on uplinks only to VLANs required in connected location.

2.14 Configure all switch end device access ports to a standard Access Port configuration. [Included in switch replacement costs in 2.10.]

2.15 Assess need for new wireless link (or not) between Town Hall and City Hall.

2.16 Assess current server backup software and determine if better solution exists. [Better solutions exist. Cost to choose and implement one included in 2.17.]

2.17 Implement true off-site backup storage that incorporates protection from Ransomware. [Initial sizing Estimate: $12k annually.]

2.18 Consider implementing Cisco WiFi network equipment for enhanced performance, capabilities, manageability, and security.

2.19 Where possible (i.e., within budget constraints), eliminate single points of failure in the network. Where not possible, stock on-site spares or have 2-4 hr response contracts with vendors.

2.20 Implement SNMP server / network infrastructure logging (history and alerting for network infrastructure issues). [Estimate $5000 annually for on-site – may be possible to add to 3.2.2.]

Key: P1 items in Red, **P2 in Blue**, P3 in Black.

2.21 Once new network infrastructure equipment is in place, implement Quality of Service for excellent Voice over IP call quality, as well as protecting bandwidth for other critical network applications.

Goal 3: Implement multi-layered infrastructure security:

Sub-Goal 3.1: Implement Multi-Factor Secure Access

3.1.1 On-site Wired and Wireless Access:

3.1.1.1 Ensure that City legal team review and approve network login banner language. [Estimate: 1 hr legal team cost.]

3.1.1.2 Until switched infrastructure can be replaced, improve security on it by requiring encrypted protocols for access, different user and privileged passwords, and eliminating shared passwords. [Estimate: $500]

3.1.1.3 Consider implementing Cisco ISE (Identity Services Engine). ISE identifies users and devices, and supplies network access policies to the network infrastructure equipment based on that identification, no matter where on the network they connect.

Note: ISE is THE modern way to control network access, AND access to all resources. It is somewhat expensive to set up initially, but makes *everything* automatically more secure, and many other security policies and features easier to implement (including all physical connections, wireless connections, BYOD, Rapid Threat Containment, etc). To get an actual estimate will require engaging experts in installing ISE. [DDLLC is very capable of using it on a daily basis, and training M. Ortiz.] Based on past experience, however, $50k would be a good budget number.

3.1.1.4 If ISE will not be implemented, set up port security on all switches (requires replacing non-Cisco hubs/dumb switches with Cisco). [Estimate: $1000 for port security, monitoring for one week, and training M. Ortiz]. Cost for switch replacement is in 2.10.]

3.1.2 Remote access:

3.1.2.1 Remove all shared VPN accounts and replace with personally-identifiable, user-specific ones. [Estimate: DDLLC $2500]

3.1.2.2 Implement NPS on AD servers, and then use Group membership to control who can log into each F/W VPN group. [Estimate: DDLLC $1500]

3.1.2.3 Implement DUO for Multi-Factor Authentication. [Estimate: $7200 annually for service, DDLLC $3000 to implement]

Sub-Goal 3.2: Complete Network Flow Visibility and Alarms

Key: P1 items in Red, **P2 in Blue**, P3 in Black.

3.2.1 Integrate the Cisco FTD Firewalls with Cisco Defense Orchestrator (inexpensive Firewall tools) or with Cisco FirePower Management Center. [Estimate: $3500 for Cisco FMC Virtual machine on VMWare, $840 annual support. DDLLC $2500 to configure and integrate two firewalls.

3.2.2 Once network infrastructure is upgraded to Full Flexible Netflow-capable devices, implement Cisco StealthWatch Cloud for full Network traffic flow visibility. [Estimate: Unknown. We will need to run a trial to see the amount of traffic and associated cost.]

Sub-Goal 3.3: Internal Segmentation / Firewalling

3.3.1 Implement additional IP address subnetting (e.g., so WiFi users, City Hall wired connections, and Waste Water are not all on 192.168.211.0/24). [Estimate: DDLLC $2500. Also will require M. Ortiz time and WW device management time.]

3.3.2 Implement a DMZ so that connections initiated from the Internet that must be permitted inbound (i.e., mail), do not terminate on the internal Servers subnet! [This risk is what led to the recent incident. Estimate: DDLLC $500.]

3.3.3 Modify network design so that Granicus encoder at Town Hall does not provide a non-firewalled, back-door entry from the Internet. [This item now covered by 3.3.4.]

3.3.4 Determine location of other Internet access points discovered by Kroll, and either remove them or secure with a firewall. [Estimate: DDLLC $1500 to locate other Internet access points, and if possible, simply remove or use current firewall to protect the connections. If additional firewall equipment is found to be required, that will be an additional cost to acquire and to implement.]

3.3.5 Determine best method for internal security segmentation that City can afford, and implement (such as Cisco ISE integrated with Cisco switches). [DDLLC $250 to work with ISE experts to get accurate quote. Implementation costs will be determined as part of that process.]

3.3.6 Unless another solution is implemented (such as ISE), isolate parts of the network one from the other by Firewalling them one from the other with only *necessary* traffic permitted through the firewall (i.e., Waste Water Treatment, Water Treatment, City Hall, Police Department). [Estimate: DDLLC $5000]

Sub-Goal 3.4: Threat Protection

3.4.1: Integrate new Cisco FTD (Firepower Threat Defense) Firewall with Cisco SecureX, and monitor the web-based SecureX console for detected threats. (Integrate other Cisco security products with SecureX as well, if / when they are implemented.) [DDLLC $1k to integrate both the existing Cisco FTD1120 main firewall with SecureX, as well as the newly ordered Cisco FTD1010 firewall for CY, and to monitor weekly for two months.]

3.4.2: Set up new Cisco FTD Firewall with URL category filtering (new capability that was not available on previous ASA Firewall), according to the City's network security policy (if one exists). [Estimate: DDLLC $1000]

3.4.3: Assess current in-use application Crowdstrike, and compare with Cisco AMP For Endpoints (Advanced Malware Protection) capabilities. (The combination of Cisco Umbrella and AMP For Endpoints has proven to be extremely capable of protecting devices from most malware, including Ransom Ware.) [Estimate: DDLLC $1000]

3.4.4: Either purchase and use Penetration testing software internally to detect known security "holes" (e.g., due to missing server Operating System patches), or hire a service to perform this service on a regular basis. [Estimate: TBD]

3.4.5: Create network security policy, if one does not already exist, and train employees. [DDLLC: $5000]

3.4.6: Strongly suggest implementing Cisco Umbrella DNS-layer protection on all supported endpoints. This is inexpensive, extremely effective protection against browsing to Internet locations that host malware (such as Ransom Ware). [Estimate: $6500/yr Subscription, $650/ yr support. DDLLC $3500 to implement.]

3.4.7: Move Windows Server environment to modern version (instead of 2012). [M. Ortiz to complete.]

3.4.8: Modify Windows Server environment to use more secure protocols. [M. Ortiz to complete. If DDLLC assistance is needed, existing general support contract may be utilized.]

Sub-Goal 3.5: Effective Forensics

3.5.1: Unless item 3.4.3 results indicate otherwise, implement Cisco AMP For Endpoints (Advanced Malware Protection). AMP for Endpoints gives visibility into what the malware did, exactly: how it arrived, what processes it started, files it may have modified, etc. It has many protective engines built-in that detect malware actions and block them, real-time. This way, the endpoint is not only protected from most malware up-front, but also can provide critical information on remediation required in case of a brand new "Day 0" attack that was not detectable as malware at the time it entered the network. This can save a lot of time by letting staff know if a device should be re-imaged, or just a few files need to be removed. AMP for Endpoints also includes an effective Anti-Virus. [Note: Cisco Secure Endpoint (formerly AMP For Endpoints") can replace all other endpoint security products presently in use. Estimate: $29k for Annual Subscription and (hopefully) initial installation services, $4455 for annual support contract, DDLLC internal setup assistance: $2500]

3.5.2: Implement Cisco SAL: Security Analytics and Logging (previously StealthWatch Cloud). Not only is SAL critical for Network Visibility, but the logging function is *critical* for having network data available for analyzing security events after-the-fact. [Estimate: $9k/yr for

Annual subscription, with 90 days event storage, $1100/yr for Cisco support, DDLLC integration / configuration: $2250]

Assumed **Most Likely Path Forward for The City of Fort Bragg:**

P1 Items:

Estimate of initial implementation and annual costs: ~ $162,617

Estimate of annual subscriptions/support contracts after first year: ~ $60k

Note: The annual subscription / support cost of certain other endpoint security (i.e., Crowdstrike, Symantec, Carbon Black) products would end and so not all of this annual figure would be “new” costs.