



RFP #5-2021 Information Technology Consulting and Technical Services

For Lexington-Fayette Urban County Government



Prepared by:

Lola Stone

LStone@cbisecure.com

800.747.8585

March 30, 2021

Version 1.1



March 30, 2021

Mr. Todd Slatin
Corporate Procurement
200 East Main Street
Lexington, KY 40507

Re RFP #5-2021 Information Technology Consulting and Technical Services

Dear Mr. Slatin,

Creative Breakthroughs, Inc. (CBI) welcomes this opportunity to submit the following response to the LFUCG RFP **#5-2021 Information Technology Consulting and Technical Services**. CBI specializes in delivering world class cybersecurity consulting services and solutions and are focusing our response on delivering Penetration Testing and Vulnerability Testing services, and Info Security Remediation, and Info Security End-User Training.

Our team consists of industry leading and certified professionals specializing in these services. CBI has over 29 years of experience providing these services to government, healthcare, manufacturing, education organizations of all sizes. CBI was founded in 1991 and is headquartered in Ferndale, Michigan with a specific focus on the Central US region. We have offices in Lexington, Nashville, Detroit, and Cincinnati.

CBI is partnered with Esource Resources, and minority-owned company for this proposal. Esource Resource is by owned by an African American who is also disabled and veteran. Details of this partnership are included in this proposal.

This response details the history of CBI and explains the process for service delivery. You will also find biographies of the personnel who will be engaged on LFUCG projects, reference accounts of where we have performed these services, and our understanding and commitment to the LFUCG philosophies. Please let me know of any questions and/or comments that you or your team have. We will be happy to provide explanations or expansion on any of our offerings.

We look forward to hearing from you soon.

Respectfully,

Lola Stone

Lola Stone
Account Manager | CBI
502.295.4294
lstone@cbisecure.com



Firm Submitting Proposal: **Creative Breakthroughs, Inc.**

Complete Address: **1200 Woodward Heights** **Ferndale** **48220**
Street City Zip

Contact Name: **Lola Stone** Title: **Senior Account Executive**

Telephone Number: **(502) 295-4294** Fax Number: **(248) 256-3335**

Email address: **lstone@cbisecure.com**



Table of Contents

Executive Summary.....	5
Company Information	6
Company Name and Address.....	6
Technology and Consulting Business Partners	6
Staff Resumes/Team Bios	7
CBI Affirmative Action Plan	11
WORKFORCE ANALYSIS FORM.....	12
Description of Services	13
Service Focus.....	14
Service Summary	14
Cost of Services.....	16
General Provisions.....	25
Affidavit	26
Insurance Requirements	28
APPENDIX A: Supporting Minority Partner Information	29
APPENDIX B: Sample Statement of Work.....	39
CBI differentiators.....	39
Minority Partner	39
Statement of Work.....	40
Objectives	40
Scope and Approach	40
Approach and Methodology.....	42
Service Delivery Features.....	42
Service Methodology	43
Penetration Testing Overview	43
Project Deliverables	44
Project Management	44



Executive Summary

Creative Breakthrough, Inc. (CBI) is pleased to provide this proposal to LFUCG specifically for your Information Security Services projects. The CBI team has done our best to submit a proposal that follows your guidelines, is easy to read, and provides the necessary information. We welcome further interaction with your team should you have questions.

CBI is experienced and responding to this RFP for the following Information Security Services projects:

- Penetration Testing
- Vulnerability Testing
- Info Security Remediation
- Info Security End-User Training

This RFP response contains our company information including a sample of our team bios, references, human resources information, description of services, a sample Statement of Work, and minority partner information and required forms.

The following highlights our differentiators and strengths:

- Specialized firm with 100% of resources focused on cybersecurity
- Have performed over 2800 projects like the ones listed.
- Exceptionally strong team with experience as former CISOs, military cybersecurity, and related roles
- In business for 30 years
- Heavy concentration of clients located in the Midwest with many in government
- Minority and veteran participation- we have a minority partner (Esource Resources) we work often that is owned by an African American who is also disabled and a veteran. They will be subcontracted to provide project management services for work we do with LFUCG. Their services will be at least 10% of the total project cost. Esource Resources' credentials and information have been included in this RFP response in Appendix A.
- Our Passion-CBI created the red team 17 years ago because we were passionate about information security and ethical hacking. We felt back then that the demand for penetration testing services would increase and we wanted to position ourselves for success. We did so by employing the best and the brightest in the industry. Today, most firms involved in cyber security and penetration testing got into this space to profit. We got into this space 17 years ago because we thought “how cool would it be if we could employ a team of ethical hackers and get paid to hack!”
- Our Skillset - Our list of certifications, such as OSCP/SANS/CISSP, are important qualifiers to many customers but we do not believe they are the only ones. The skillset CBI has is by far one of our strongest differentiators. By employing previous application development as active red team application penetration testers, we’ve able to provide remediation guidance that goes far beyond what a vulnerability scanning tool is going to recommend.



- Our Reports - CBI has worked very hard over the years to create reports of which we are proud. Our customers constantly tell us they appreciate our ability to translate these findings into interpretable content, while still maintaining the necessary technical remediation data. As mentioned before, we are proud of our reports and have included a sample as part of our response.

Company Information

Company Name and Address

Creative Breakthroughs, Inc.
1200 Woodward Heights
Ferndale, MI 48220

Technology and Consulting Business Partners

CBI partners with the following technology providers;

Accenture	IBM	Saviynt
Broadcom	Imperva	SentinelOne
Check Point	Imprivata	ServiceNow
CrowdStrike	KnowBe4	SolarWinds
CyberArk	LogRhythm	Sophos
Cylance	McAfee	Splunk
Darktrace	MicroFocus	Spy Cloud
Deep Instinct	Mimecast	SumoLogic
Duo Security	Mobile Iron	Tanium
Elastic	Okta	Tenable
Ericom	PaloAlto	Thales/Gemalto
Exabeam	PKware	Thycotic
FireEye	Proofpoint	Trend Micro
Firemon	Q1 Dynamics	Tufin
Forcepoint	Qualys	Valimail
Forescout	Quantum	Varonis
Fortinet	Rapid7	Veeam
Fortinet	RiskIQ	Veritas
Gigamon	RSA	Zscaler
HCL	SafeBreach	

For the services proposed, CBI will not be utilizing other consulting partners. All work will be performed by CBI staff.



Staff Resumes/Team Bios

The CBI Team is comprised of several highly skilled and qualified security consultants. A sample of these resources background and skillset is included below. Specific names have been anonymized, where necessary, to protect the confidentiality of our team and resources. Specific names will be released upon project award.



Shaun Bertrand VP, Advanced Testing Services	
Credentials	<ol style="list-style-type: none"> 1. CISSP 15+ years 2. President / Founder of Grand Traverse ISSA Chapter 3. Adjunct professor at University of Michigan and Eastern Michigan University 4. Bug Bounty Enthusiast
Skills Summary	Penetration Testing, Red Teaming, Social Engineering, Web Applications / OWASP, Evasion, Obfuscation, ICS/SCADA, IoT, Leadership. Ability to work directly with CxO's, board members, and executive management.



Team Leader Senior Consultant	
Credentials	<ol style="list-style-type: none"> 1. Bachelor's Degree in Information Assurance Eastern Michigan University, CISSP 2. Former DoD background. TS/SCI Cat II Security Clearance 3. Frequent Speaker at security conferences
Skills Summary	Penetration Testing, Red Teaming, Social Engineering, Web Applications / OWASP, Physical Security, Evasion, Obfuscation, ICS/SCADA, Leadership.



Team Leader Senior Consultant	
Credentials	<ol style="list-style-type: none"> 1. Offensive Security Certified Professional – OSCP 2. GIAC Web Application Penetration Tester – GWAPT 3. Certified Penetration Testing Engineer – C PTE 4. Certified Information Systems Auditor – CISA 5. ITIL v.3 Foundations 6. Adjunct Professor; Ferris State University 7. B.S. Computer Information Systems Master Business Administration – Advanced Studies Information Security and Network Management
Skills Summary	Penetration Testing, Red Teaming, Social Engineering, Web Applications / OWASP, Evasion, Obfuscation, ICS/SCADA, IoT, Encryption, Leadership.



Consultant	
Credentials	<ol style="list-style-type: none"> 1. Offensive Security Web (OSWE), GIAC Certified Incident Handler (GCIH) GIAC Certified UNIX Security Administrator (GCUX) CEH GIAC Network Forensic Analyst (GNFA) GIAC Continuous Monitoring Certification (GMON) GIAC Penetration Tester (GPEN) GIAC Certified Incident Handler (GCIH) GIAC Web Application Penetration Tester (GWAPT) 2. MBA Management of Information Technology, B.S. Computer Science
Skills Summary	Web Applications / OWASP, Mobile Applications, API Testing, Red Teaming, Evasion, Obfuscation, IoT, Encryption.



Consultant	
Credentials	<ol style="list-style-type: none"> 1. Offensive Security Certified Professional (OSCP) 2. Certified Information Systems Auditor (CISA) 3. Certified Information Systems Security Professional (CISSP) 4. Risk and Information System Control (CRISC) 5. ISACA CISA instructor
Skills Summary	Penetration Testing, Red Teaming, Social Engineering, Web Applications / OWASP, Evasion, Obfuscation, ICS/SCADA, IoT, Encryption.



David Mamikonyan – Senior VP Architecture and Implementation	
Credentials	<ol style="list-style-type: none"> 1. Advise and recommend security technologies and architectures 2. Review and map security controls to industry regulations and standards (PCI, SOX, SANS 20) 3. Provides security awareness training 4. Designer of complex security solutions to achieve compliance, mitigate risk and ensure satisfactory security audits
Skills Summary	Advanced technical expertise in cybersecurity, analysis, design, and implementation; Advanced expertise in 24 by 7 operational management. Experienced in leading highly skilled engineers, implementation teams and SOC analysts



Consultant	
Credentials	<ol style="list-style-type: none"> 1. Certified Information Security Manager (CISM) 2. Certified Data Privacy Solutions Engineer (CDPSE) 3. Certified Identity Management Professional (CIMP) 4. ITIL Foundation v3 (ITIL)
Skills Summary	<ul style="list-style-type: none"> • Information Security Governance; Program Development & Management; Incident Management; Risk Management; Controls Audit Assurance • Privacy by design (bridging Technology and Legal); Data Lifecycle; Data Privacy; Privacy Architecture; Privacy Best Practices; Privacy Governance • Identity Management; Threat Management; Project Management; IAM Architecture, Protocols, and Standards; Compliance Assurance • Organizational Strategy, Design, Transition, Operation, Improvement; IT Service Management • Organizational Leadership, Strategy, & Development



Angel Swaynie -- Project Manager	
Credentials	<ol style="list-style-type: none"> 1. Bachelor of Business Administration 2. Certifications: <ul style="list-style-type: none"> • Project Management Professional • SAFe 4 Agilist • Business Agility Foundations
Skills Summary	<ul style="list-style-type: none"> • Statement of Work Analysis • Budget Analysis • Stakeholder Identification • Development of Schedule • Development of Budget • Development of Project Plan • Development of Project Status Reports • Facilitate Communication Touchpoints • Monitor Project Progress • Monitor Quality of Delivery • Monitor & Execute Change Requests • Confirmation of Report Delivery • Initiation of Project Close • Maintenance of Project Repository



Other Information

- a. location of staff – **all CBI staff are in the continental United States.**
- b. hourly rate of pay – **See Cost of Services**
- c. travel and living expenses – **invoiced at cost, not to exceed \$2,500 per week**
- d. indicate if the staff is sub-contracted or an employee – **all consultants are full-time CBI employees**

References*

Macomb County
1 South Main
Mount Clemens, MI 48043

Northside Hospital
1000 Johnson Ferry Road NE,
Sandy Springs, Atlanta

*Due to the confidential nature of our business in cybersecurity, we honor our clients' requests only to provide contact names, phone numbers, and email information once we can give them a "heads up" that someone will be calling regarding the work we have done for them. We are happy to provide this information at that time.



CBI Affirmative Action Plan

Diversity, Equity and Inclusion



At CBI we know that celebrating a diverse team in an inclusive work culture is key to the Core Values our business is built upon, and to providing our clients with world-class professional services. The unique skills, knowledge, backgrounds, and perspectives of our team members are at the core of our business and the value we provide.

Our Core Values

Authenticity
Client First
Blue-Collar Work Ethic
Performance-Based Culture

01

04

Detroit Area Rescue Team

As a Detroit-based organization, CBI is dedicated to giving back to the communities in which we work and live.

02

05

WomSA

CBI is a primary sponsor of WomSA, the Women's Security Alliance, dedicated to the success of women in cybersecurity.

03

06

Veteran-Friendly Employer

CBI is proud to be recognized by the Michigan Veterans Affairs Agency as a Veteran-Friendly Employer.

Workforce Well-being

CBI is proud to offer various employee programs to support the mental health of our team members and their families.

Inclusion and Belonging

Inclusion is everyone's job. All CBI team members complete education and training on the importance of and cultivating a safe and inclusive work environment.





WORKFORCE ANALYSIS FORM

Name of Organization: Creative Breakthroughs, Inc.

Categories	Total	White (Not Hispanic or Latino)		Hispanic or Latino		Black or African American (Not Hispanic or Latino)		Native Hawaiian and Other Pacific Islander (Not Hispanic or Latino)		Asian (Not Hispanic or Latino)		American Indian or Alaskan Native (not Hispanic or Latino)		Two or more races (Not Hispanic or Latino)		Total	
		M	F	M	F	M	F	M	F	M	F	M	F	M	F	M	F
Administrators	0																
Professionals	71	47	17	1	1	2						1	2			52	1
Superintendents	0																
Supervisors	24	18	5		1											18	6
Foremen	0																
Technicians	0																
Protective Service	0																
Paraprofessionals	0																
Office/Clerical	1		1														1
Skilled Craft	0																
Service/Maintenance	0																
Total:	96																

Prepared by: Janae Brosko, HRBP
(Name and Title)

Date: 3 / 16 / 2021
Revised 2015-Dec-15



Description of Services

CBI is a trusted cybersecurity advisor to many of the world's top organizations. Founded in 1991, CBI provides innovative and customizable solutions to help ensure data is secure, compliant, and available. We take an advisory-led approach to safeguard our clients against the evolving threat landscape—providing comprehensive visibility into the maturity of their security capabilities and addressing gaps before they can be exploited. We are dedicated to the relentless pursuit of mitigating risks and elevating cybersecurity for companies across all sizes and sectors.



Years of Service

CBI has been delivering security services and solutions since 1991.

- Information Security
- Policy Development and Review
- Planning and Analysis
- Penetration Testing
- Vulnerability Testing
- Risk Management Assessment
- Info Security Audit and Compliance
- Info Security Remediation
- Info Security End-User Training



Service Focus

CBI’s focus is cybersecurity. Our proposal, therefore, addresses the LFUCG’s desire to find qualified consultants to deliver superior information security services. We are proposing to deliver the following;

Information Security	Policy Development and Review Planning and Analysis Penetration Testing Vulnerability Testing Risk Management Assessment Info Security Audit and Compliance Info Security Remediation Info Security End-User Training	See Below for Hourly Rates.	
----------------------	--	-----------------------------	--

Service Summary

Penetration Testing/Vulnerability Testing

CBI has been conducting penetration tests and vulnerability assessments for the last 16 years. As an organization we were at the front lines of helping to contribute to various testing frameworks and standards such as PTES, NIST, and OWASP. Our strong reputation in this industry has been established because of our long track record of conducting successful and valuable penetration tests for enterprise organizations. We employ highly skilled penetration testers and application developers on the red team during this time to ensure we deliver a superior service edge compared to other vendors.

CBI has conducted over 1,600 engagements of similar size, scope, and complexity. CBI also has extensive experience in all industry verticals, government, healthcare, manufacturing, finance, and defense. Every individual on the CBI red team has the relevant and trustworthy credentials and certifications required for such sensitive testing. We have resources with Top Secret clearance for various defense contracts on which the CBI Red Team is engaged. Our firm believes that organizations need more than just tactical guidance. We understand that a strategic focus is also required to put our customers on a more proactive path. More importantly, we position our testing as an opportunity to better evaluate the effectiveness of controls. By being able to leverage guidance from CBI on how to tune existing controls, it is possible to establish a better return on the investments that have been made.

In addition, the CBI Red Team has all the industry certifications required to demonstrate our experience and expertise in this space, including but not limited to; CISSP, OSCP, OSCE, SANS penetration testing, SANS web application testing, HTCIA, InfraGard membership, ISSA membership, Michigan Cyber Civilian Corps (MiC3), and many other certifications and affiliations. Various CBI team members, including the Sr. Vice President, have recently been awarded medals from the Pentagon and Army for their efforts in an invitation only Bug Bounty program.



CBI delivers Penetration Testing and Vulnerability Testing services in a structured methodology. The approach in which the penetration test will be conducted will be either White hat (full information provided), black hat (no information provided), or gray hat (some information provided). Depending on LFUCG's requirements, CBI is experienced in providing the following:

- External Penetration Test - penetration test against the external (WAN) environment.
- Internal Penetration Test - penetration test against the internal (LAN) environment.
- Social Engineering - security awareness testing through simulated social engineering campaigns.
- Lateral Movement & Privilege Escalation - when an external system is compromised, the next attack vector is to move laterally and escalate privileges.
- Wireless Assessment - evaluation and analysis of security threats and risks related to the in scope wireless networks.
- Physical Assessment - assessment of physical security controls and countermeasures.
- Post Penetration Testing Collaboration - upon completion of the penetration testing engagement, CBI will facilitate onsite purple team collaboration to review and improve detection capabilities.

Please refer to Appendix B for a sample statement of work and further details.

Information Security Remediation

CBI helps you quickly investigate incidents and thoroughly remediate the environment, so you can get back to what matters most: your business. CBI successfully delivers security remediation services by first understanding the specific challenge at hand so we can best prioritize and specify the corrective action that will maximize and elevate your security posture. Our approach is designed to assess current IR capabilities, ensure you have a trusted partner on standby before an incident occurs, reduce the time it takes to respond to an incident, minimize its impact and help you recover faster now, and in the future.

Information Security End-User Training

CBI provides the option of building a custom security end-user training class and offering solutions from top end-user security training partners, KnowB4 and Proofpoint. Depending on LFUCG's requirements, whether to meet unique security training requirements or offer a more generalized approach, CBI will deliver training that best meets your overall strategic needs.



Cost of Services

Depending on project requirements, CBI will provide a team comprised of the following consultant types to the Client to perform services. CBI will also utilize fixed fee pricing whenever project requirements will allow. Any additional time or tasks required with all projects will be accompanied by a change order.

Vulnerability Testing/PEN Testing Service Categories	Hourly Rate
Director	\$350
Consultant	\$255
Analyst	\$200
Project Manager	\$175

Travel and expenses will be billed at actual cost in addition to the professional fees above.

Please see Attachment B for other details.

Risk Remediation and Security Awareness Service Categories	Hourly Rate
Director	\$325
Consultant	\$325
Project Manager	\$175

Travel and expenses will be billed at actual cost in addition to the professional fees above.



Attachment A

Attachment A contains a list of the technologies used by the Lexington-Fayette Urban County Government. Please enter the average experience (years) of qualified employees who may provide IT services in the Experience column. You may enter the number of employees the average applies to, e.g., “5 years, 3 employees”. The Comments column should be used to provide LFUCG with information that should be considered during the vendor selection process.

Please note that CBI does not provide any services listed in Attachment A. For your convenience, CBI is showing only the table row that identifies the services we are proposing.

Attachment B

Attachment B contains a list of services the Lexington-Fayette Urban County Government may need provided. Please use the notes column to identify any information that should be considered during the vendor selection process. Exceptions to billing should be included in the notes, e.g., weekend rate adjustments.

Service		Rate	Notes
Information Security	Policy Development and Review Planning and Analysis Penetration Testing Vulnerability Testing Risk Management Assessment Info Security Audit and Compliance Info Security Remediation Info Security End-User Training	See Page 12.	Project work can also be delivered on a fixed-bid cost basis.



LFUCG MWDBE PARTICIPATION FORM
Bid/RFP/Quote Reference #__ RFP #5-2021 _____

The MWDBE subcontractors listed have agreed to participate on this Bid/RFP/Quote. If any substitution is made or the total value of the work is changed prior to or after the job is in progress, it is understood that those substitutions must be submitted to Central Purchasing for approval immediately.

MWDBE Company, Name, Address, Phone, Email	Work to be Performed	Total Dollar Value of the Work	% Value of Total Contract
1. Esource Resources, LLC, 7114 Lakeview Parkway W Dr. Indianapolis, IN 46268 Kimberly Everett 317-402-5579 kimberly.everette@esourcesresources.net	Project Management	To Be Determined	10%
2.			
3.			
4.			

The undersigned company representative submits the above list of MWDBE firms to be used in accomplishing the work contained in this Bid/RFP/Quote. Any misrepresentation may result in the termination of the contract and/or be subject to applicable Federal and State laws concerning false statements and false claims.

Creative Breakthroughs, Inc. _____
Company

Julie Spiller _____
Company Representative

March 16, 2021 _____
Date

VP Bus Dev & Community Outreach
Title



LFUCG MWDBE SUBSTITUTION FORM
Bid/RFP/Quote Reference #_ RFP #5-2021 _____

The substituted MWDBE subcontractors listed below have agreed to participate on this Bid/RFP/Quote. These substitutions were made prior to or after the job was in progress. These substitutions were made for reasons stated below and are now being submitted to Central Purchasing for approval. By the authorized signature of a representative of our company, we understand that this information will be entered into our file for this project.

SUBSTITUTED MWDBE Company Name, Address, Phone, Email	MWDBE Formally Contracted/ Name, Address, Phone, Email	Work to Be Performed	Reason for the Substitution	Total Dollar Value of the Work	% Value of Total Contract
1. Not applicable at this time					
2.					
3.					
4.					

The undersigned acknowledges that any misrepresentation may result in termination of the contract and/or be subject to applicable Federal and State laws concerning false statements and false claims.

CBI acknowledges this form and will complete it when applicable.

Creative Breakthroughs, Inc. _____
Company

Julie Spiller _____
Company Representative

March 16, 2021 _____
Date

VP Bus Dev & Community Outreach
Title



MWDBE QUOTE SUMMARY FORM
Bid/RFP/Quote Reference #_ RFP #5-2021 _____

The undersigned acknowledges that the minority subcontractors listed on this form did submit a quote to participate on this project.

Company Name Creative Breakthroughs, Inc.	Contact Person Lola Stone
Address/Phone/Email 1200 Woodward Heights, Ferndale, MI 48220 lstone@cbisecure.com 502-295-4294	Bid Package / Bid Date RFP #5-2021

MWDBE Company Address	Contact Person	Contact Information (work phone, Email, cell)	Date Contacted	Services to be performed	Method of Communication (email, phone meeting, ad, event etc.)	Total dollars \$\$ Do Not Leave Blank (Attach Documentation)	MBE * AA HA AS NA Female	Veteran
Esource Resources, LLC, 7114 Lakeview Parkway W Dr. Indianapolis, IN 46268	Kimberly Everett	317-402-5579	3/16/21	Project Management	email	Total dollars will Equal 10% of Total project.	AA	Yes, Also disabled

(MBE designation / AA=African American / HA= Hispanic American/AS = Asian American/Pacific Islander/ NA= Native American)

The undersigned acknowledges that all information is accurate. Any misrepresentation may result in termination of the contract and/or be subject to applicable Federal and State laws concerning false statements and claims.

***CBI acknowledges this form, has communicated with our primary MWDBE partner, and will obtain specific quotes when project is identified.**

Creative Breakthroughs, Inc. _____
Company

Julie Spiller _____
Company Representative

March 16, 2021 _____
Date

VP Bus Dev & Community Outreach
Title



LFUCG SUBCONTRACTOR MONTHLY PAYMENT REPORT

The LFUCG has a 10% goal plan adopted by city council to increase the participation of minority and women owned businesses in the procurement process. In order to measure that goal LFUCG will track spending with MWDBE vendors on a monthly basis. By the signature below of an authorized company representative, you certify that the information is correct, and that each of the representations set forth below is true. Any misrepresentation may result in termination of the contract and/or prosecution under applicable Federal and State laws concerning false statements and false claims. Please submit this form monthly to the Division of Central Purchasing/ 200 East Main Street / Room 338 / Lexington, KY 40507.

Bid/RFP/Quote # RFP #5-2021 _____
Total Contract Amount Awarded to Prime Contractor for this Project _____

Project Name/ Contract #	Work Period/ From: _____ To: _____
Company Name:	Address: _____
Federal Tax ID:	Contact Person: _____

Subcontractor Vendor ID (name, address, phone, email)	Description of Work	Total Subcontract Amount	% of Total Contract Awarded to Prime for this Project	Total Amount Paid for this Period	Purchase Order number for subcontractor work (please attach PO)	Scheduled Project Start Date	Scheduled Project End Date

By the signature below of an authorized company representative, you certify that the information is correct, and that each of the representations set forth below is true. Any misrepresentations may result in the termination of the contract and/or prosecution under applicable Federal and State laws concerning false statements and false claims.

CBI acknowledges this form and will provide completed documentation at monthly intervals as appropriate.

Creative Breakthroughs, Inc. _____
Company

Julie Spiller _____
Company Representative

March 16, 2021 _____
Date

VP Bus Dev & Community Outreach
Title



LFUCG STATEMENT OF GOOD FAITH EFFORTS

Bid/RFP/Quote #_ RFP #5-2021 _____

By the signature below of an authorized company representative, we certify that we have utilized the following Good Faith Efforts to obtain the maximum participation by MWDBE business enterprises on the project and can supply the appropriate documentation.

JS Advertised opportunities to participate in the contract in at least two (2) publications of general circulation media; trade and professional association publications; small and minority business or trade publications; and publications or trades targeting minority, women and disadvantaged businesses not less than fifteen (15) days prior to the deadline for submission of bids to allow MWDBE firms to participate.

CBI has reached out to multiple firms and organizations to partner with on in working with LFUCG.

JS Included documentation of advertising in the above publications with the bidders good faith efforts package

Please see Appendix A: Supporting Minority Partner Information for further details.

JS Attended LFUCG Central Purchasing Economic Inclusion Outreach event
A CBI representative has not yet attended the LFUCG Central Purchasing Economic Inclusion Outreach event but plans to attend the next one that is scheduled.

JS Attended pre-bid meetings that were scheduled by LFUCG to inform MWDBEs of subcontracting opportunities

CBI plans to attend pre-bid meetings that are scheduled by LFUCG to inform MWDBEs of subcontracting opportunities. To our knowledge, these meeting have not been scheduled in relation to RFP #5-2021.

JS Sponsored Economic Inclusion event to provide networking opportunities for prime contractors and MWDBE firms

CBI has not yet sponsored an Economic Inclusion event but will make efforts to support this as opportunities arise.

JS Requested a list of MWDBE subcontractors or suppliers from LFUCG Economic Engine and showed evidence of contacting the companies on the list(s).

CBI requested and has received the list of MWDBE subcontractors from Sherita Miller. Evidence is provided in Appendix A.

JS Contacted organizations that work with MWDBE companies for assistance in finding certified MWDBE firms to work on this project. Those contacted and their responses should be a part of the bidder's good faith efforts documentation.

CBI has reached out to several organizations and companies. Evidence has been provided in Appendix A.



- __JS__ Sent written notices, by certified mail, email, or facsimile, to qualified, certified MWDBEs soliciting their participation in the contract not less than seven (7) days prior to the deadline for submission of bids to allow them to participate effectively.
CBI has sent written notices to several organization and companies. Evidence has been provided in Appendix A.
- __JS__ Followed up initial solicitations by contacting MWDBEs to determine their level of interest.
CBI has followed up and secured a minority partner (Esource Resources) for our interactions with LFUCG. We are also following up on the other organizations in case we need other partners to service LFUCG.
- __JS__ Provided the interested MWBDE firm with adequate and timely information about the plans, specifications, and requirements of the contract.
CBI is communicating details to interested MWBDE firms.
- __JS__ Selected portions of the work to be performed by MWDBE firms in order to increase the likelihood of meeting the contract goals. This includes, where appropriate, breaking out contract work items into economically feasible units to facilitate MWDBE participation, even when the prime contractor may otherwise perform these work items with its own workforce
Acknowledged by CBI.
- __JS__ Negotiated in good faith with interested MWDBE firms not rejecting them as unqualified without sound reasons based on a thorough investigation of their capabilities. Any rejection should be so noted in writing with a description as to why an agreement could not be reached.
Acknowledge by CBI.
- __JS__ Included documentation of quotations received from interested MWDBE firms which were not used due to uncompetitive pricing or were rejected as unacceptable and/or copies of responses from firms indicating that they would not be submitting a bid.
Acknowledged by CBI.
- __JS__ Bidder has to submit sound reasons why the quotations were considered unacceptable. The fact that the bidder has the ability and/or desire to perform the contract work with its own forces will not be considered a sound reason for rejecting a MWDBE quote. Nothing in this provision shall be construed to require the bidder to accept unreasonable quotes in order to satisfy MWDBE goals.
Acknowledged by CBI.
- __JS__ Made an effort to offer assistance to or refer interested MWDBE firms to obtain the necessary equipment, supplies, materials, insurance and/or bonding to satisfy the work requirements of the bid proposal
Acknowledged by CBI.
- __JS__ Made efforts to expand the search for MWDBE firms beyond the usual geographic boundaries.



CBI has reached out to many firms in many geographies. We have multiple MWDBE firms with currently partner with.

JS Other - any other evidence that the bidder submits which may show that the bidder has made reasonable good faith efforts to include MWDBE participation.

Please see Appendix A for further documentation.

Failure to submit any of the documentation requested in this section may be cause for rejection of bid. Bidders may include any other documentation deemed relevant to this requirement. Documentation of Good Faith Efforts are to be submitted with the Bid, if the participation Goal is not met.

The undersigned acknowledges that all information is accurate. Any misrepresentations may result in termination of the contract and/or be subject to applicable Federal and State laws concerning false statements and claims.

Creative Breakthroughs, Inc. _____
Company

Julie Spiller _____
Company Representative

March 16, 2021 _____
Date

VP Bus Dev & Community Outreach
Title



General Provisions

Following is our standard language for Limitation of Liability. CBI welcomes the opportunity to discuss further with LFUCG.

1. LIMITATIONS OF LIABILITY.

- 1.1** IN NO EVENT, REGARDLESS OF THE LEGAL BASIS FOR THE CLAIM, WILL EITHER CBI OR CLIENT, OR THEIR AFFILIATES, OR ANY OF THEIR SHAREHOLDERS, DIRECTORS, OFFICERS, EMPLOYEES OR AGENTS, BE LIABLE TO THE OTHER, WHETHER IN CONTRACT OR IN TORT OR UNDER ANY OTHER LEGAL THEORY (INCLUDING, WITHOUT LIMITATION, STRICT LIABILITY AND NEGLIGENCE), FOR ANY INCIDENTAL, CONSEQUENTIAL, SPECIAL, EXEMPLARY OR INDIRECT DAMAGES, LOSSES, EXPENSES OR COSTS OF ANY KIND, NOR, WITHOUT LIMITATION, LOSS OF PROFITS OR REVENUES, LOSS OF USE, LOSS OR CORRUPTION OF DATA, BUSINESS INTERRUPTION, OR ANY OTHER INDIRECT, SPECIAL, EXEMPLARY, PUNITIVE, MULTIPLE, INCIDENTAL, CONSEQUENTIAL OR SIMILAR DAMAGES, ARISING OUT OF OR IN CONNECTION WITH THE AGREEMENT, ANY CBI OFFER DOCUMENT, QUOTE OR OTHERWISE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.
- 1.2** NOTWITHSTANDING ANYTHING HEREIN TO THE CONTRARY, IN NO EVENT WILL CBI'S OR ITS AFFILIATES', OR THEIR SHAREHOLDERS, DIRECTORS, OFFICERS, EMPLOYEES' OR AGENTS', LIABILITY UNDER THE AGGREGATE CLAIMS MADE BY CLIENT EXCEED AN AMOUNT EQUAL TO (A) THE TOTAL AMOUNT OF FEES ACTUALLY PAID OR OWED FOR THE PRODUCT UNDER THE CBI OFFER DOCUMENT GIVING RISE TO THE CLAIM; OR (B) THE TOTAL AMOUNT OF FEES ACTUALLY PAID FOR THE PRIOR TWELVE (12) MONTH PERIOD FOR THE SERVICES UNDER THE CBI OFFER DOCUMENT GIVING RISE TO THE CLAIM.
- 1.3** CLIENT UNDERSTANDS AND AGREES THAT THE FOREGOING LIMITATIONS OF LIABILITY ARE ESSENTIAL ELEMENTS OF THIS AGREEMENT AND THAT IN THE ABSENCE OF SUCH LIMITATIONS THE MATERIAL AND ECONOMIC POSITION OF THE CBI OFFER DOCUMENT WOULD BE SUBSTANTIALLY DIFFERENT.



Affidavit

AFFIDAVIT

Comes the Affiant, Steve Barone, CEO, and after being first duly sworn, states under penalty of perjury as follows:

1. His/her name is Lola Stone and he/she is the individual submitting the proposal or is the authorized representative of Creative Breakthroughs, Inc. the entity submitting the proposal (hereinafter referred to as "Proposer").
2. Proposer will pay all taxes and fees, which are owed to the Lexington-Fayette Urban County Government at the time the proposal is submitted, prior to award of the contract and will maintain a "current" status in regard to those taxes and fees during the life of the contract.
3. Proposer will obtain a Lexington-Fayette Urban County Government business license, if applicable, prior to award of the contract.
4. Proposer has authorized the Division of Central Purchasing to verify the above-mentioned information with the Division of Revenue and to disclose to the Urban County Council that taxes and/or fees are delinquent or that a business license has not been obtained.
5. Proposer has not knowingly violated any provision of the campaign finance laws of the Commonwealth of Kentucky within the past five (5) years and the award of a contract to the Proposer will not violate any provision of the campaign finance laws of the Commonwealth.
6. Proposer has not knowingly violated any provision of Chapter 25 of the Lexington-Fayette Urban County Government Code of Ordinances, known as "Ethics Act."

Continued on next page



7. Proposer acknowledges that "knowingly" for purposes of this Affidavit means, with respect to conduct or to circumstances described by a statute or ordinance defining an offense, that a person is aware or should have been aware that his conduct is of that nature or that the circumstance exists.

Further, Affiant sayeth naught.

Steve Barone

STATE OF Michigan

COUNTY OF Macomb

The foregoing instrument was subscribed, sworn to and acknowledged before me by Steve Barone on this the 23 day of March, 2021.

My Commission expires: 8-6-22

[Signature]
NOTARY PUBLIC, STATE AT LARGE

DANIELLE TATUM
NOTARY PUBLIC - STATE OF MICHIGAN
COUNTY OF MACOMB
My Commission Expires Aug. 6, 2022
Acting in the County of _____



Insurance Requirements

Please note that CBI has reviewed the insurance requirements and will comply as specified. Upon receipt of a project award, we will forward a Certificate of Insurance for your records.



APPENDIX A: Supporting Minority Partner Information

RE: LFUCG RFP #5-2021

Kimberly Everette <kimberly.everette@esourceresources.net>
To: Julie Spiller

Reply

Follow up. Start by Tuesday, March 16, 2021. Due by Tuesday, March 16, 2021.

- 2020 Mid-StatesMSDC Certificate - Esource Resources, LLC.pdf 82 KB
- 2019-2022 SDVOB Certification.pdf 155 KB
- Capability Statement 2021.pdf 283 KB

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe. Please forward any suspicious content to support@cbisecure.com.

Julie,
We would love to partner with you as your MBE partner. I have attached our certifications. Please let me know if you need anything else. Below is our GSA info.

GSA-IT Schedule 70

GSA Section 70
47QTCA19D006W
DUNS Number: 141045653

Kimberly Everette

cell. 317 402 5579 || fax. 800 454 7091

email. Kimberly.everette@esourceresources.net || web. www.esourceresources.net



GSA Schedule

PSS Schedule (70 Corp): 47QTCA19D006W
SIN 132-56 Health Information Technology Services
SIN 132-51 Information Technology Professional Services

Esource Resources 7114 Lakeview Parkway West Dr., Indianapolis, IN 46268

certified MBE, DBE & SDVOB

From: Julie Spiller <jspiller@cbisecure.com>
Sent: Tuesday, March 16, 2021 11:15 AM
To: Kimberly Everette <kimberly.everette@esourceresources.net>
Subject: LFUCG RFP #5-2021

Hi Kimberly, attached is an RFP that CBI is responding to for cybersecurity services. We would like to partner with Esource Resources for your project management services on these projects if we are selected. The RFP is not for a specific project at this time but to become an approved partner. Once we have been selected and specific projects are called out, we will work with you to obtain further information as required. Please respond with your acknowledgement and interest in working with us as well as your applicable certifications.

Thank you,
Julie

 Julie Spiller
VP Business Development & Community Outreach
m: 586.915.2063
w: cbisecure.com



THIS CERTIFIES THAT

Esource Resources, LLC

dba Esource Resources, LLC



* Nationally certified by the: **MID-STATES MINORITY SUPPLIER DEVELOPMENT COUNCIL**

*NAICS Code(s): 561330; 561320; 541512; 541511; 423430

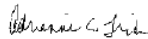
* Description of their product/services as defined by the North American Industry Classification System (NAICS)

05/10/2020

Issued Date

IN01469

Certificate Number


Adrienne Trimble



05/10/2021

Expiration Date

Carolyn E. Mosby, President/CEO

By using your password (NMSDC issued only), authorized users may log into NMSDC Central to view the entire profile: <http://nmsdc.org>

Certify, Develop, Connect, Advocate.

* MBEs certified by an Affiliate of the National Minority Supplier Development Council, Inc.®



DEPARTMENT OF VETERANS AFFAIRS
Center for Verification and Evaluation
Washington DC 20420

5/8/2019
In Reply Refer To: **00VE**

Mr. Eddie L. Rivers, Jr.
Esource Resources, LLC
DUNS: 141045653
9150 Harrison Park Ct., Ste. B
Indianapolis, IN 46216

Dear Mr. Rivers:

On behalf of the U.S. Department of Veterans Affairs (VA), Center for Verification and Evaluation (CVE), I am writing to inform you that your application for reverification has been approved. Esource Resources, LLC will remain eligible to participate in Veterans First Contracting Program opportunities with VA as a verified Service-Disabled Veteran-Owned Small Business (SDVOSB).

This verification is valid for three (3) years from the date of this letter.

Please retain a copy of this letter to confirm Esource Resources, LLC's continued program eligibility in accordance with 38 Code of Federal Regulation (CFR) § 74.12. You may reapply 120 days prior to your new expiration date by logging into <https://www.vip.vetbiz.gov/>.

To promote Esource Resources, LLC's verified status, you may use the following link to download the logo for use on your marketing materials and business cards: https://www.vetbiz.gov/cve_completed_s.jpg. In addition, please access the following link for information on next steps and opportunities for verified businesses: <http://www.va.gov/osdbu/verification/whatsNext.asp>.

While CVE has confirmed that Esource Resources, LLC is presently, as of the issuance of this notice, in compliance with the regulation, Esource Resources, LLC must inform CVE of any changes or other circumstances that would adversely affect its eligibility. Eligibility changes not reported to CVE within 60 days could result in a referral to the Office of Inspector General (OIG), a referral to the Debarment and Suspension Committee, and the initiation of cancellation proceedings—all of which could result in Esource Resources, LLC being removed from the VIP Verification Program.

Please be advised all verified businesses may be required to participate in one or more post-verification audits at CVE's discretion. Additionally, this letter and other

*"World Class Professionals
Enabling Veteran Business Opportunities by Protecting the Veteran Advantage - One Vet at a Time"*



Page 2
Mr. Eddie L. Rivers, Jr.

information pertaining to Esource Resources, LLC's verification application may be subject to Freedom of Information Act (FOIA) requests. However, FOIA disclosures include exceptions regarding the personal privacy of individuals, and VA policy similarly provides limitations on the release of individuals records.

If Esource Resources, LLC receives a negative size determination from the U.S. Small Business Administration (SBA), CVE must act in accordance with 38 CFR § 74.2(e). Also note, if at any time Esource Resources, LLC discovers that it fails to meet the size standards for any NAICS Code(s) listed on its VIP profile, CVE requires such NAICS Code(s) be removed within five (5) business days. If these NAICS Codes are not removed within the allotted five (5) business days, CVE may request SBA conduct a formal size determination. In addition, CVE may initiate a referral to OIG, a referral to the Debarment and Suspension Committee and pursue cancellation proceedings. All of the aforementioned referrals and procedures could result in Esource Resources, LLC being removed from the VIP Verification Program.

Thank you for your service to our country and for continuing to serve America through small business ownership.

Sincerely,

A handwritten signature in black ink that reads "Thomas McGrath". The signature is written in a cursive, flowing style.

Thomas McGrath
Director
Center for Verification and Evaluation



Business Summary

Esource Resources, LLC (Esource) is a VA, Center for Verification and Evaluation (CVE) verified Service-Disabled Veteran-Owned Small Business (SDVOSB) Esource is registered and verified in the Vendor Information Pages (VIP) database. Esource Resources, Inc (Esource), a minority business enterprise (MBE), veteran business enterprise (VBE), service-disabled veteran-owned small business (SDVOSB) and disadvantaged business enterprise (DBE), was founded in Indianapolis in 2002 based on the simple idea of providing high quality, value-adding consulting services. Over the years, we have remained dedicated to this ideal, and are proud of the extensive experience we have built in providing collaborative solutions in healthcare, as well as the private and the public sectors.

CAPABILITIES

A proven track record of successfully managing and executing high-visibility, data-focused projects with subcontract partners.

A staffing approach which emphasizes long-term, direct employment of expert Information Security Consultant staff to foster workforce stability, maintain turnaround time and quality performance standards, and increase client-specific Information Security Consultant expertise.

Sound processes for contract administration (including on-boarding, security clearances, training, and monthly reporting), enabling us to shepherd staff through the lengthy on-boarding process as quickly as possible.

EXPERTISE

To fulfill our client's expectations in any environment, it takes motivated, experienced, and highly skilled people. Esource is committed from day one to the growth and development of our employees. In all of the geographies we operate in, we deliver our solutions using local talent to give back to the economies that have supported us.

Esource focuses on attracting and retaining talented individuals. Esource respects the work our clients are doing for their constituents and the importance of delivering high-value projects on time and within budget.

NAICS Codes

- ▶ 561330-Staffing Services
- ▶ 541511-Applications Software Services





COMPANY INFORMATION

Address: 7114 Lakeview Parkway West Dr
Indianapolis, In 46258

Phone: (317) 402-5579

Cage Code: 3MVH2

Contact name: Kimberly Everette

Tax: 800-454-7091

D&B: 141045653

Email: Kimberlyeverette@esourcesources.net

Customers

IU Health (2009-2017)

1701 N Senate
Boulevard, Indianapolis, IN 46202

Value: \$2,000,000

Type:

561330-Staffing Services
541511-Applications Software
Services

- ▶ Provided EHR (Cerner HIM)
- ▶ Reporting and medical record support
- ▶ Performed Clinical Informatics (including reporting)
- ▶ Operational support
- ▶ End user support reporting needs assessment
- ▶ Delivered improvement and efficiency recommendations to leadership

Eskenazi Health (2015- Current)

720 Eskenazi Ave
Indianapolis, IN 46202

Value: \$2,000,000

Type:

561330-Staffing Services
541511-Applications Software
Services

- ▶ Oversaw and provided resources for the Epic/EHR implementation project.
- ▶ Our Epic trainers supported Eskenazi's EHR Go-Live and activation with an elbow to elbow support role that focused on performance, support and training for the client's customized Epic software platform.
- ▶ Esource worked in other Epic modules (ADT, Beaker, Cadence Validation, Epic Interface
- ▶ (IUHP), in 2017-2018
- ▶ Esource conducted an audit of IUHP's contractual compliance. We provided a detailed report of all exceptions identified along with the implications on the overall population in the scope and presented to Eskenazi Health leadership.

United States Air Force (2020)

The Pentagon Arlington County
Virginia, U.S.

Type:

541430-Graphic Design
Services

- ▶ Created livestream graphics for AFMS SLW livestream conference
- ▶ Editing and reformatting AFMS Historical posters
- ▶ Creates the logo design for the AFMS SLW event
- ▶ Redesigning the 2020 Air Force Toolkit booklet

We developed, implemented and configured solutions required to meet system requirements (i.e. SQL Server, ProClarity, SharePoint Server and Connector, and a user interface capable of: loading multiple forecast iterations from Excel, verifying Sarbanes Oxley requirements, locking finalized forecasts, and configuration of pre-defined data uploads for end users to maintain hierarchy data). Esource also delivered Microsoft SQL Server reporting, integration, and analysis services.





Submission to MEDI for minority partner (<http://www.medisuccess.info/about-us/>)



- HOME
- ABOUT US
- EVENTS & ONLINE REGISTRATION
- FAQ
- TRAININGS AND SERVICES



Your entry has been successfully sent.

Your entered data.:

Name:

Julie Spiller

E-mail Address:

jspiller@cbisecure.com

Phone:

586-915-2063

General question:

Hello, we are seeking a partnership with a MWDBE firm to assist us with cybersecurity projects at LFUCG. Please let me know if you know of MWDBE firms with skills in the following areas:

- Policy Development and Review
- Planning and Analysis
- Penetration Testing
- Vulnerability Testing
- Risk Management Assessment
- Info Security Audit and Compliance
- Info Security Remediation
- Info Security End-User Training
- Project Management
- Cybersecurity Consulting

Thank you!

Email to Commerce Lexington to request minority partners.



CBI is Seeking MWDBE Partner for LFUCG



Julie Spiller
To: tyra@commercelexington.com

[

Hello, we are seeking a partnership with a MWDBE firm to assist us with cybersecurity projects at LFUCG. Please let me know if you know of MWDBE firms with skills in the following areas:

- Policy Development and Review
- Planning and Analysis
- Penetration Testing
- Vulnerability Testing
- Risk Management Assessment
- Info Security Audit and Compliance
- Info Security Remediation
- Info Security End-User Training
- Project Management
- Cybersecurity Consulting

Thank you!
Julie



Julie Spiller
VP Business Development & Community Outreach
m: 586.915.2063
w: cbisecure.com
jspiller@cbisecure.com





Email to Small Business Development Council requesting minority partners:

CBI is Seeking MWDBE Partner for LFUCG



Julie Spiller
To: smack3@email.uky.edu

Hello, we are seeking a partnership with a MWDBE firm to assist us with cybersecurity projects at LFUCG. Please let me know if you know of MWDBE firms with skills in the following areas:

- Policy Development and Review
- Planning and Analysis
- Penetration Testing
- Vulnerability Testing
- Risk Management Assessment
- Info Security Audit and Compliance
- Info Security Remediation
- Info Security End-User Training
- Project Management
- Cybersecurity Consulting

Thank you!
Julie



Julie Spiller

VP Business Development & Community Outreach
m: 586.915.2063
w: cbisecure.com
jspiller@cbisecure.com





RE: CBI is Seeking MWDBE Partner for LFUCG



Sherita Miller <smiller@lexingtonky.gov>

To: Julie Spiller



LFUCG Certified List_February 2021.xlsx
146 KB

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe. Please forward any suspicious content to support@cbise

Good afternoon Julie,

Attached is a copy of LFUCG's certified list of minority, women and veteran owned businesses. This is an overall list of businesses with various specialties.

Thanks, Sherita

Sherita Miller
Minority Business Enterprise Liaison
Central Purchasing

859.258.3323 office
lexingtonky.gov



From: Julie Spiller <jspiller@cbisecure.com>
Sent: Tuesday, March 16, 2021 1:33 PM
To: Sherita Miller <smiller@lexingtonky.gov>
Subject: CBI is Seeking MWDBE Partner for LFUCG

[EXTERNAL] Use caution before clicking links and/or opening attachments.

Hello, we are seeking a partnership with a MWDBE firm to assist us with cybersecurity projects at LFUCG. Please let me know if you know of MWDBE firms with skills in the following areas:

- Policy Development and Review
- Planning and Analysis
- Penetration Testing
- Vulnerability Testing
- Risk Management Assessment
- Info Security Audit and Compliance

The following organizations were also contacted:

<https://www.wbckentucky.org/>



APPENDIX B: Sample Statement of Work

CBI has prepared a sample Statement of Work which illustrates how we perform a thorough security assessment to meet specific compliance mandates and due diligence requirements that will not just “check the box” but provide value to LFUCG in helping to discover weaknesses in one or more of the following areas:

- Visibility to determine gaps in detection, technology, and processes.
- Policies
- Remediation
- Overall risk handling

CBI is also focused on the following objectives:

- To leverage advanced and manual techniques that more effectively identify critical threats.
- Use the assessment to measure the effectiveness of controls, tools, processes, and response.
- To provide prioritized tactical and strategic recommendations based on identified vulnerabilities that allow the organization to quickly remediate discovered threats.
- To build a framework for continuous security improvement.

CBI’s Advanced Testing Services goes beyond the conventional exploitation vectors used by traditional firms. CBI does not use one specific tool or unique application to conduct these engagements. CBI uses a team-oriented effort with advanced skillsets to manually examine and explore every avenue of attack. Approximately 25% of the organization is dedicated to Advanced Testing Services.

Fees and Contract Duration – You will see in the pricing section that our pricing is broken out by eight different line items totaling \$140,000 in one-time fees. This is a fixed fee proposal with estimated project duration between 6-8 weeks.

CBI differentiators:

- Our Passion. CBI created the red team 16 years ago because we were passionate about information security and ethical hacking. We felt back then that the demand for penetration testing services would increase and we wanted to position ourselves for success. We did so by employing the best and the brightest in the industry. Today, most firms involved in cyber security and penetration testing got into this space to profit. We got into this space 16 years ago because we thought “how cool would it be if we could employ a team of ethical hackers and get paid to hack!”
- Our Skillset. Our list of certifications, such as OSCP/SANS/CISSP, are important qualifiers to many customers but we do not believe they are the only ones. The skillset CBI has is by far one of our strongest differentiators. By employing previous application development as active red team application penetration testers, we’ve able to provide remediation guidance that goes far beyond what a vulnerability scanning tool is going to recommend.
- Our Reports. CBI has worked very hard over the years to create reports of which we are proud. Our customers constantly tell us they appreciate our ability to translate these findings into interpretable content, while still maintaining the necessary technical remediation data. As mentioned before, we are proud of our reports and have included a sample as part of our response.

Minority Partner

Project management is built into the proposed Item Descriptions in Appendix D: Pricing and will be provided by one of our minority partners, Esource Resources. They are a LFUCG approved minority supplier. CBI will subcontract up to 10% to Esource Resources for the project management portion of these offerings. Esource Resources is a Minority Business Enterprise (MBE), Disabled Business Enterprise (DBE), and Service-Disabled Veteran Owned Small Business (SDVOSB). Further information on Esource Resources can be found in the Appendix A.



Statement of Work

This sample Statement of Work shows how CBI will govern the project to meet all project criteria:

Project Name: Penetration Testing Contract Number: _____
 Customer Contact: _____ Date of Issue: 9/8/2020
 Document Version: 1.0 Last Updated by: Shaun Bertrand

This Statement of Work ("SOW") is made by and between Creative Breakthroughs, Inc. ("CBI") and Client and is effective as of the date last signed below by the Parties ("Effective Date"). This SOW is governed by the terms and conditions posted on CBI's website at <https://www.cbisecure.com/CBI-Terms-of-Sale-Products-Services.pdf>. In the event that this SOW is not signed by Client and submitted to CBI for execution within 30 days from the date of issue listed above ("Expiration Date"), CBI's offer to perform the Services is null and void. The Agreement shall govern in the event of any inconsistencies or ambiguities between this SOW, any SLA, PO, or Quote.

Objectives

Based on our understanding of your needs, CBI has identified the following objectives that you would like assistance to address:

- To perform a thorough security assessment to meet specific compliance mandates and due diligence requirements.
- To leverage advanced and manual techniques that more effectively identify critical threats.
- Use the assessment to measure the effectiveness of controls, tools, processes, and response.
- To provide prioritized tactical and strategic recommendations based on identified vulnerabilities that allow the organization to quickly remediate discovered threats.
- To build a framework for continuous security improvement.

Scope and Approach

CBI delivers services in a structured approach within the constraints of the in-scope assets detailed below. For further detail on our approach to services and all related assumptions, please see Appendices labeled Technical Services Description for additional detail.

The following assets/components are in scope of the engagement:

Asset/Component	Description	Scope / Quantity
External Penetration Test	Penetration test against the external (WAN) environment.	In Scope
Social Engineering	Security awareness testing through simulated social engineering campaigns.	In Scope
Lateral Movement & Privilege Escalation	When an external system is compromised, the next attack vector is to move laterally and escalate privileges.	In Scope
Internal Penetration Test	Penetration test against the internal (LAN) environment.	In Scope
Wireless Assessment	Evaluation and analysis of security threats and risks related to the in scope wireless networks.	In Scope
Physical Assessment	Assessment of physical security controls and countermeasures.	In Scope



Post Penetration Testing Collaboration	Upon completion of the penetration testing engagement, CBI will facilitate onsite purple team collaboration to review and improve detection capabilities.	In Scope
Detailed Scoping Information		
Penetration Test Methodology	The approach in which the penetration test will be conducted. White hat (full information provided), black hat (no information provided), or gray hat (some information provided).	Gray Hat
External IP's	External assets to be included in the assessment.	Up to 350 IP addresses
Social Engineering Targets	Number of targets in scope for social engineering.	Digital <ul style="list-style-type: none"> Up to 150 targets (email addresses) Analog <ul style="list-style-type: none"> Up to 5 targets (phone calls) Text <ul style="list-style-type: none"> Up to 5 targets (text messages)
Social Engineering Templates	Number of different email campaigns in scope for social engineering.	One campaign for each social engineering phase in scope (digital, analog, and text).
Internal IP's	Internal assets to be included in the assessment.	All internal networks with a concentrated focus on: <ul style="list-style-type: none"> Up to 500 servers Sampling of endpoints Sampling of remote locations
Internal Penetration Testing Delivery Model	Internal penetration testing to be conducted remotely or onsite.	Remote
Wireless Networks in Scope	Number of wireless networks (SSID's) in scope.	Up to 3 SSIDs
Physical Assessment Locations	Number of locations in scope for physical security testing.	Up to 1 location
Rules of Engagement	Identification of the allowed attacks and targeted layers of the organization.	Attack Types Allowed: <ul style="list-style-type: none"> External Testing Internal Testing Social Engineering <ul style="list-style-type: none"> Digital, Analog, and Text Wireless Testing Physical Testing



Objectives / Flags	Focused objectives to gain access to better understand the attack vectors and control effectiveness related to mission critical technologies.	<ul style="list-style-type: none">• Active Directory / Domain Admin• PHI• Customer information• Intellectual Property
Exclusions	Any exclusions explicitly prohibited from testing.	TBD

Approach and Methodology

Service Delivery Features

CBI has been conducting penetration tests and application assessments for the last 16 years. As an organization we were at the front lines of helping to contribute to various penetration testing frameworks and standards such as PTES, NIST, and OWASP. Our strong reputation in this industry has been established because of our long track record of conducting successful and valuable penetration tests for enterprise organizations. We employ highly skilled penetration testers and application developers on the red team during this time to ensure we deliver a superior service edge compared to other vendors.

CBI has conducted over 1,600 engagements of similar size, scope, and complexity. CBI also has extensive experience in all industry verticals; healthcare, manufacturing, finance, and defense. Every individual on the CBI red team has the relevant and trustworthy credentials and certifications required for such sensitive testing. We have resources with Top Secret clearance for various defense contracts on which the CBI Red Team is engaged. Our firm believes that organizations need more than just tactical guidance. CBI's red team has been in formal existence for over 15 years. We understand that a strategic focus is also required to put our customers on a more proactive path. More importantly, we position our testing as an opportunity to better evaluate the effectiveness of controls. By being able to leverage guidance from CBI on how to tune existing controls, it is possible to establish a better return on the investments that have been made.

In addition, the CBI Red Team has all the industry certifications required to demonstrate our experience and expertise in this space, including but not limited to; CISSP, OSCP, OSCE, SANS penetration testing, SANS web application testing, HTCIA, InfraGard membership, ISSA membership, Michigan Cyber Civilian Corps (MIC3), and many other certifications and affiliations. Various CBI team members, including the Director, have recently been awarded medals from the Pentagon and Army for their efforts in an invitation only Bug Bounty program. CBI offers the following competitive differentiators:

- 1. Our Passion.** CBI created the red team 16 years ago because we were passionate about information security and ethical hacking. We felt back then that the demand for penetration testing services would increase, and we wanted to position ourselves for success. We did so by employing the best and the brightest in the industry. Today, most firms involved in cyber security and penetration testing got into this space to profit. We got into this space 16 years ago because we thought "how cool would it be if we could employ a team of ethical hackers and get paid to hack!"
- 2. Our Skillset.** Our list of certifications, such as OSCP/SANS/CISSP, are important qualifiers to many customers but we do not believe they are the only ones. The skillset CBI has is by far one of our strongest differentiators. By employing previous application development as active red team application penetration testers, we've able to provide remediation guidance that goes far beyond what a vulnerability scanning tool is going to recommend.



- 3. Our Reports.** CBI has worked very hard over the years to create reports of which we are proud. Our customers constantly tell us they appreciate our ability to translate these findings into interpretable content, while still maintaining the necessary technical remediation data. As mentioned before, we are proud of our reports and have included a sample as part of our response.

Service Methodology

CBI leverages many different tactics for penetration testing, application assessments, red teaming, and social engineering. Our team will work to exploit external services, social engineering attacks, physical attacks to gain internal access, and many other tactics that will be outlined in precarious detail on the scope of work. Objectives will be clearly defined that will assess the most critical assets related to the viability of the organization. CBI will first work to conduct threat intelligence analysis to determine the probable attack vectors associated with your business and industry vertical. These tactics vary based on unique environmental variables, and generally include, but are not limited to, Open-Source Intelligence Gathering (OSINT), external service exploitation, exploiting OS and application vulnerabilities and misconfigurations, exploiting firewall vulnerabilities and misconfigurations, exploiting advanced web application vulnerabilities, Man in the Middle (MiTM) attacks, brute forcing, password spray attacks, and privilege escalation and authentication bypass attacks.

CBI understands that thorough reconnaissance and OSINT builds the foundation for a successful engagement. CBI has various different methods for OSINT, including but not limited to; public/private threat intelligence feeds, open source utilities, breach dump analysis, scraping tactics, and the ability to identify vulnerabilities without sending a single packet to the target network. The CBI team will work to first evaluate the corporate functions; physical locations, vendors/supply chain, org charts, marketing data, infrastructure data, financials, individual analysis, high value target selection, and more. CBI will then move towards more concentrated covert activities; on/off location gathering, satellite views, etc. The information gathered and analyzed will provide a blueprint for the more active testing phases that will follow.

The automated processes used during our testing are generally focused on reconnaissance, OSINT, and discovery tactics. These processes involve asset enumeration/discovery, port scanning, banner identification, basic protocol analysis, and basic vulnerability scanning. The automated processes represent a small percentage of the overall time spent in comparison to manual processes. It is estimated that automated processes represent roughly 10% of the work, while manual testing represents 90% of the work.

Penetration Testing Overview

The penetration testing service actively exploits architectural weaknesses and configuration vulnerabilities to evaluate the security posture against an advanced active threat. A red team engagement is deeper and more targeted than a traditional vulnerability assessment. CBI will first work to conduct threat intelligence analysis to determine the probable attack vectors associated with your business and industry vertical. These tactics vary based on unique environmental variables, and generally include, but are not limited to; Open Source Intelligence Gathering (OSINT), external service exploitation, exploiting OS and application vulnerabilities and misconfigurations, exploiting firewall vulnerabilities and misconfigurations, exploiting web site vulnerabilities, Man in the Middle (MiTM) attacks, brute forcing and password spraying attempts against authentication schemes, privilege escalation and authentication bypass attacks. CBI will risk-rank the findings and provide executive overview and technical guidance for remediation.



Project Deliverables

Deliverable	Description
Executive Summary Reports	Consolidated review of identified risks, impact, and prioritized remediation paths for the assessment.
Technical Remediation Reports	Detailed report outlining vulnerability specifics, attack vectors, proof of concepts, and remediation recommendations.

Project Management

CBI will provide direction and control of project personnel, and provide the framework for project communications, reporting, procedural and contractual activity. The subtasks include:

- Include a summary as part of the weekly status report of the hours used against each of the component totals.
- Review the scope of work and any associated document with the client project team.
- Develop and maintain implementation schedule with the client Project Manager.
- Establish and maintain project communications with the client Project Team.
- Review and administer the change control procedure with the client project manager (as necessary)
- Manage issues and work with the client team and management to resolve deviations from the plan.
- Create and submit weekly status reports to the client project team and management.
- Measure, track and evaluate progress against the implementation schedule.
- Participate in regularly scheduled meetings with the client project team.
- Coordinate and manage the activities of the CBI assigned personnel.