SDGblue

541 Darby Creek Road, Suite 270
Lexington, Kentucky 40509

Phone: 859.263.7344
Fax: 859.263.0608

Visit us on the web at
www.sdgblue.com

Response to RFP #13-2016 Information Technology Consulting and Technical Services

Prepared April 2016 for:

Client Name | Lexington-Fayette Urban County Government

Client Address | 200 East Main Street
Lexington, KY 40507

TABLE OF CONTENTS

PROJECT OVERVIEW

[Introduction & Objectives

SDGblue, LLC (SDGblue) is a professional services firm specializing in IT infrastructure and IT security technology solutions and consulting services. Companies use SDGblue as their technology partner in many ways to solve business needs and receive the most out of their technology investment.

Lexington-Fayette Urban County Government (LFUCG) is looking for qualified professional vendors for information technology (IT) services. The qualified vendor(s) will enable LFUCG to significantly improve information technology effectiveness, enhance its quality of services, minimize down time and support costs, ensure security of data, and maximize investment in IT.

VENDOR REQUIREMENTS

[Technology Assessment

SDGblue has experience in a variety of the technologies listed in Attachment A. Please see Attachment A for a list of some of the technologies for which SDGblue can provide Professional Services.

[Support Services

SDGblue is not proposing these services.

[Software Development

SDGblue is not proposing these services.

[Consulting Services

SDGblue can provide Consulting Services as outlined in Attachment B for the following:

Disaster Recovery/Business Continuity

Disaster Recovery/Business Continuity for information systems is a required process for developing general support systems (GSS) and major applications (MA) with appropriate backup methods and procedures for implementing data recovery and reconstitution against IT risks. Risks to information systems may be natural, technological, or human in nature.

Contingency planning refers to interim measures to recover IT services following an emergency or system disruption. Interim measures may include the relocation of IT systems and operations to an alternate site, the recovery of IT functions using alternate equipment, or the performance of IT functions using manual methods.

The capability to recover and reconstitute data should be integral to the information system design concept during the Initiation phase of the Software Development Life Cycle of a system. Recovery strategies should be built into the architecture of the system during the Development phase. The contingency processes should be tested and maintained during the Implementation phase; contingency plans should be exercised and maintained during the Operations/Maintenance phase.

NIST SP 800-34, Contingency Planning Guide for Information Technology Systems, details a seven-step methodology for developing an IT contingency process and plan. These seven steps are summarized below:

Phase 1: Develop Contingency Planning Policy Statement

A formal department or agency policy provides the authority and guidance necessary to develop an effective contingency plan. The statement should define the agency's overall contingency objectives; identify leadership, roles and responsibilities, resource requirements, test, training, and exercise schedules; and develop maintenance schedules and determine the minimum required backup frequency.

Phase 2: Conduct Business Impact Analysis

A business impact analysis (BIA) is a critical step to understanding the information systems components, interdependencies, and potential downtime impacts. The BIA helps to identify and prioritize critical IT systems and components. Contingency plan strategies and procedures should be designed in consideration of the results of the BIA.

A BIA is conducted by identifying the system's critical resources. Each critical resource is then further examined to determine how long functionality of the resource could be withheld from the information system before an unacceptable impact is experienced. The impact may be something that materializes over time or may be tracked across related resources and dependent systems (e.g., cascading domino effect). The time identified is called a maximum allowable outage (MAO). Based on the potential impacts, the amount of time the information system can be without the critical resource then provides a recourse recovery priority around which an organization can plan recovery activities.

The balancing point between the MAO and the cost to recover establishes the information system's recovery time objective (RTO). Recovery strategies must be created to meet the RTO. The strategy must also address recovering information system critical components within a priority, as established by their individual RTOs.

Phase 3: Identify Preventive Controls

In some cases, implementing preventive controls might mitigate outage impacts identified by the BIA. Preventive controls are measures that detect, deter, and/or reduce impacts to the system. When cost-effective, preventing an impact is desired over implementing recovery strategies (therefore risking data loss and impact to the organization). Preventive measures are specific to individual components and the environment in which the components operate. Common controls include:

- Uninterruptible power supply (UPS);
- Fire suppression systems;
- Gasoline or diesel-powered generators;
- Air conditioning systems with excess capacity to permit failure of certain components;
- Heat-resistant and waterproof containers for backup media and vital non-electronic records; and
- Frequent, scheduled data backups.

Phase 4: Develop Recovery Strategies

When a disruption occurs despite the preventive measures implemented, a recovery strategy must be in place to recover and restore data and system operations within the RTO period. The recovery strategy is designed from a combination of methods, which together address the full spectrum of information system risks. The most cost-effective option, based on potential impact, should be selected and integrated into the information system architecture and operating procedures.

System data must be backed up regularly; therefore, all IT contingency plans should include a method and frequency for conducting data backups based on system criticality. Data that is backed up may need to be stored offsite and rotated frequently, depending upon the criticality of the system.

Major disruptions to system operations may require restoration activities to be implemented at an alternate site. The type of alternate site selected must be based on RTO requirements and budget limitations. Equipment for recovering and/or replacing the information system must be provided as part of the recovery strategy. Cost, delivery time, and compatibility factors must also be considered when determining how to provide the necessary equipment. Agencies must also plan for an alternate site that, at a minimum, provides workspace for all contingency plan personnel, equipment, and the appropriate IT infrastructure necessary to execute IT contingency plan and system recovery activities.

The recovery strategy requires personnel to implement the procedures and test operability. Generally, a member of the organization's senior leadership is selected to activate the plan and lead overall recovery operations. Appropriate teams of personnel (at least two people to ensure there is a primary and alternate available to execute procedures) are identified to be responsible for specific aspects of the plan. Personnel should be chosen to staff the teams based on their normal responsibilities, system knowledge, and availability to recover the system on an on-call basis. A line of succession should be defined to ensure that someone could assume the role of senior leadership if the plan leader is unable to respond.

Phase 5: Develop IT Contingency Plan

Procedures for executing the recovery strategy are outlined in the IT contingency plan. The plan must be written in a format that will provide the users (recovery team leadership and members) the context in which the plan is to be implemented and the direct procedures, based on role, to execute.

The NIST SP 800-34 presents a sample format for developing an IT contingency plan. The format defines three main phases that govern the actions to be taken following a system disruption. The Notification/Activation phase describes the process of notifying recovery personnel and performing a damage assessment. The Recovery phase describes a course of action for recovery teams and personnel to restore IT operations at an alternate site or using contingency capabilities. The final phase, Reconstitution, outlines actions that can be taken to return the system to normal operating conditions.

Additionally, the format contains the Supporting Information and Appendices components, which provide supplemental information necessary to understand the context in which the plan is to be used and gives additional information that may be necessary to execute procedures (e.g., emergency contact information and the BIA).

Phase 6: Plan Testing, Training, and Exercises

Personnel selected to execute the IT contingency plan must be trained to perform the procedures, the plan must be exercised, and the system strategy must be tested.

Plan testing should include:

- System recovery on an alternate platform from backup media
- System performance using alternate equipment
- Coordination among recovery teams
- Restoration of normal operations
- Internal and external connectivity
- Notification procedures

Personnel training should include:

- Purpose of the plan
- Security requirements
- Cross-team coordination and communication
- Team-specific processes
- Reporting procedures
- Individual responsibilities

Plan exercises should be designed to examine, individually and then collectively, various components of the entire plan. Exercises may be conducted in a classroom setting: discussing specific components of the plan and/or impact issues; or they may be functional exercises: simulating the recovery using actual replacement equipment, data, and alternate sites.

Phase 7: Plan Maintenance

The IT contingency plan must always be maintained in a ready state for use immediately upon notification. At least, annual reviews of the plan must be conducted to ensure that key personnel and vendor information, system components and dependencies, the recovery strategy, vital records, and operational requirements are up to date. While some changes may be obvious (e.g., personnel turnover or vendor changes), others will require analysis. The BIA should be reviewed periodically and updated with new information to identify new contingency requirements and priorities. Changes made to the plan are noted in a record of changes, dated, and signed or initialed by the person making the change. The revised plan, or plan sections are circulated to those with plan responsibilities. Because of the impact that plan changes may have on interdependent business processes or information systems, the changes must be clearly communicated and properly annotated in the beginning of the document.

Technical Requirements Gathering

SDGblue's Technology Assessment approach includes the following criteria:

- Assess and document current server infrastructure components
- Assess and document current network infrastructure components (WAN, LAN, internet connectivity)
- Assess and document current end-user device components
- Assess and document other IT services delivered to end-users (applications, email, shared services, etc.)
- Assess disaster recovery and business continuity requirements and current capabilities
- Assess existing security controls and other safeguards currently in place to protect information assets

IT Strategic Planning

SDGblue can customize our Strategic Planning and Roadmapping to fit our client's needs. Our approach typically includes the following criteria:

- Interviews with leadership and key end-users / business leaders to understand what they need from IT with regard to support and new initiatives
- Review and discussion of the existing / future IT budget to get an understanding of the parameters within which the client must manage IT expenditure
- Review of existing IT processes, whether formalized or not, to gauge level of "maturity" in day-to-day IT operations that support the business (functionally and strategically)
- Review and discussion of any compliance requirements associated with security of information systems and/or specific data
- Interviews with IT staff to understand their skillsets and how those skills align with existing or potential future technology

IT Governance

SDGblue provides strategic direction to help enterprises understand the issues and the strategic importance of IT, so that they can sustain their operations and implement the strategies required to extend their activities into the future. SDGblue's IT governance program, based on the Information Systems Audit and Control Association (ISACA) framework, aims at ensuring that expectations for IT are met and IT risks are mitigated.

SDGblue will provide Information Security Services as outlined in Attachment B for the following:

Policy Development and Review

SDGblue currently provides these services to clients in two capacities:

- A single engagement measuring existing controls, where SDGblue obtains and reviews copies of relevant policy and procedure documents for information security. SDGblue will compare these documents to technical controls in place to evaluate the consistency between policies and controls. Additionally, SDGblue security analysts will perform an on-site interview with staff involved in operations to review the implementation of key security controls and processes. As part of our security assessment services, we will also review security policies and processes to make determinations on the adequacy of the documentation and overall security program.
- An ongoing service provided by one of our virtual CISOs. Initially, SDGblue would review and update the content of the existing policies, and then ongoing efforts to ensure that all policies are up to date, regulatory requirements are met, and relevant procedures are in place to facilitate implementation throughout the organization. This service goes hand in hand with other ongoing services to build an overall IT strategy.

Planning and Analysis

In order to facilitate the security and compliance maturity goals of our clients, SDGblue recommends the execution of various projects, with each project implemented into an overall strategy of establishing and maintaining compliance along with a movement toward information security best practices. SDGblue can provide a dedicated resource to evaluate current weaknesses and risks and to develop a detailed remediation and risk management plan going forward. Typically, these services begin with an emphasis on assessment activity, review of documentation, strategy sessions, developing business-driven technology roadmaps, and planning technology decisions for short-term and long-term.

The initial work could include areas such as:

- *Information Security Strategic Planning & Roadmap* – Develop Information Security Roadmap that will provide clarity on the various security initiatives needed to improve and maintain your security posture as well as regulatory compliance.
- *Information Security Policies Update* – Review and update the content about the existing Security Policies.
- *Security Awareness Training* – Develop and/or improve relevant Security Awareness training for employees to support compliance as well as good security practices. Program would be developed through various inputs including: results of any social engineering exercises, results of risk analysis, results of compliance assessment, and learning habits of workforce members. Once established, the program would be required during onboarding process, and updated annually via a CBT-based solution (tracks attendance, passing of exam / quizzes, logs non-participation, etc. for reporting purposes).
- *Security Risk Management Program Development* – Develop tracking mechanism to ensure that all security deficiencies are tracked, assigned, and managed going forward. Ensure visibility with Senior Management and monitor progress overtime. SDGblue's process includes acquisition of a risk repository tool, which will be populated through the execution of the risk analysis, and risks will be treated and managed going forward based on the plan within this tool. This allows for transparent visibility of all involved and provides a seamless way to track progress toward remediation of risks.

An ongoing role, as described here, could include such services as listed below:

- *Information Security Policies Management* – Ensure that all Information Security Policies are up to date, meet regulatory requirements, and have relevant procedures to facilitate their implementation throughout the organization.

- *Disaster Recovery Plan Management* – Update existing Disaster Recovery plan and ensure its management going forward. Schedule updates to Business Impact Analysis once a year and testing as appropriate in agreement with management.
- *Information Security and Awareness Training* – Maintain program for complying with policies by enabling and educating workforce on how to secure confidential data. This program would also include development of regular security reminders to workforce.
- *Security Logging and Monitoring* – Review available security audit logs and other security reports. Establish Security Incident Response process to follow up on suspicious activities.
- *Remediation Planning and Risk Management* – Develop and maintain plans for remediation of administrative, physical, and technical safeguards. Develop risk management plan for risk treatment based on risk tolerance of leadership. Plans will guide all efforts in establishing and maintaining compliance. The plan would be produced in the event of an audit or investigation to show the findings and demonstrate that there is a detailed plan in place to manage follow up activities.
- *Interface to external providers and auditors* – Primary interface to providers who conduct technical security assessment activities (vulnerability scans, penetration testing, etc.) As assessment activities are completed and plans developed, there will be an obvious need for solutions implementation and changes to existing infrastructure that will improve security posture and help meet compliance requirements. SDGblue can provide the interface to external resources to validate implementation, document remediation activity and align to appropriate standards within regulatory requirements.
- *Monthly External Scan* – High level technical review of the perimeter for any new systems or network vulnerabilities. Follow up on any critical or high vulnerabilities to strengthen the network perimeter and to minimize security exposures from the Internet.

Penetration Testing

SDGblue's penetration testing services are designed to simulate attack patterns and methods used in real-world attacks to see how your organization can prevent, detect, and respond to advanced threat actors. Our services are designed to fulfill not only regulatory requirements (such as PCI), but can provide additional consulting services and on site education (which is one of our core values) to ensure that your staff are made aware of those real-world threats and how to configure your environment to protect against them. Our certified and experienced professionals use cutting edge tools and industry accepted methodologies such as the Penetration Testing Execution Standard (PTES) to ensure that all your needs are met, and remediation testing is included to ensure that identified issues are completely corrected. Our goal is to not only meet your regulatory requirements, but ensure that your environment is protected from the advanced threat actors that are making organizations notorious around the globe.

Goals of SDGblue's Penetration Testing Services: In addition to meeting regulatory requirements, the overall objective is to simulate a real-world attack against our client's IT Security Program and assets by testing the effectiveness of technically implemented controls and procedures, as well as employee awareness of threats. The overall objective of the assessment from a high level has two main goals:

- To determine whether and how a malicious user can gain unauthorized access to assets that affect the fundamental security of the system, files, logs and/or cardholder data
- To confirm the applicable controls, such as scope, vulnerability management, methodology, and segmentation required in regulations such as PCI DSS are in place

Some additional goals of the assessments are to help our clients:

- Manually identify vulnerabilities not found during a standard automated analysis
- Identify elevated risks that may be present due to combining multiple, lower-risk vulnerabilities in a particular sequence
- Identify whether an internal attacker could successfully escalate their privileges, gain access to sensitive data, and exfiltrate data from the network

- Assess the effectiveness of currently implemented Security Program and controls
- Test their ability to successfully detect and react to attacks

Our Rules of Engagement: Methods used in cyber breaches can be broadly categorized into three different basic forms:

- Physical Attacks
- Technical Attacks
- Social Engineering Attacks

Depending on the goals of the specific test identified in the scoping phase, SDGblue may include one or all of these methods in our testing process. SDGblue will work with our clients to determine:

- Testing Goals
- Authorized Testing Times
- Proper Communication Plan (Who and When)
- Emergency Contact Procedures

These are all critical elements to determine in the planning phases of a penetration test to ensure the assessment is successful and meets the needs and expectations of our clients.

Our Approach: Additionally (and depending on the goal of the testing) we can break our penetration tests into three distinct phases, each with varying levels of access provided by the client:

- External Security Assessment (Black Box)
  - Client only provides a list of IP addresses in scope, testing is conducted from the external Internet to identify and verify exploitable vulnerabilities (often considered low hanging fruit) that could allow a remote attacker to gain a foothold to pivot to the internal network or steal sensitive information.
  - Testing includes Open Source Intelligence Gathering, Reputation Analysis or Internet Facing IP addresses and Domains, and both network and application layer vulnerability scanning (including manual analysis and exploitation of identified vulnerabilities).
- Internal Security Assessment (Gray Box)
  - Access is provided by the client to the internal network, and testing is conducted to identify and verify remotely exploitable vulnerabilities. Also known as a "Zero Day Card", this type of testing simulates a remote attacker that is able to gain a remote foothold on the network without access to credentials.
- Internal Security Assessment (White Box)
  - Access and credentials are provided to the internal network. In this case, SDGblue works as a trusted partner to quickly identify and verify all known vulnerabilities, and security misconfigurations. Credentials are used to scan and verify both client side and remotely exploitable vulnerabilities. SDGblue performs manual reviews of Server, Workstation, and Network device configurations to identify compliance with best practices, conducts effectiveness testing against many security controls (such as Antimalware, IDS/IPS, Web Filtering, Firewall Configurations, and technical controls used to enforce password complexity), and reviews the network design and architecture to ensure compliance with industry best practices.

Our Report: Our reports are designed to meet all the specific criteria outlined in the Penetration Testing Execution Standard (PTES) as well as the Penetration Testing Guidance released in March 2015 by the PCI Security Standards Council. Our reports include:

- Organizational and Analyst Information/Qualifications
- Executive Summary of Results and Recommendations
- Detailed Scoping Information
- Methodology

- Narrative
- Description of Environment (Discovery)
- Detailed, Technical Results on Individual Issues Identified

In addition to the report, SDGblue will provide a structured ZIP file containing all the raw data collected during the testing process.

Vulnerability Testing

SDGblue has experience working with clients for overall security testing by scanning systems in scope using vulnerability testing software. Verification testing quantifies the severity of a given vulnerability and helps to eliminate false positives reported by automated tools. Testing consists of conducting specific, manual probe tests to take advantage of identified vulnerabilities. SDGblue personnel can exploit vulnerabilities to assess impact.

Our security assessment services will provide you with the information you need to take an accurate pulse of the readiness of your organization's enterprise security program. SDGblue has developed a time-tested and proven technical testing methodology that is both comprehensive and efficient. In our experience, we have found that organizations can best leverage this type of investment by establishing a baseline and then comparing itself to that baseline each year. This disciplined approach provides a valid comparison from year-to-year while also allowing the organization to test the success of remediation activities from the prior year.

Assessment Areas / Scope:

- (NS) Network Security Review
  - Firewall Assessment
  - Policy / Rule Review
  - Optimization Review
  - Network Architecture and Design Review (Compartmentalization)
  - Network Device Review (Device Hardening)
  - Remote Access Controls / VPN Review
  - Egress Security Control Examination (Web Filter, IDS/IPS, Firewall)
- (HS) Host Security Review
  - Vulnerability Scanning
  - Malware Protection Review
  - Endpoint Encryption Review for Laptops
  - Configuration Standards Review (against CIS Standards – other standards available upon request)
  - Principle of Least Privilege Review
  - Windows Share Privilege Review (No Credentials, and with Standard Domain User)
  - Printer Security Review
- (UAM) User and Account Management Review
  - Account Management Practices
  - Password Policy Enforcement
- Stale / Unused Accounts
  - (PES) Physical and Environmental Security Control Review
  - Access Controls and Reporting
  - Fire Suppression
  - Supporting Utilities
  - Environmental Hazards (other)
- (PR) Policy Review
  - High level review of provided policies and procedures to ensure compliance with applicable regulatory requirements

Security Testing and Analysis:

- *Compartmentalization* – SDGblue will conduct extensive testing for proper network compartmentalization to ensure the internal attack surface is minimized from systems at a higher risk of compromise, including networks that house management interfaces for critical servers and network infrastructure.
- *Egress Control Examination* – Knowing that it takes a combination of people, processes, and technology to make an effective security control, SDGblue uses exclusive, in-house developed tools to examine the effectiveness of all three aspects to assess the effectiveness of your organization's IDS/IPS systems and web application filters.
- *Vulnerability Scanning* – SDGblue uses multiple automated tools to gather information which allows for greater coverage. Additionally, SDGblue's comprehensive methodology includes custom back end processing to correlate results from multiple, disparate tools and ensures that only verified findings are presented in the final report.
- *Principle of Least Privilege Review* – Using in-house developed tools and methodology, SDGblue will review the risk to your organization posed by users running with excessive privilege performing higher risk, daily activities.
- *Windows SMB Share Review* – SDGblue will perform custom reviews of privilege levels of Windows SMB shares for internal users, making note of areas where risk may be increased by overly-permissive permissions
- *Policy Review* – SDGblue will review security policies and processes to make determinations on the adequacy of the documentation and overall security program.

SDGblue's Web Application Security services are designed to promote an overall security strategy by either consulting with clients to build a security program which includes the applications used, or by helping clients locate vulnerabilities at the application layer, quickly and accurately giving our clients insight into what vulnerabilities need to be fixed and where to find them. We can advise our clients of industry trends in application security and potential areas for proactively addressing their risk. We assist our clients by using multiple tools and tests to eliminate false positives, reduce remediation time, and provide more value. We have experience in examining operating system and web server-centric environments by reviewing open port scanning, system enumeration, general host misconfigurations, risk of susceptibility to denial of service attacks, password weaknesses, and access controls. We are familiar with exploits using Directory Traversal and Enumeration, Application Logic Weaknesses, Cross-Site Scripting, SQL Injection (error and blind), Parameter Injection Command Execution, Buffer Overflow Weaknesses, Path Manipulation and Truncation, Automatic Form-Filling, SSL Support and Strength, Sensitive Developer Comments, Error Message Identification, Permissions Testing, Susceptibility to Brute Force Authentication attacks, and User Session Handling.

Risk Management Assessment

SDGblue understands the importance of a risk management process, which will ultimately lead to LFUCG having a better understanding of its risk conditions. SDGblue utilizes the NIST 800-30 Risk Assessment process to create a Risk Analysis.

Specifically, the NIST 800-30 process includes a nine step process, outlined below. Information gathered in the security assessment services will be a primary input into the Risk Analysis creation process.

Risk Analysis Process:

1. System Characterization
2. Threat Identification
3. Vulnerability Identification (Technical Assessments)
4. Control Analysis
5. Likelihood Determination

6. Impact Analysis
7. Risk Determination
8. Control Recommendations
9. Results Documentation

Info Security Audit and Compliance

SDGblue can develop reporting for audit and compliance needs based on information received from various aspects of security testing and policy review. Deliverables may include:

- *Information Security Management Services*: Information Security Roadmap, various reports, incident tracking, Security Awareness documentation, audit logging, and other elements to be developed based on existing controls and to provide alignment of actual processes with published and implemented procedures.
- *Compliance and Security Assessment*: Reporting deliverable with separate components for compliance and security, each with specific next steps, which will be incorporated into strategic planning, budget, and overall direction of the Information Security roadmap.
- *Remediation and Risk Management Planning*: Tracking and reports provided with monthly updates on progress toward achieving compliance, addressing risks, and technical or non-technical remediation of gaps in compliance with regulatory requirements.

Info Security Remediation

SDGblue can develop and maintain plans for remediation of administrative, physical, and technical safeguards. As part of an overall risk management program, we will plan for risk treatment based on risk tolerance of leadership. Plans will guide all efforts in establishing and maintaining compliance. The plan could be produced in the event of an audit or investigation to show the findings and demonstrate that there is a detailed plan in place to manage follow up activities.

In relation to security assessment testing, we can also perform remediation scanning efforts to ensure that any remediation actions have completely resolved previously identified risks.

Info Security End-User Training

SDGblue can develop and/or improve relevant Security Awareness training for employees to support Security Compliance as well as good security practices. The program would be developed through various inputs including: results of any social engineering exercises, results of risk analysis, results of compliance assessment, and learning habits of workforce members. Once established, the program would be required during the onboarding process, and updated annually via a CBT-based solution (tracks attendance, passing of exam / quizzes, logs non-participation, etc. for reporting purposes). This type of service could be customized.

An ongoing program could also include development of regular security reminders to the workforce, which could be a regulatory requirement.

COST OF SERVICES

1. Fee schedule for proposed services:

Disaster Recovery / Business Continuity	$175.00 per hour
Technical Requirements Gathering	$190.00 per hour
IT Strategic Planning	$190.00 per hour
IT Governance	$190.00 per hour
Policy Development and Review	$190.00 per hour
Planning and Analysis	$190.00 per hour
Penetration Testing	$190.00 per hour
Vulnerability Testing	$157.50 per hour
Risk Management Assessment	$190.00 per hour
Info Security Audit and Compliance	$190.00 per hour
Info Security Remediation	$190.00 per hour
Info Security End-User Training	$190.00 per hour*

2. SDGblue typically provides a Scope of Work (SOW) for the engagement defined. These can be billed as an hourly rate, or as a fixed fee project if required.
   *Info Security End-User Training can also be provided on a per user cost depending on the SOW defined.
3. SDGblue would not charge travel or expenses for these services in Fayette County.
4. See Attachment B.

COMPANY INFORMATION

1. SDGblue, LLC
   541 Darby Creek Road, Suite 270
   Lexington, KY 40509
2. SDGblue has partnerships with many technology firms, including but not limited to:
   - Algosec
   - Avaya Inc.
   - Blue Coat Systems
   - Brocade
   - Certes Networks
   - Check Point Software Technologies, Inc.
   - Cisco Systems, Inc.
   - Citrix
   - Dell
   - Dell SecureWorks
   - EMC Corporation
   - Entrust
   - Forcepoint, LLC (formerly Websense)
   - Fortinet
   - HP Enterprise Security Group
   - Intel Security (formerly McAfee)

- LogRhythm
- Microsoft
- Nimble Storage Inc.
- OpenDNS
- Palo Alto Networks
- Rapid7
- RSA Security Inc.
- Splunk, Inc.
- Symantec
- Tenable Network Security
- Trend Micro
- Varonis

SDGblue can also use subcontractors to provide other information security services, including but not limited to:

- Oxford Computer Group – Identity Management services
- Principle Logic, LLC – Web Application Security services

3. Our team:

	Gui Cozzi | Director of Security Consulting Group & CISO Gui brings over sixteen years of IT security experience, successfully implementing pragmatic and risk-based security programs to meet compliance with various industries' security requirements. Prior to SDGblue, he developed and implemented an Information Security Program at the nation's third-largest faith-based health system. His previous titles include Director of Security Strategy & Risk Management, Technical Services Manager, Security Specialist, and IT Security Consultant. Additionally, he has been an ISACA Topic Leader on Risk Management, and is a member of the Kentucky Health Information Exchange Privacy & Security Committee. His certifications include: CISA, CISSP, CRISC, HITRUST, and CMBA.
	Michael Gilliam | Consulting Manager – Security Team Lead Michael is an Information Security Analyst whose qualifications include several security-related designations, and detailed knowledge of technical security tools, technologies, and best practices. His extensive experience includes creating, maintaining, and deploying security solutions protecting networks, systems, and information assets for federal and state government agencies, as well as private sector organizations in the healthcare and financial industries. Michael brings over ten years of experience in the information technology field, and has been with SDGblue since 2012. His certifications include: CISSP, Security+, Network+, IACRB Certified Computer Forensics Examiner, and Snort Certified Professional.

John Askew | Senior Security Consultant

John is a Senior Security Consultant with over nine years of experience in vulnerability and risk management, security event management, and security program development. John has contributed to a number of security consulting offerings at SDGblue, including a methodology for assessing and improving the overall maturity of IT security programs. John also has experience writing software in a variety of programming languages, such as python, rust, and haskell. Overall, John brings a pragmatic approach to security consulting that favors guiding principles and creative solutions over products and prescription. His certifications include: CompTIA Security + and CISSP.

Mike Brancato | Senior Security Analyst

Mike has over sixteen years of experience in successfully planning, designing, and implementing solutions for information security needs in large corporate environments to maintain regulatory compliance and meet business objectives. His expertise includes security policy and procedure development, security project management, and leading/directing the deployment, implementation, and completion of IT and security projects. Prior to working at SDGblue, Mike held positions as an Information Systems Security Specialist, Systems Support Manager, Network Manager, and Network Engineer. His certifications include: CISSP.

Dan Collins | Associate Security Analyst

Dan is a skilled Security Consultant who is experienced in performing security assessments for a wide range of organizations in various industries. He works with clients to analyze vulnerabilities and make risk-based decisions regarding information security, as well as providing user-awareness evaluation through social engineering exercises. Prior to working at SDGblue, he worked as a Junior Software Developer, Research Technician, and served in the United States Air Force as a Joint Terminal Attack Controller. His certifications include: CompTIA Security +.

Corey Shell | Associate Security Analyst

Corey has over eight years of experience as an Information Technology and Security Consultant. Prior to working at SDGblue, he was a network administrator and technology consultant. He has a wide range of both security and technical experience, including security risk/vulnerability analysis, software integration, system administration, and data management. Corey will graduate with his Master's degree in Information Security & Assurance in 2016. His certifications include: Certified Ethical Hacker, CompTIA A+, Network+, Security+, and Server+.

Amy Justice | Senior Security and Compliance Consultant

Amy has over eight years of experience working in Information Technology and Information Security fields, assisting clients with being compliant by using security best practices and regulatory requirements. She has worked in the healthcare and technology industries, as well as the Department of Defense. Amy's previous positions include Security Consultant, Information Security Analyst and IT audit roles with the University of Kentucky Medical Center, and Security Coordinator with ACS/Xerox. She also has several years of experience in Project Management supporting clients in Six Sigma and ITIL Service Management Projects. Her certifications include: CCFSP, Security+, ITIL in IT Service Management, and Six Sigma Green Belt.

Mike Neal | Senior Security and Compliance Consultant

Mike has over ten years of experience in the IT security industry, providing consulting to SDGblue clients in regulated industries where Information Security and Compliance are a strategic part of overall operations. His consulting services include HIPAA Security and Risk Analysis, HIPAA Compliance, Virtual CIO / Virtual CISO, Disaster Recovery, Strategic Management Consulting, IT Management, Project Management, and Solutions / Services Architecture. His certifications include: HCISSP and CRISC.

Kevin Beaver | Information Security Consultant

Kevin Beaver is an Information Security Consultant, writer, professional speaker, and expert witness with over twenty-seven years of experience in IT and twenty-one years in information security. He specializes in performing independent security assessments, with a focus on web and mobile application testing, to help businesses minimize their IT risks, take the pain out of compliance, and uncheck checkboxes that keep creating a false sense of security. He has written/co-written twelve books on information security including the best-selling Hacking For Dummies and The Practical Guide to HIPAA Privacy and Security Compliance. Kevin has written 800+ articles and guest blog posts on information security and is a regular contributor to websites such as TechTarget's SearchSecurity.com, Ziff Davis' Toolbox.com, and IBM's SecurityIntelligence.com. His certifications include: CISSP and CompTIA IT Project +.

	Jimmy Noll | Chief Technology Officer Jimmy is a leader in IT Management and Business Development with over twenty-eight years of industry experience. His professional experiences include building and maintaining frameworks focused on data compliance and information security. He is skilled at producing effective business plans, budgeting, setting strategy, risk management, vision casting, new revenue streams and growth. He is skilled at directing technology teams that focus on business requirements, implementation and support with an emphasis on relationships and client satisfaction. He holds a wide range of technical and professional certifications, including: CISSP, CCSE, CCSP, and CCNA.
	Donna Schlosser | Senior Security Engineer Donna is a seasoned security professional working in the field for twenty-nine years with a range of experience covering Boundary and EndPoint Protection, Log Collection/Event Correlation, and Risk Analysis. Her years of experience have provided in-depth knowledge of many security tools to include firewall management (Checkpoint, Cisco ASA, Palo Alto Networks, and Juniper SRX). Configuring and troubleshooting all aspects of security tool implementation has become her trademark. Donna is able to see the "big picture" of an issue and quickly assist in finding a creative and supportable solution. Her certifications include: CISSP, GCIA Certified Intrusion Analysis (Silver) and Juniper JCNIS-FW and JNCIA-SSL.

a. Our staff largely works out of our Lexington, KY headquarters with a few exceptions:
   - Jimmy Noll's office is in Cincinnati, OH. Jimmy regularly spends time in Lexington.
   - Donna Schlosser's office is in Murfreesboro, TN. Donna regularly spends time in Lexington.
   - Kevin Beaver's office is in Atlanta, GA. Typically, his services are provided remotely rather than onsite.

b. Our hourly rates can be found in the Cost of Services section of this document.

c. Travel and Expenses for our staff is non-billable in Fayette County.

d. All staff members on the team are employees, with one exception:
   - Kevin Beaver is a subcontractor.

4. SDGblue, LLC, through its parent company, FourPointOh, Inc. (formerly Systems Design Group, Inc.) has been in business since July, 1991. We have been providing IT security consulting services since 2000.
5. SDGblue is proud of our record of providing quality security services to our clients and serving as their trusted security partners. We believe the clients listed here have security requirements that are similar to yours, and we would be pleased if you contacted them to inquire about our performance.

KY Commonwealth Office of Technology	Louisville Metro Government
David Carter Deputy Director of IT Security Branch (502) 564-8734	**Jason Ballard** CIO (502) 574-4347

ADDITIONAL INFORMATION

SDGblue typically provides a Scope of Work (SOW) for the engagements required. Specific projects can be scoped as determined by LFUCG.

ATTACHMENT A

Technology	Experience	Comments
Microsoft Windows 2003, 2008, 2012, 2016	Average 13 years 5 people	SDGblue is capable of performing these actions: System configuration, system implementation, infrastructure maintenance, network support, and IT technical training / knowledge transfer.
Microsoft Windows 7, 8, 10 Desktop	Average 6 years 6 people	SDGblue is capable of performing these actions: System configuration, system implementation, infrastructure maintenance, network support, and IT technical training / knowledge transfer.
Microsoft Office 365, Architecture and Design	Average 4 years 4 people	SDGblue is capable of performing these actions: System configuration, system implementation, infrastructure maintenance, network support, and IT technical training / knowledge transfer.
Microsoft PowerShell	Average 6 years 4 people	SDGblue is capable of performing these actions: System configuration, system implementation, infrastructure maintenance, network support, and IT technical training / knowledge transfer.
Microsoft Active Directory	Average 15 years 4 people	SDGblue is capable of performing these actions: System configuration, system implementation, infrastructure maintenance, network support, and IT technical training / knowledge transfer.
Microsoft Exchange 2010, 2013	Average 12 years 5 people	SDGblue is capable of performing these actions: System configuration, system implementation, infrastructure maintenance, network support, and IT technical training / knowledge transfer.
AIX versions 5.x, 6.x, 7.x	N/A	
Linux	Average 10 years 5 people	SDGblue is proficient in server administration, configuration, programming, scripting, and command-line interface operations for a variety of Linux/Unix environments.
Internet Information Server (IIS)	Average 15 years 5 people	SDGblue is capable of performing these actions: System configuration, system implementation, infrastructure maintenance, network support, and IT technical training / knowledge transfer.
F5 BigIP	N/A	
VMware	Average 6 years 6 people	SDGblue is capable of performing these actions: System configuration, system implementation, infrastructure maintenance, network support, and IT technical training / knowledge transfer.

VMware VirtualCenter	Average 6 years 6 people	SDGblue is capable of performing these actions: System configuration, system implementation, infrastructure maintenance, network support, and IT technical training / knowledge transfer.
VMware ESX	Average 6 years 6 people	SDGblue is capable of performing these actions: System configuration, system implementation, infrastructure maintenance, network support, and IT technical training / knowledge transfer.
Microsoft Access	N/A	
Microsoft SQL Server 2008, 2012, 2014, 2016	N/A	
Oracle Database 10, 11, 12, 13	N/A	
SharePoint Services (on premise and cloud)	N/A	
Microsoft Office SharePoint Server	N/A	
Microsoft .NET Framework 2+	N/A	
Microsoft Project Server	N/A	
ESRI Geodatabase (10.2.1 and higher)	N/A	
ESRI ArcGIS for Server (10.2.1 and higher)	N/A	
ESRI ArcGIS for Desktop (10.2.1 and higher)	N/A	
ESRI ArcGIS Online (10.2.1 and higher)	N/A	
ESRI ArcReader (10.2.1 and higher)	N/A	
Visual Studio	N/A	
VBA	N/A	
Python	N/A	
JavaScript	N/A	
HTML5	N/A	
C#	N/A	
C++	N/A	
Ruby	N/A	
Ruby on Rails	N/A	
Visual Basic 6.0	N/A	
ASP.NET	N/A	

VB.NET	N/A	
jQuery	N/A	
Web Services	N/A	
PHP Development	N/A	
RPG IV	N/A	
BCD Presto	N/A	
ADO	N/A	
Moodle	N/A	
AJAX	N/A	
Technology Experience Comments		See additional technologies listed at the bottom of this list.
Node.js	N/A	
Chef, Puppet, Troposphere	N/A	
Amazon Web Services (AWS) Architecture	Average 1 year 2 people	SDGblue is capable of performing these actions: System configuration, system implementation, infrastructure maintenance, network support, and IT technical training / knowledge transfer
Amazon Web Services (AWS) DevOps	N/A	
Microsoft Azure Architecture	N/A	
Microsoft Azure DevOps	N/A	
Palo Alto Firewalls	Average 3 years 2 people	SDGblue is capable of performing these actions: System configuration, system implementation, infrastructure maintenance, network support, and IT technical training / knowledge transfer.
Splunk	5 years 1 person	SDGblue is capable of performing these actions: System configuration, system implementation, infrastructure maintenance, network support, and IT technical training / knowledge transfer.
Switching & Routing	Average 14 years 6 people	SDGblue is capable of performing these actions: System configuration, system implementation, infrastructure maintenance, network support, and IT technical training / knowledge transfer.
Vulnerability Scanning (Nessus)	Average 6 years 2 people	SDGblue is capable of performing these actions: System configuration, system implementation, infrastructure maintenance, network support, and IT technical training / knowledge transfer.

Patch Management	Average 10 years 6 people	SDGblue is capable of performing these actions: System configuration, system implementation, infrastructure maintenance, network support, and IT technical training / knowledge transfer
IBM BigFix	N/A	
PeopleSoft HCM 9.0	N/A	
PeopleSoft FSCM 8.9	N/A	
PeopleTools 8.49	N/A	
Symantec Control Compliance	5 years 1 person	SDGblue is capable of performing these actions: System configuration, system implementation, infrastructure maintenance, network support, and IT technical training / knowledge transfer
Symantec Data Loss	5 years 1 person	SDGblue is capable of performing these actions: System configuration, system implementation, infrastructure maintenance, network support, and IT technical training / knowledge transfer
Symantec Data Center Security	5 years 1 person	SDGblue is capable of performing these actions: System configuration, system implementation, infrastructure maintenance, network support, and IT technical training / knowledge transfer
LogRhythm	Average 3 years 3 people	SDGblue is capable of performing these actions: System configuration, system implementation, infrastructure maintenance, network support, and IT technical training / knowledge transfer
Check Point Firewalls	Average 8 years 4 people	SDGblue is capable of performing these actions: System configuration, system implementation, infrastructure maintenance, network support, and IT technical training / knowledge transfer
EndPoint Security	Average 10 years 8 people	SDGblue is capable of performing these actions: System configuration, system implementation, infrastructure maintenance, network support, and IT technical training / knowledge transfer

Service		Rate	Notes
Software Development			
	ASP.NET	N/A	
	C#	N/A	
	JavaScript	N/A	
	Ruby	N/A	
	Ruby on Rails	N/A	
	C++	N/A	
	HTML5	N/A	
	VB.NET	N/A	
	Python	N/A	
	Visual Basic 6.0	N/A	
	ESRI ArcGIS	N/A	
	ADO 2.X + Web Services	N/A	
	Microsoft Access	N/A	
Database Design			
	SQL Server	N/A	
	SQL Server Express	N/A	
	MySQL	N/A	
	ESRI Enterprise Geodatabase	N/A	
	Oracle	N/A	
Consulting			
	Disaster Recovery/Bus Continuity	$ 175.00	Plan, Build, Assist and Develop plans for organizations. Test existing plans.

	Technical Requirements Gathering	$ 190.00	Perform Roadmaps and Technical Assessments
	IT Strategic Planning	$ 190.00	Perform Roadmaps and Technical Assessments
	IT Governance	$ 190.00	Work with Health Care, Financial and Manufacturing to build compliance programs
	IT Project Management	N/A	
	Certified Project Management (PMP)	N/A	
	Network Technologies	N/A	
	Software Development	N/A	
	PeopleSoft HCM (9.0)	N/A	
	PeopleSoft FSCM (8.9)	N/A	
Server Application Implementation			
	Microsoft SharePoint	N/A	
	Microsoft Project Server	N/A	
	Microsoft SQL Server	N/A	
	Microsoft Exchange	N/A	
	Microsoft Windows	N/A	
	VMware Virtual Center	N/A	
	VMware ESX	N/A	
	ESRI ArcGIS Server	N/A	
Training			
	Microsoft SharePoint	N/A	
	Microsoft Project Server	N/A	
	Microsoft SQL Server	N/A	
	Visual Studio Team Suite	N/A	
	Visual Studio 2008	N/A	

	VMware	N/A	
Network Support			
	F5 BigIP	N/A	
	Microsoft Active Directory	N/A	
	Microsoft Windows	N/A	
	VMware	N/A	
Information Security			
	Policy Development and Review	$ 190.00	Plan, Develop, Implement, Test
	Planning and Analysis	$ 190.00	Roadmap, Implement, Test, Validate
	Penetration Testing	$ 190.00	Plan, Target, Test, Validate
	Vulnerability Testing	$ 157.50	Plan, Target, Test, Validate
	Risk Management Assessment	$ 190.00	Plan, Identify, Rank, consider mitigating controls
	Info Security Audit and Compliance	$ 190.00	Plan, Identify, Rank, consider mitigating controls
	Info Security Remediation	$ 190.00	Plan, Architect, Implement, Test
	Info Security End-User Training	$ 190.00	Plan, Implement, Learning Management System training delivery, Test, Validate
Enterprise DevOps & "Cloud"			
	Cloud Architecture and Design	N/A	
	Code Development and Maintenance	N/A	
	Enterprise System Administration	N/A	
	Version Control	N/A	
	Infrastructure as Code (IaC)	N/A	
	Platform as a Service (PaaS)	N/A	
	Software as a Service (SaaS)	N/A	
	Infrastructure as a Service (IaaS)	N/A	

Designation of Responsibility for Implementation

The CFO has the responsibility for designing and ensuring the effective implementation of SDGblue's Affirmative Action Program (AAP). These responsibilities include, but are not limited to, the following:

1. Developing Equal Employment Opportunity (EEO) policy statements, affirmative action programs and internal and external communication procedures;
2. Assisting in the identification of AAP/EEO problem areas;
3. Assisting management in arriving at effective solutions to AAP/EEO problems;
4. Designing and implementing an internal audit and reporting system that:
   a) Measures the effectiveness of SDGblue's program;
   b) Determines the degree to which AAP goals and objectives are met; and
   c) Identifies the need for remedial action;
5. Keeping SDGblue's President informed of equal opportunity progress and reporting potential problem areas within the company;
6. Reviewing the company's AAP for qualified minorities and women with all managers and supervisors at all levels to ensure that the policy is understood and is followed in all personnel activities;
7. Auditing the contents of the company's bulletin board to ensure compliance information is posted and up-to-date; and
8. Serving as liaison between SDGblue and enforcement agencies.

Responsibilities of Managers and Supervisors

It is the responsibility of all managerial and supervisory staff to implement SDGblue's AAP. These responsibilities include, but are not limited to:

1. Assisting in the identification of problem areas, formulating solutions, and establishing departmental goals and objectives when necessary;
2. Reviewing the qualifications of all applicants and employees to ensure qualified individuals are treated in a nondiscriminatory manner when hiring, promotion, transfer, and termination actions occur; and
3. Reviewing the job performance of each employee to assess whether personnel actions are justified based on the employee's performance of his or her duties and responsibilities.

Action-Oriented Programs

SDGblue will institute action programs to eliminate identified problem areas and to help achieve specific affirmative action goals. These programs include:

1. Conducting annual analysis of job descriptions to ensure they accurately reflect job functions;
2. Reviewing job descriptions by department and job title using job performance criteria;
3. Making job descriptions available to recruiting sources and available to all members of management involved in the recruiting, screening, selection and promotion processes;
4. Evaluating the total selection process to ensure freedom from bias through:
   a) Reviewing job applications and other pre-employment forms to ensure information requested is job-related;
   b) Evaluating selection methods that may have a disparate impact to ensure that they are job-related and consistent with business necessity;
   c) Training personnel and management staff on proper interview techniques; and
   d) Training in EEO for management and supervisory staff;
5. Using techniques to improve recruitment and increase the flow of minority and female applicants. SDGblue will undertake the following actions:
   a) Include the phrase "Equal Opportunity/Affirmative Action Employer" in all printed employment advertisements;

    b) Place help wanted advertisement, when appropriate, in local minority news media and women's interest media;
    c) Disseminate information on job opportunities to organizations representing minorities, women and employment development agencies when job opportunities occur;
    d) Encourage all employees to refer qualified applicants;
    e) Actively recruit at secondary schools, junior colleges, colleges and universities with predominantly minority or female enrollments; and
    f) Request employment agencies to refer qualified minorities and women;
6. Ensuring that all employees are given equal opportunity for promotion. This is achieved by:
    a) Posting promotional opportunities;
    b) Offering counseling to assist employees in identifying promotional opportunities, training and educational programs to enhance promotions and opportunities for job rotation or transfer; and
    c) Evaluating job requirements for promotion

<u>Internal Audit and Reporting System</u>

The CFO has the responsibility for developing and preparing the formal documents of the AAP. The CFO is responsible for the effective implementation of the AAP; however, responsibility is likewise vested with each department manager and supervisor. SDGblue's audit and reporting system is designed to:

- Measure the effectiveness of the AAP/EEO program;
- Document personnel activities;
- Identify problem areas where remedial action is needed; and
- Determine the degree to which SDGblue's AAP goals and objectives have been obtained.

The following personnel activities are reviewed to ensure nondiscrimination and equal employment opportunity for all individuals without regard to their race, color, sex, sexual orientation, gender identity, religion, or national origin:

- Recruitment, advertising, and job application procedures;
- Hiring and promotion;
- Rates of pay and any other forms of compensation including fringe benefits;
- Job assignments, job classifications, and job descriptions;
- Sick leave, leaves or absence, or any other leave;
- Training, apprenticeships, attendance at professional meetings and conferences; and
- Any other term, condition, or privilege of employment.

The following documents will be maintained as a component of SDGblue's internal audit process:

1. An applicant flow log showing the name, race, sex, date of application, job title, interview status and the action taken for all individuals applying for job opportunities;
2. Summary data of external job offers and hires, promotions, resignations, terminations, and layoffs by job group and by sex and minority group identification;
3. Summary data of applicant flow by identifying, at least, total applicants, total minority applicants, and total female applicants for each position;
4. Maintenance of employment applications (not to exceed one year); and
5. Records pertaining to SDGblue's compensation system.

<u>Guidelines on Discrimination Because of Religion or National Origin</u>

It is the policy of SDGblue to take affirmative action to insure that applicants are employed, without regard to their religion or national origin. Such action includes, but is not limited to the following employment practices: hiring, promotion, demotion, transfer, recruitment or recruitment advertising, layoff, termination, rates of pay or other forms of compensation and selection for training. In addition, the following practices have been or will be implemented:

1. The policy concerning SDGblue's obligation to provide equal employment opportunity without regard to religion or national origin is communicated to all employees via employee handbooks, policy statement and the Affirmative Action Program. (See Exhibit A, page 6)
2. Internal procedures will be developed to insure that SDGblue's obligation to provide equal employment opportunity without regard to religion or national origin is being fully implemented.
3. Employees will be informed at least annually of SDGblue's commitment to equal employment opportunity for all persons, without regard to religion or national origin.
4. Recruiting sources will be informed of our commitment to provide equal employment opportunity without regard to religion or national origin.
5. Employment records of all employees will be reviewed to determine the availability of promotable and transferable employees.
6. Contacts with religious and ethnic organizations will be made for purposes of advice, education, technical assistance and referral of potential employees as necessary to accomplish the purpose of this program.
7. SDGblue will engage in recruitment activities at educational institutions with significant enrollments of students from various ethnic and religious groups.
8. Ethnic and religious media may be used for employment advertising.

Reasonable accommodations to the religious observances and practices of employees or prospective employees will be made, unless doing so would result in undue hardship. In determining whether undue hardship exists, factors such as the cost to the company and the impact on the rights of other employees would be considered.

Exhibit A – Copy of EEO Policy in Employment Handbook (Page 9)

Equal Employment Opportunity

SDGblue is committed to the principles of equal employment. We are committed to complying with all federal, state, and local laws providing Equal Employment Opportunities, and all other employment laws and regulations. It is our intent to maintain a work environment which is free of harassment or discrimination because of sex, race, religion, color, national origin, physical or mental disability, genetic information, age, military service, veteran status, sexual orientation/gender identity, or any other status protected by federal, state or local laws. SDGblue is dedicated to the fulfillment of this policy in regard to all aspects of employment, including recruiting, hiring, placement, promotion, termination, layoff, recall, transfer, leave of absence, and compensation and training.

SDGblue will conduct a prompt and thorough investigation of all allegations of discrimination or any violation of the Company's Equal Employment Opportunity Policy in as confidential a manner as possible. SDGblue will take appropriate corrective action, if and where warranted. SDGblue prohibits retaliation against any employee who provides information about, complains, or assists in the investigation of any complaint of discrimination or violation of the Company's Equal Employment Opportunity Policy.

SDGblue expects all employees to strictly adhere to this policy. We are all responsible for upholding SDGblue's Equal Employment Opportunity policy and any claimed violations of that policy should be brought to the attention of your supervisor, the CFO or the President.

See signed and notarized Affidavit below:

AFFIDAVIT

Comes the Affiant, C. Glen Combs, and after being first duly sworn, states under penalty of perjury as follows:

1. His/her name is C. Glen Combs and he/she is the individual submitting the proposal or is the authorized representative of SDGblue, LLC, 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.

STATE OF Kentucky

COUNTY OF Fayette

The foregoing instrument was subscribed, sworn to and acknowledged before me by Bonnie Kendrick on this the 27th day of April, 2016.

My Commission expires: Oct. 7, 2016

Bonnie Kendrick
NOTARY PUBLIC, STATE AT LARGE

BONNIE KENDRICK
Notary Public
State at Large
Kentucky
My Commission Expires Oct 7, 2016

Notary ID 475152

EQUAL OPPORTUNITY AGREEMENT

See signed Equal Opportunity Agreement below:

EQUAL OPPORTUNITY AGREEMENT

The Law

- Title VII of the Civil Rights Act of 1964 (amended 1972) states that it is unlawful for an employer to discriminate in employment because of race, color, religion, sex, age (40-70 years) or national origin.

- Executive Order No. 11246 on Nondiscrimination under Federal contract prohibits employment discrimination by contractor and sub-contractor doing business with the Federal Government or recipients of Federal funds. This order was later amended by Executive Order No. 11375 to prohibit discrimination on the basis of sex.

- Section 503 of the Rehabilitation Act of 1973 states:

  > *The Contractor will not discriminate against any employee or applicant for employment because of physical or mental disability.*

- Section 2012 of the Vietnam Era Veterans Readjustment Act of 1973 requires Affirmative Action on behalf of disabled veterans and veterans of the Vietnam Era by contractors having Federal contracts.

- Section 206(A) of Executive Order 12086, Consolidation of Contract Compliance Functions for Equal Employment Opportunity, states:

  > *The Secretary of Labor may investigate the employment practices of any Government contractor or sub-contractor to determine whether or not the contractual provisions specified in Section 202 of this order have been violated.*

****

The Lexington-Fayette Urban County Government practices Equal Opportunity in recruiting, hiring and promoting. It is the Government's intent to affirmatively provide employment opportunities for those individuals who have previously not been allowed to enter into the mainstream of society. Because of its importance to the local Government, this policy carries the full endorsement of the Mayor, Commissioners, Directors and all supervisory personnel. In following this commitment to Equal Employment Opportunity and because the Government is the benefactor of the Federal funds, it is both against the Urban County Government policy and illegal for the Government to let contracts to companies which knowingly or unknowingly practice discrimination in their employment practices. Violation of the above mentioned ordinances may cause a contract to be canceled and the contractors may be declared ineligible for future consideration.

Please sign this statement in the appropriate space acknowledging that you have read and understand the provisions contained herein. Return this document as part of your application packet.

Bidders

I/We agree to comply with the Civil Rights Laws listed above that govern employment rights of minorities, women, Vietnam veterans, handicapped and aged persons.

	SDGblue, LLC
Signature	*Name of Business*

WORKFORCE ANALYSIS FORM

See signed Workforce Analysis Form below:

WORKFORCE ANALYSIS FORM

Name of Organization: SDGblue, LLC

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	4	3	1													3	1
Professionals	18	12	4			1				1						14	4
Superintendents																	
Supervisors																	
Foremen																	
Technicians																	
Protective Service																	
Para-Professionals	2	1	1													1	1
Office/Clerical	9	5	2			1	1									6	3
Skilled Craft																	
Service/Maintenance																	
Total:	33	21	8			2	1			1						24	9

Prepared by: ______________________ **Date:** 04 / 27 / 2016

(Name and Title)

Revised 2015-Dec-15

Statement on SDGblue's Efforts to Ensure Disadvantaged Business Enterprises (DBE) Contract Participation

SDGblue is aware of the Lexington-Fayette Urban County Government's goal to ensure Equal Employment Opportunities, to obtain at least ten percent (10%) utilization of Disadvantaged Business Enterprises, including MBE's and WBE's, and to also include Veteran-Owned Businesses at a goal of three percent (3%) total procurement costs.

In efforts to actively and aggressively participate and contribute to those goals, SDGblue has already taken or will be implementing the following actions:

1. SDGblue has established an Affirmative Action Plan;
2. Has conducted current workforce and utilization analysis;
3. Has created an organizational display that represents the utilization of women and minorities at SDGblue;
4. Has published policy statements and notices within the Employment Handbook and within the workplace explaining SDGblue's commitment to Equal Employment Opportunity;
5. Has contacted Lexington-Fayette Urban County Government's Division of Central Purchasing for help in identifying qualified, certified businesses to solicit for potential contracting opportunities.
6. Will begin tracking and creating reports of all annual payments submitted to MWVDBE's for work done or materials purchased for this contract.

See signed LFUCG Statement of Good Faith Efforts below:

LFUCG STATEMENT OF GOOD FAITH EFFORTS

Bid/RFP/Quote #____RFP # 13-2016 Information Technology Consulting and Technical Services

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.

_____ 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.

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

__X__ Attended LFUCG Central Purchasing Economic Inclusion Outreach event

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

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

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

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

_____ Sent written notices, by certified mail, email or facsimile, to qualified, certified MWDBEs soliciting their participation in the contract not less that seven (7) days prior to the deadline for submission of bids to allow them to participate effectively.

_____ Followed up initial solicitations by contacting MWDBEs to determine their level of interest.

_____ Provided the interested MWBDE firm with adequate and timely information about the plans, specifications, and requirements of the contract.

_____ 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

_____ 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.

_____ 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.

_____ 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.

_____ 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

_____ Made efforts to expand the search for MWDBE firms beyond the usual geographic boundaries.

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

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.

SDGblue, LLC	
Company	**Company Representative**
04/27/2016	President and CEO
Date	**Title**

GENERAL PROVISIONS

See signed General Provisions below:

GENERAL PROVISIONS

1. Each Respondent shall comply with all Federal, State & Local regulations concerning this type of service or good.

   The Respondent agrees to comply with all statutes, rules, and regulations governing safe and healthful working conditions, including the Occupational Health and Safety Act of 1970, *29 U.S.C. 650 et. seq.*, as amended, and KRS Chapter 338. The Respondent also agrees to notify the LFUCG in writing immediately upon detection of any unsafe and/or unhealthful working conditions at the job site. The Respondent agrees to indemnify, defend and hold the LFUCG harmless from all penalties, fines or other expenses arising out of the alleged violation of said laws.

2. Failure to submit ALL forms and information required in this RFP may be grounds for disqualification.

3. Addenda: All addenda, if any, shall be considered in making the proposal, and such addenda shall be made a part of this RFP. Before submitting a proposal, it is incumbent upon each proposer to be informed as to whether any addenda have been issued, and the failure to cover in the bid any such addenda may result in disqualification of that proposal.

4. Proposal Reservations: LFUCG reserves the right to reject any or all proposals, to award in whole or part, and to waive minor immaterial defects in proposals. LFUCG may consider any alternative proposal that meets its basic needs.

5. Liability: LFUCG is not responsible for any cost incurred by a Respondent in the preparation of proposals.

6. Changes/Alterations: Respondent may change or withdraw a proposal at any time prior to the opening; however, no oral modifications will be allowed. Only letters, or other formal written requests for modifications or corrections of a previously submitted proposal which is addressed in the same manner as the proposal, and received by LFUCG prior to the scheduled closing time for receipt of proposals, will be accepted. The proposal, when opened, will then be corrected in accordance with such written request(s), provided that the written request is contained in a sealed envelope which is plainly marked "modifications of proposal".

7. Clarification of Submittal: LFUCG reserves the right to obtain clarification of any point in a bid or to obtain additional information from a Respondent.

8. Bribery Clause: By his/her signature on the bid, Respondent certifies that no employee of his/hers, any affiliate or Subcontractor, has bribed or

attempted to bribe an officer or employee of the LFUCG.

9. Additional Information: While not necessary, the Respondent may include any product brochures, software documentation, sample reports, or other documentation that may assist LFUCG in better understanding and evaluating the Respondent's response. Additional documentation shall not serve as a substitute for other documentation which is required by this RFP to be submitted with the proposal,

10. Ambiguity, Conflict or other Errors in RFP: If a Respondent discovers any ambiguity, conflict, discrepancy, omission or other error in the RFP, it shall immediately notify LFUCG of such error in writing and request modification or clarification of the document if allowable by the LFUCG.

11. Agreement to Bid Terms: In submitting this proposal, the Respondent agrees that it has carefully examined the specifications and all provisions relating to the work to be done attached hereto and made part of this proposal. By acceptance of a Contract under this RFP, proposer states that it understands the meaning, intent and requirements of the RFP and agrees to the same. The successful Respondent shall warrant that it is familiar with and understands all provisions herein and shall warrant that it can comply with them. No additional compensation to Respondent shall be authorized for services or expenses reasonably covered under these provisions that the proposer omits from its Proposal.

12. Cancellation: If the services to be performed hereunder by the Respondent are not performed in an acceptable manner to the LFUCG, the LFUCG may cancel this contract for cause by providing written notice to the proposer, giving at least thirty (30) days notice of the proposed cancellation and the reasons for same. During that time period, the proposer may seek to bring the performance of services hereunder to a level that is acceptable to the LFUCG, and the LFUCG may rescind the cancellation if such action is in its best interest.

A. Termination for Cause

(1) LFUCG may terminate a contract because of the contractor's failure to perform its contractual duties

(2) If a contractor is determined to be in default, LFUCG shall notify the contractor of the determination in writing, and may include a specified date by which the contractor shall cure the identified deficiencies. LFUCG may proceed with termination if the contractor fails to cure the deficiencies within the specified time.

(3) A default in performance by a contractor for which a contract may be terminated shall include, but shall not necessarily be limited to:

(a) Failure to perform the contract according to its terms, conditions and specifications;

(b) Failure to make delivery within the time specified or according to a delivery schedule fixed by the contract;

(c) Late payment or nonpayment of bills for labor, materials, supplies, or equipment furnished in connection with a contract for construction services as evidenced by mechanics' liens filed pursuant to the provisions of KRS Chapter 376, or letters of indebtedness received from creditors by the purchasing agency;

(d) Failure to diligently advance the work under a contract for construction services;

(e) The filing of a bankruptcy petition by or against the contractor; or

(f) Actions that endanger the health, safely or welfare of the LFUCG or its citizens.

B. At Will Termination

Notwithstanding the above provisions, the LFUCG may terminate this contract at will in accordance with the law upon providing thirty (30) days written notice of that intent, Payment for services or goods received prior to termination shall be made by the LFUCG provided these goods or services were provided in a manner acceptable to the LFUCG. Payment for those goods and services shall not be unreasonably withheld.

13. Assignment of Contract: The contractor shall not assign or subcontract any portion of the Contract without the express written consent of LFUCG. Any purported assignment or subcontract in violation hereof shall be void. It is expressly acknowledged that LFUCG shall never be required or obligated to consent to any request for assignment or subcontract; and further that such refusal to consent can be for any or no reason, fully within the sole discretion of LFUCG.

14. No Waiver: No failure or delay by LFUCG in exercising any right, remedy, power or privilege hereunder, nor any single or partial exercise thereof, nor the exercise of any other right, remedy, power or privilege shall operate as a waiver hereof or thereof. No failure or delay by LFUCG in exercising any right, remedy, power or privilege under or in respect of this Contract shall affect the rights, remedies, powers or privileges of LFUCG hereunder or shall operate as a waiver thereof.

15. Authority to do Business: The Respondent must be a duly organized and authorized to do business under the laws of Kentucky. Respondent must be in good standing and have full legal capacity to provide the services specified under this Contract. The Respondent must have all necessary right and lawful authority to enter into this Contract for the full term hereof and that proper corporate or other action has been duly taken authorizing the Respondent to enter into this Contract. The Respondent will provide LFUCG with a copy of a corporate resolution authorizing this action and a letter from an attorney confirming that the proposer is authorized to do business in the State of Kentucky if requested. All proposals must be signed by a duly authorized officer, agent or employee of the Respondent.

16. Governing Law: This Contract shall be governed by and construed in accordance with the laws of the Commonwealth of Kentucky. In the event of any proceedings regarding this Contract, the Parties agree that the venue shall be the Fayette County Circuit Court or the U.S. District Court for the Eastern District of Kentucky, Lexington Division. All parties expressly consent to personal jurisdiction and venue in such Court for the limited and sole purpose of proceedings relating to this Contract or any rights or obligations arising thereunder. Service of process may be accomplished by following the procedures prescribed by law.

17. Ability to Meet Obligations: Respondent affirmatively states that there are no actions, suits or proceedings of any kind pending against Respondent or, to the knowledge of the Respondent, threatened against the Respondent before or by any court, governmental body or agency or other tribunal or authority which would, if adversely determined, have a materially adverse effect on the authority or ability of Respondent to perform its obligations under this Contract, or which question the legality, validity or enforceability hereof or thereof.

18. Contractor understands and agrees that its employees, agents, or subcontractors are not employees of LFUCG for any purpose whatsoever. Contractor is an independent contractor at all times during the performance of the services specified.

19. If any term or provision of this Contract shall be found to be illegal or unenforceable, the remainder of the contract shall remain in full force and such term or provision shall be deemed stricken.

Signature

04/27/2016

Date

EXCEPTIONS REQUESTED FOR RISK MANAGEMENT PROVISIONS INSURANCE AND INDEMNIFICATION

Our current Professional Liability coverage is $1 million per occurrence, $2 million aggregate. We would request an exception to the requirement for $3 million aggregate.