Guidehouse

The West Virginia Department of Administration
West Virginia Office of Technology
Request for Proposal

Cyber Security Risk Program

Provided to:

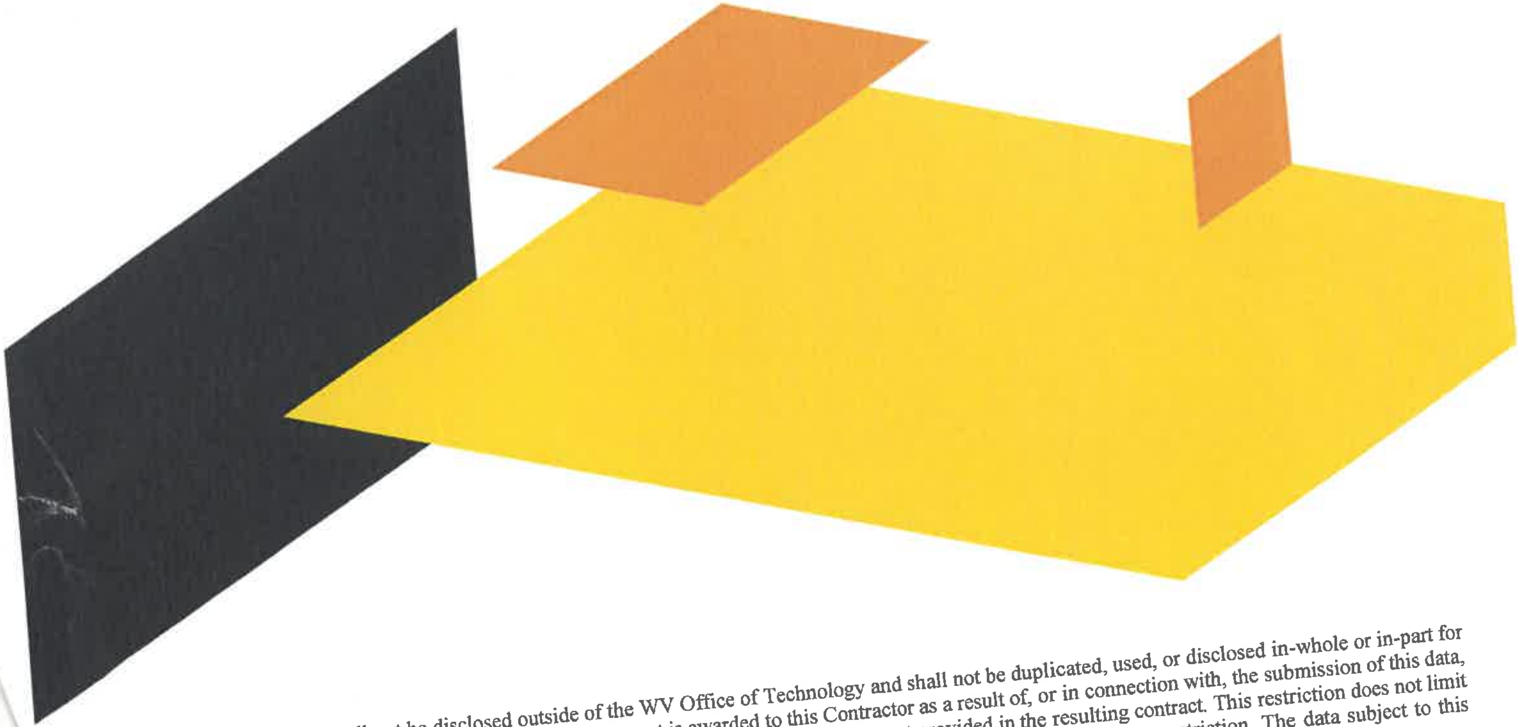
Jessica Chambers
Department of Administration, Purchasing Division
2019 Washington E
Charleston, WV 25305-0130

Response to RFP
August 29, 2019

Provided by:

Guidehouse LLP (formerly PricewaterhouseCoopers Public Sector LLP)
Chris O'Brien
Partner
1800 Tysons Boulevard
7th Floor
McLean, VA 22102-4257
cobrein@guidehouse.com

Taxpayer Identification Number (TIN): 82-4596065
Data Universal Numbering System (DUNS): 079529872
Commercial and Government Entity (CAGE) Code: 783T6



This proposal includes data that shall not be disclosed outside of the WV Office of Technology and shall not be duplicated, used, or disclosed in-whole or in-part for any purpose other than to evaluate this proposal. If, however, a contract is awarded to this Contractor as a result of, or in connection with, the submission of this data, the WV Office of Technology shall have the right to duplicate, use, or disclose the data to the extent provided in the resulting contract. This restriction does not limit the WV Office of Technology's right to use information contained in this data if it is obtained from another source without restriction. The data subject to this estriction are contained in all pages/sheets herein.

his proposal does not constitute a contract to perform services. Final acceptance of this engagement by Guidehouse is contingent upon successful completion of idehouse's acceptance procedures. Any engagement arising out of this proposal will be subject to the execution of our formal engagement contract, including our dard terms and conditions and fees and billing rates established therein.

We bring direct GRC tool solicitation and implementation experience: We are deeply familiar with the business requirements, vendor landscape, and configuration considerations of governance, risk management, and compliance (GRC) tools in the public sector. Our team has supported GRC tool deployments across the United States using Archer, RiskVision, Oracle and others. While we know the technology landscape well, we are objective and not tied to any specific vendor or technology. Our goal is to ensure that WVOT procures and deploys a tool that meets West Virginia's needs and sets the Cyber Risk Program up for success.

We have the best people. Our team members not only have the right technical skills for this engagement, but also possess the intangible qualities you will need in a consultant. Our team works collaboratively with your staff to help facilitate issues, create consensus, and hold stakeholders accountable to keep the project moving forward. Our proposed team members have directly supported public sector agencies with similar engagements including planning and implementing enterprise risk management programs and governance, risk, and compliance solutions.

We focus on quality. We are a proud recipient of the 2014 Malcolm Baldrige Quality Award and the only professional services firm to have received this award.

If you have any questions about this proposal or our qualifications, please contact:

Nini Donovan, Managing Director
Phone: (617) 596-7633
Email: ndonovan@guidehouse.com

We understand that your choice of a partner in this endeavor is an important decision. We are confident that our extensive experience and commitment, combined with our highly skilled team and deep resources uniquely position us to assist you in achieving your goals. We appreciate the opportunity to present our approach and credentials in the following pages.

Sincerely,

Chris O'Brien

Chris O'Brien
Partner | US State and Local Government Practice
Phone: (773) 909-4360
Email: COBrien@guidehouse.com

Table of Contents

Section **Page**

Our Understanding

State and Local government IT departments face a constantly shifting landscape of cyber risk. The proliferation of access points, connected devices, and siloed systems creates a challenging enough environment to mitigate existing risks, let alone identify and contain new threats and vulnerabilities that arise on a daily basis. Risk management requires consistently defined policies, dependable and accessible tools for analysis, and a robust and unified program to identify, monitor, assess, and respond to cyber threats. It has been Guidehouse's experience that organizations must embrace cybersecurity as a risk management problem versus just a compliance challenge.

West Virginia has taken a significant step forward to improve the cybersecurity posture of the state by establishing a cybersecurity office and allocating resources to address threats that are not a matter of "if," but "when." West Virginia Code 5A-6B-1 takes the necessary first step in calling for a comprehensive risk assessment and defining standards to enable an "apples to apples" comparison of risks. These standards will allow WVOT and state agencies at-large to define and understand the true nature of their risk program, and in turn, more effectively allocate time, infrastructure investments, and other resources to mitigate those risks that can be expected to have the highest impact on the organization's mission.

The West Virginia Office of Technology (WVOT) has been tasked with leading the State's cyber risk efforts and seeks a partner that will plan for, create, implement, and ultimately turn over a new cyber risk program for the state in 24 calendar months. The partner will provide strong program management skills and cybersecurity expertise, and leverage industry knowledge to support WVOT with two solicitations for procuring audit services and a GRC solution. Additionally, the vendor must exhibit clear and effective communication with all key stakeholders.

We would be honored to partner with WVOT to build a cyber risk program for the Mountain State. We have supported numerous public sector clients in carrying out cybersecurity risk assessment, risk management, and program development projects. Our team is assisting the Department of State in building its cybersecurity risk office and all accompanying policies, standards, assessment and communication documentation. For the State of Massachusetts, Guidehouse set up the State's identity and access management program, rolling out the program to agencies statewide and improving the cybersecurity posture of the State. Guidehouse conducted a cyber risk assessment for Center for Medicare Services (CMS) executives where we produced risk statements and led an executive level discussion on risk tolerance levels and prioritization of resources. We have also

Case in Point

Guidehouse Built the First Department of State Cyber Risk Program

Guidehouse supported the Department of State to implement and execute the creation of a new cyber risk office, and associated cyber risk management program across the Tier 1 (organizational), Tier 2 (mission/business), and Tier 3 (systems) elements of the organization. Our team created a department-wide Cybersecurity Risk Management Strategy document, outlining how and why the organization should address cyber risk, and updated foundational policy documents. Our Cybersecurity Risk Management Strategy led to the development and approval of a new enterprise cybersecurity risk management office, charged with leading the identification, management, and monitoring of cybersecurity risk to the Department's mission and business processes. We proposed a structure focused on five key capabilities to help the Department of State better address cyber risk: High Value Assets (HVA) project coordination, cyber risk analysis, cyber risk assessment, governance, and project management.

implemented numerous GRC tools for public sector clients including RiskVision, RSA Archer, and Oracle giving us deep knowledge of GRC tool business requirements, vendor offerings, and configuration considerations.

Our approach and timeline is guided by this experience across the public sector, by RFP requirements, and by the latest industry guidance, standards, and understanding of threats. We have focused our approach on the NIST Risk Management Framework, the NIST Cyber Security Framework, and defined guidance from NIST on performing risk assessments. We recommend that WVOT also utilize these frameworks and guidance for the development of your cyber risk program. We have also allowed for some flexibility in the timing of the GRC tool solicitation. Our current state review at the start of the project will give us a deeper understanding of your organization and WV's needs to determine if WVOT should consider selecting a GRC tool earlier in the program development process. In some situations, it can be more effective from both a program development and cost perspective to design a program around the functions of the tool, rather than to try to customize the tool to unique processes and functions. Our proposal assumes that we will define the security risk program first and then support WVOT in its GRC solicitation, but we will encourage additional discussion to best address WV's needs.

Case in Point

Enterprise Security Policy and Program Development at the Massachusetts Department of Transportation

Guidehouse supported MassDOT in setting up an enterprise security program and designing policies to make cybersecurity an enterprise-wide priority. The Guidehouse team assessed MassDOT's existing information security policy landscape for gaps relative to best practices and industry leading standards. The team drafted a new set of standard enterprise security policies addressing these gaps uniformly across the organization. Finally, Guidehouse socialized these policies and developed a governance model, KPIs, and an implementation plan to support MassDOT's successful adoption of these policies. Guidehouse maintained a Project Management Office (PMO) throughout the life of the project and assisted MassDOT in establishing the right measures, structure, and stakeholder involvement to be effective in the implementation and monitoring of enterprise security policies across the organization.

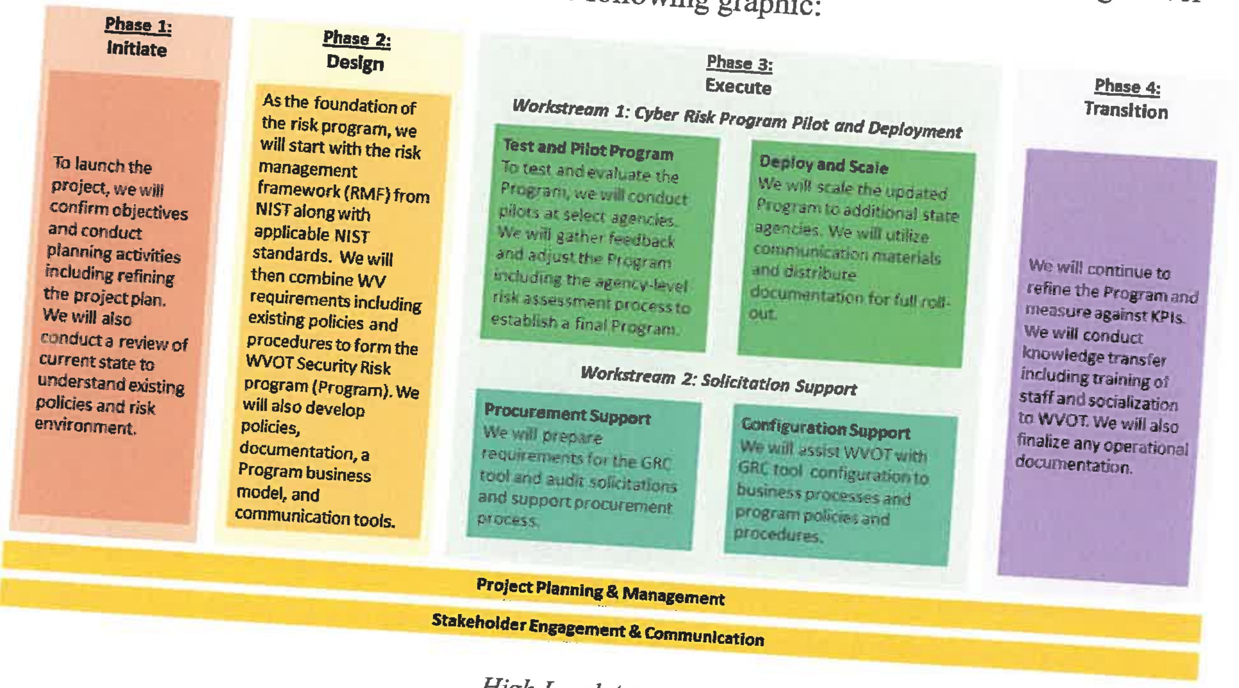
Definition of our terminology

In this proposal we use the term "Risk Management Framework" (RMF) strictly when referencing the standard NIST framework. We use the term "Cyber Risk Program" (Program) to include the implementation and operationalization of the RMF within WV requirements.

Our Approach

Approach Summary

A well-structured and comprehensive cyber risk program is essential to supporting the WVOT's mission to provide highly reliable, secure, and cost-effective technology services to the approximately 210 entities served within the West Virginia Executive Branch. Drawing from our experience in standing up cyber risk programs and leading cybersecurity engagements across the United States, we define a 4-phase approach that meets WVOT's requirements outlined in the RFP and proposes additional activities that will set the program up for success. A high-level overview of our approach is captured in the following graphic:



Phase 1: Initiate

To launch the project, we will confirm objectives and conduct planning activities including refining the project plan. We will also conduct a review of current state to understand existing policies and risk environment.

Phase 2: Design

As the foundation of the risk program, we will start with the risk management framework (RMF) from NIST along with applicable NIST standards. We will then combine WV requirements including existing policies and procedures to form the WVOT Security Risk program (Program). We will also develop policies, documentation, a Program business model, and communication tools.

Phase 3: Execute

Workstream 1: Cyber Risk Program Pilot and Deployment

Test and Pilot Program To test and evaluate the Program, we will conduct pilots at select agencies. We will gather feedback and adjust the Program including the agency-level risk assessment process to establish a final Program.

Deploy and Scale We will scale the updated Program to additional state agencies. We will utilize communication materials and distribute documentation for full roll-out.

Workstream 2: Solicitation Support

Procurement Support We will prepare requirements for the GRC tool and audit solicitations and support procurement process.

Configuration Support We will assist WVOT with GRC tool configuration to business processes and program policies and procedures.

Phase 4: Transition

We will continue to refine the Program and measure against KPIs. We will conduct knowledge transfer including training of staff and socialization to WVOT. We will also finalize any operational documentation.

Project Planning & Management

Stakeholder Engagement & Communication

High Level Approach

We will begin our engagement in phase 1 – **initiate** - by setting up a project management office, developing a comprehensive project management plan, and conducting a current state review of existing risk and cybersecurity policies and procedures. In phase 2 – **design** – we will set the foundation of the WV cyber risk program (Program) by adopting a risk management framework (RMF) guided by NIST standards and WVOT's needs and requirements. To establish the Program in this phase, we will share leading change management, communications, and policy development methodologies to design a robust communication plan, clear Program policies and procedures, and a sustainable business model for the new Program. We will incorporate existing West Virginia policies and procedures along with the RMF to design the WVOT cyber risk Program. In phase 3 – **execute** - our team will divide into two separate workstreams. In workstream 1 – *cyber risk program pilot and deployment* – we will pilot the Program and gather earnings to improve the Program prior to developing a full roll-out plan of the Program to all executive agencies. In workstream 2 – *solicitation support* – our team will assist WVOT in the procurement of a Governance, Risk, and Compliance (GRC) tool and compliance audit solicitation and advise WVOT on configuration of the solicited services. Finally, in phase 4 – **operationalize** - our team will come back together into a single workstream to assess progress against KPIs for the Program's continuous improvement and undertake socialization and training activities so that WVOT is fully equipped to sustain the Program well into the future.

We outline these phases in further detail in subsequent pages of the approach.

Detailed Approach

Phase One: Initiate

Phase 1: Initiate
Purpose To set up PMO and build a common understanding of current state
Key Activities ***PMO (RFP 4.2.1.7)*** • Establish project governance and project management structure • Convene kick off meeting • Develop comprehensive project management plan to include timeline, communication plan, dependencies, milestones, risk register, etc. **(RFP 4.2.2.1)** • Confirm project objectives • Establish status reporting template and meeting cadence for project team and executive sponsors ***Current State Review*** • Collect and review relevant documentation including any existing risk assessments, policies, organizational charts, technology infrastructure, and audit reports • Conduct stakeholder interviews • Identify federal and state requirements • Discuss the advantages and disadvantages of accelerating the selection of a GRC tool
Outcomes • Project management plan including schedule, milestones, communication plan, risk register, and governance • Kick off meeting • Current state review

Project Management Office (RFP 4.2.1.7)

We believe that it is essential to set up a project correctly from the outset. We understand the unique dynamics of building a statewide program across different departments and agencies and the criticality of strong project management, communications and change management practices. We will quickly work to **identify the key players** and establish open channels of communication between Guidehouse and the WVOT Project Team. We will officially launch our project with a **project kick-off meeting** to align project objectives, set expectations, and refine our project plan. In this meeting, we will discuss **project governance** and **meeting cadence** ensuring that Guidehouse and WVOT staff are in frequent contact throughout the project, share progress, and address any roadblocks or constraints quickly and early. From this initial meeting and early consultations between the WVOT and Guidehouse project managers, the Guidehouse team will prepare a refined **project management plan** that provides an updated approach and project overview that includes project scope, roles and responsibilities, timelines, potential risks and issues, assumptions, and dependencies for the project.

Guidehouse is recognized as a world leader in program and project management

- Guidehouse is the only Advisory firm that is a founding member of the PMI Corporate Council.
- Guidehouse was selected to participate in PMI's pilot Organizational Program Management Maturity Model (OPM3®) assessments, recognizing our PM discipline and thought leadership.
- Guidehouse thought leaders contributed to the development of the Government edition of the PMBOK©.

Our **project management methodology** is agile, resulting in an iterative approach that adjusts to the changing demands of the project. We embrace a culture of continuous improvement, documenting lessons learned and seeking feedback to adjust activities for maximum impact and effectiveness. In addition, our team will ensure **transparency** with the WVOT project team communicating early and often to make our partnership to launch this Program a collective success.

In addition to the technical cybersecurity and risk management expertise, we pay special attention to the people elements of this engagement. Establishing a risk management program is a transformation. It changes practices, how decisions are made and how resources are allocated requiring a cultural change. We are known in the industry for our ability to implement change successfully in complex environments. To do this, we use our proven **change management methodology**, (re)Vision®, which focuses on three key principles: people centric change, human centered design, and behavioral economics. Our approach goes beyond traditional change techniques and gets into stakeholders' minds to truly change behavior surrounding cyber risk.

People Centric Change

Anchored in business strategy and desired outcomes. Example activities include change readiness assessments, change vision and strategy, change agent network, and communications planning.

Human Centered Design

Understanding and designing a personal and empowering experience for stakeholders using a five-step process: empathize, define, ask "what if," prototype, and document.

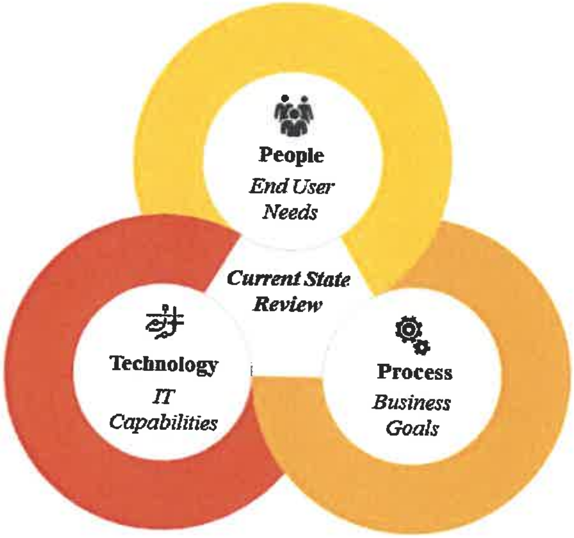
Behavioral Economics

Science-driven tactics and techniques used to create environments that nudge people toward positive change. Example activities include framing, timing, cues, and social context.

Current State Review

As part of our initiate phase, we will conduct a **current state review** of WVOT's existing cybersecurity policies and risk environment. We will request and carefully review existing documentation including risk assessments, policies, organizational charts, technology infrastructure, and audit reports. We will **conduct interviews** with WVOT project team members to understand cyber risk program needs. We will come to understand WVOT's objectives and constraints, organizational structure, and existing policies and identify relevant federal and state requirements. This current state review will provide a baseline understanding for future analysis to occur in the proceeding project phase as we move towards program design and implementation.

Our methodology for the current state review will rely on our tested **people, process, and technology** framework. As we analyze documentation, conduct interviews, and build an understanding of WVOT's needs and existing policies, we will ask questions about the people involved, processes in place, and technology infrastructure available at WVOT. It is important in this phase that we talk with stakeholders that represent leadership, business/mission process, and information systems. We need to get an understanding of how risk is perceived today by the entire organization, how risk decisions are made, what the risk appetite is, and what the risk tolerance criteria are.



Finally, the current state review provides us with an opportunity to evaluate if the GRC tool should be selected earlier in the project timeline. There are advantages in choosing a leading GRC tool that has a proven track record of helping large organizations better manage risks because WVOT could then design its Program around the functions and capabilities of the tool. This could save time over building a program that would require significant, and often costly, customization of the GRC tool. There are disadvantages as well. For instance if WVOT has unique processes that it wants to implement in its Program, it would be difficult to accelerate the choice of a tool until those processes were defined. Our approach accommodates this decision point and accelerated timeline and allows for flexibility to best meet WV's needs.

Phase 2: Design

Phase 2: Design

Purpose

To design a cyber risk program (Program) that is based on the NIST Risk Management Framework, WV policies and standards, and appropriate NIST standards and guidance

Key Activities

Cyber Risk Program Development (RFP 4.2.1.1)

- Identify most critical information assets (i.e. high value assets) and align to applications and agencies
- Evaluate agencies with the highest risk exposure based off their assets and any mandated compliance requirements
- Establish risk profiling procedure and questionnaire
- Develop risk prioritization and accountability taking into account organization maturity and tiering.

Cyber Risk Program Documentation/Creation (RFP 4.2.1.2) and Communication (RFP 4.2.1.7)

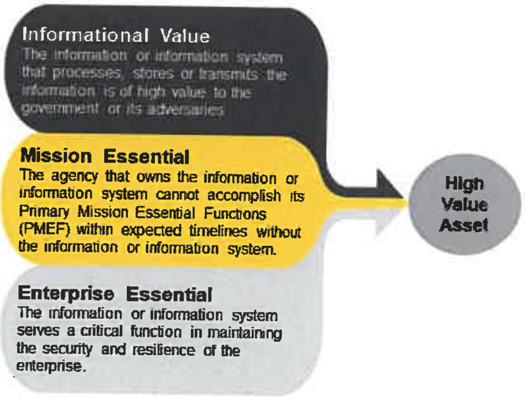
- Develop policies and operations procedures, reporting templates, and Program roadmap
- Define roles and responsibilities between central teams and agencies
- Document approach, tools, templates for agencies to apply Program and manage audit and assessment activities
- Define sustainable business model and determine charge back policies **(RFP 4.2.1.6)**
- Design cyber risk program pilot including timeline, communications, key performance indicators, assessment team members, and 3 groups of differing size, complexity and mission to perform the pilot on.

Outcomes

- Risk assessment results **(Payment Milestone A.2.2.8)**
- Draft Program ready for pilot
- Cyber risk program documentation including policies, procedures **(Payment Milestone A.2.2.7)**, reporting templates **(Payment Milestone A.2.2.2)**, and communication materials
- Program roadmap **(Payment Milestone A.2.2.3)**
- Draft sustainable business model for resources required to run and sustain the cyber risk program

Cyber Risk Management Program Development (RFP 4.2.1.1)

After gaining an understanding of WVOT's processes, policies, and requirements in phase 1, our team will **inventory critical assets (also known as High Value Assets)**, identify the parts of the organization whose mission/business processes are considered higher risk/value, and utilize the NIST **risk management framework (RMF)** to design WVOT's cyber risk program. While the Program needs to work to assess all cyber risks to the organization, it is important to have an initial understanding of high value assets and high risk processes to ensure the Program addresses these critical elements. A necessary first step is determining the IT assets that are most critical for West Virginia and the impact if critical data and information systems become degraded or compromised. This agency impact analysis will rely on stakeholder interviews, documentation reviews and available audit reports. After identifying critical business processes and what IT systems those processes depend on, we will profile assets on three criteria: informational value, mission essential, and enterprise essential.

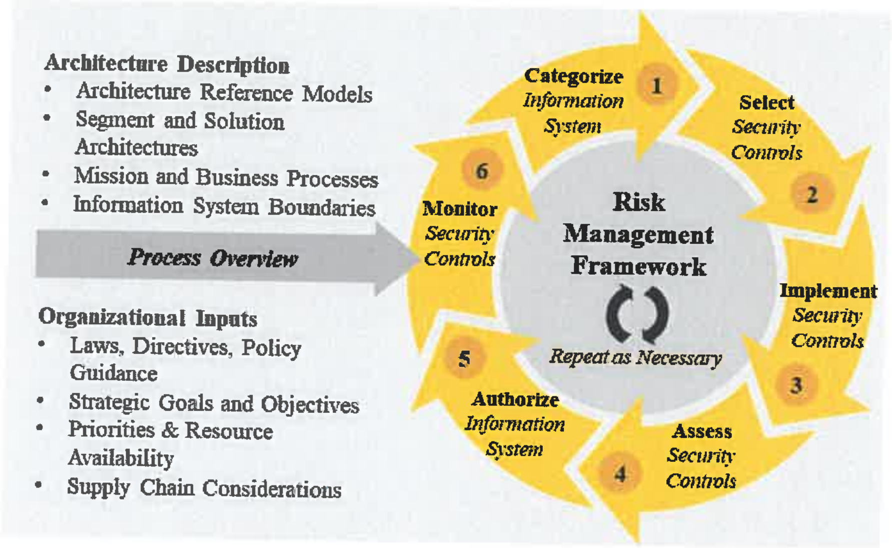


Informational Value
The information or information system that processes, stores or transmits the information is of high value to the government or its adversaries

Mission Essential
The agency that owns the information or information system cannot accomplish its Primary Mission Essential Functions (PMEF) within expected timelines without the information or information system.

Enterprise Essential
The information or information system serves a critical function in maintaining the security and resilience of the enterprise.

Our team will assess each of the State's critical assets and information security against industry best practices and mandated compliance requirements. Our team will use the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) and NIST Cyber Security Framework (CSF) – among other industry standards and guidance – as references. Specifically, we will rely on NIST Risk Management Framework (NIST Special Publication 800.37 "Guide for Applying Risk Management Framework to Federal Information Systems") for our approach, which is included below:


Architecture Description
• Architecture Reference Models
• Segment and Solution Architectures
• Mission and Business Processes
• Information System Boundaries
Process Overview
Organizational Inputs
• Laws, Directives, Policy Guidance
• Strategic Goals and Objectives
• Priorities & Resource Availability
• Supply Chain Considerations
1 Categorize Information System
2 Select Security Controls
3 Implement Security Controls
4 Assess Security Controls
5 Authorize Information System
6 Monitor Security Controls
Risk Management Framework
Repeat as Necessary

Based on an understanding of critical assets, industry guidance, and West Virginia laws and regulations, our team will begin to adopt elements of the NIST RMF tailored to West Virginia's needs and requirements. We will convene meetings and workshops with the WVOT Chief Technology Officer (CTO), Deputy CTO, cybersecurity leads, stakeholders, and engineers to refine the framework and develop a **risk profiling procedure and questionnaire** that can be modeled in common GRC tools. This procedure will incorporate risk questionnaires across organizational, mission/business process, and information systems. In our experience, it is important to define risk tolerance and appetite at the organization level for the risk profiling to be most effective. Our approach includes working with WVOT to help define their risk appetite and tolerance and incorporate this understanding into the risk profile process.

The benefits of a risk profile process include:

- **Standardizing** the assessment of business information risk
- Determining the **relative risk tolerance** for business risk decisions
- Providing a risk **decision methodology** and guidance for stakeholders
- Creating a **repeatable process** for assessing risk within the context of business needs

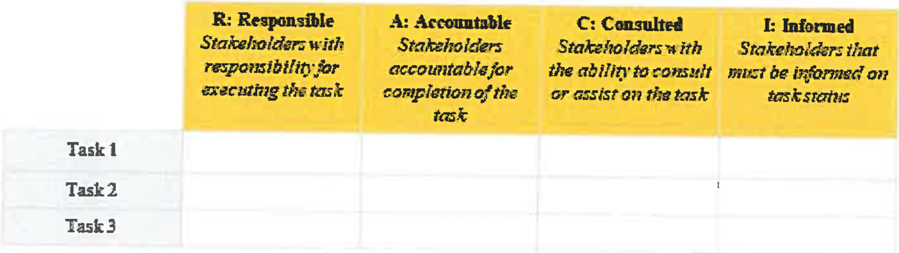
The framework will consider the maturity and needs of each State organization with ownership being assigned between a 3-tiered bottom-up organizational alignment:

- Tier 1 - State
- Tier 2 - Department
- Tier 3 - Agency

We will then pilot this risk profile process with three initial stakeholders of different size, complexity and risks and refine it based on feedback.

Cyber Risk Program Documentation/Creation (RFP 4.2.1.2)

To establish the cyber risk program, Guidehouse will define **policies and operational procedures**, outline **roles and responsibilities**, and develop clear and accessible communications materials and **reporting templates**. To clearly define roles and responsibilities, Guidehouse will establish a stakeholder matrix for WVOT's cyber risk program. The matrix will align appropriate stakeholders to Program goals and tasks by defining the following roles by activity:



	R: Responsible *Stakeholders with responsibility for executing the task*	**A: Accountable** *Stakeholders accountable for completion of the task*	**C: Consulted** *Stakeholders with the ability to consult or assist on the task*	**I: Informed** *Stakeholders that must be informed on task status*
Task 1				
Task 2				
Task 3				

RACI Stakeholder Matrix

Our team will design an actionable cyber risk **Program roadmap**. The roadmap will clearly outline key implementation activities, address change management and communications to different levels of stakeholders, and provide the tools and templates needed to launch the Program successfully both in WVOT and at the agency-level. Documentation will include guidance on how agencies will manage audit and assessment activities as part of the Program. Examples of specific education and documentation distribution activities include:

- Create a knowledge management site that is a repository of all critical documentation
- Educate stakeholders on the enablement of tools through memos, emails, and other available mediums
- Create Standard Operating Procedures (SOPs) for Cyber Risk Program activities
- Develop FAQ's and "guidebooks" to support State agencies with questions or concerns

- Conduct webinars, information sessions, and surveys to collect critical feedback on the effectiveness of the Program from agencies and stakeholders
- Develop campaign materials including posters, newsletters, educational videos to increase Program buy-in

Guidehouse Guiding Principle

Cyber risk decisions are made at the intersection of both business and information technology (IT) functions, and must be informed by a methodology that is repeatable, easy to comprehend, and even easier to communicate.

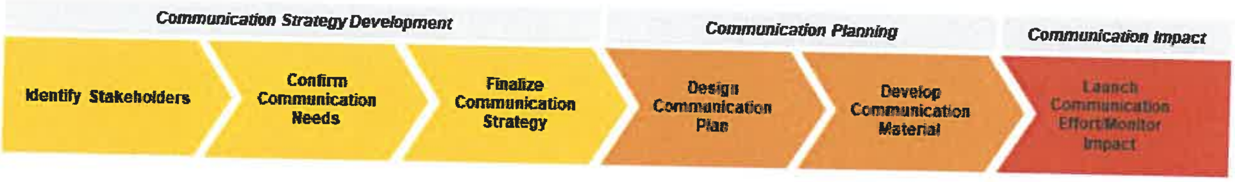
Furthermore, all materials created by the Guidehouse team will support **WV custom branding** and be refined and improved based on feedback.

As an additional step to establish the Program, our team will design a **sustainable business model** for on-going cyber risk support to WV agencies. Defining this model and determining the costs of risk management services will require a review of WVOT's existing charge back model and infrastructure, current cyber security service and software contracts, and benchmarking cost against similar size organizations. Once this review and benchmarking is completed and the required services are identified, Guidehouse will create an initial service catalog for use. The service catalog will include a crosswalk of average price for cyber risk management services that are based on the complexity, and security requirements of individual systems. The work of a cyber professional ebbs and flows and we will define steps for agencies to manage consumption through **economies of scale** or cost sharing to maximize the time spent working. Additionally, cyber resources can be easily reassigned during times of emergencies to perform incident response and other activities. We will also make recommendations on the on-going resources required to execute the cyber risk program.

Case in Point

Security Awareness Campaign and Training Program Development at the Massachusetts Department of Transportation

Guidehouse supported the Massachusetts Department of Transportation to implement a Security Awareness and Training Program that was successfully rolled out to 7,000+ MassDOT and MBTA information system users. The team managed a cross-functional team across multiple departments including human resources, training, information technology, and information security to deploy the training. As part of the campaign, the team developed posters, newsletters, videos, and other materials to promote security culture. Through effective change management, Guidehouse drove compliance from 2% to over 80%. The team's efforts ultimately resulted in MassDOT and MBTA meeting all Key Performance Indicators (KIPs) for year one and two of the program.


Communication Strategy Development
Communication Planning
Communication Impact
Identify Stakeholders
Confirm Communication Needs
Finalize Communication Strategy
Design Communication Plan
Develop Communication Material
Launch Communication Effort/Monitor Impact

Phase 3: Execute

In phase 3, the Guidehouse team will split into two parallel workstreams:

- **Workstream 1: Cyber Risk Program Pilot and Deployment**
- **Workstream 2: Solicitation Support**

Workstream 1: Cyber Risk Program Pilot and Deployment (RFP 4.2.1.2, RFP 4.2.1.5)

Phase 3: Execute

Workstream 1: Cyber Risk Program Pilot and Deployment

Purpose

To test program, adjust to pilot results, and proceed to roll-out to all agencies

Key Activities

Test and Pilot Cyber Risk Program (RFP 4.2.1.2)

- Pilot cyber risk program with three agencies of differing size, complexity and risks.
- Assess results and document lessons learned from pilot
- Adjust program policies, procedures, and materials to reflect lessons learned

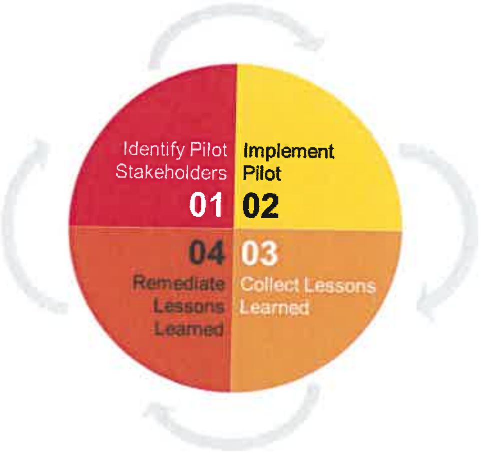
Deploy and Scale Cyber Risk Program (RFP 4.2.1.5)

- Develop roll out plan to incrementally deploy cyber risk program to agencies
- Develop and conduct training activities
- Engage stakeholders, advertise program and carry out communications plan
- Support implementation to agencies

Outcomes

- Pilot implementations in three agencies
- Updated Program **(Payment Milestone A.2.2.1)**
- Cyber Risk Program roll out plan **(Payment Milestone A.2.2.6)**

To assess the efficacy of the cyber risk Program, the Guidehouse team will **pilot the Program** in three agencies of differing size, complexity and risks. These pilots will be conducted in representative agencies and will test key aspects of the Program including the application of the RMF, risk profiles, risk questionnaires, policies and procedures, communications materials, and the Program plan. Workshops will be organized with pilot agency stakeholders and questionnaires distributed to solicit feedback and identify lessons learned. Guidehouse and WVOT will then convene to review and incorporate lessons learned into an updated framework and revised Program materials. Our pilot process builds remediation time into the overall project plan milestones and deadlines to ensure continuous improvement.



Pilot Methodology

Following these pilots, we will be prepared to **scale** the pilot program incrementally across more state agencies. Our team will execute the communication plan, distribute Program materials, policies, and templates and engage key stakeholders. We will bound the pilot and roll-out to nine months and work with you to prioritize the agencies and departments that will be covered in that period.

Workstream 2: Solicitation Support (RFP 4.2.1.3, RFP 4.2.1.4)

Phase 3:Execute
Workstream 2: Solicitation Support

Purpose
To support WVOT procurement process, define requirements, and assist with post-solicitation tool and audit support

Key Activities

Procurement Support (RFP 4.2.1.3 and RFP 4.2.1.4)

- Conduct market research to define the specifications and goals needed to create compliance audit and GRC tool solicitations
- Assist WVOT in developing compliance audit solicitation
- Assist WVOT in developing GRC tool solicitation
- Review solicitation vendor responses and advise reviewers
- Provide guidance and assistance to WVOT to process and assist agencies in using the audit solicitation

Configuration Support (RFP 4.2.1.4)

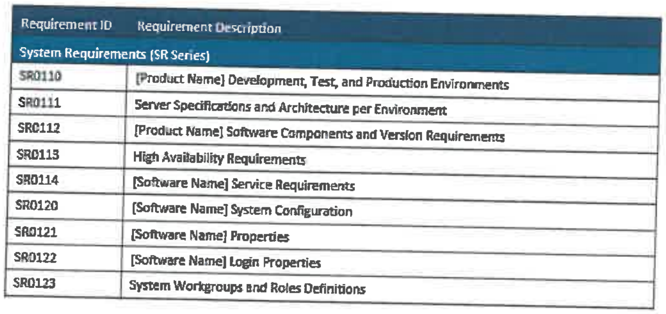
- Configure the governance tool to support future assessment
- Establish baseline security and use procedures for the tool
- Customize the tool to align with state specific requirements established during programs development.
- Train users to utilize the governance tool and develop policies and procedures for the governance tool.

Outcomes

- Compliance audit procurement solicitation **(Payment Milestone A.2.2.4)**
- GRC tool procurement solicitation **(Payment Milestone A.2.2.4)**
- Configuration of governance tool **(Payment Milestone A.2.2.5)**

Procurement Support

While Phase 3: workstream 1 pilots the cyber risk program, Phase 3: workstream 2 will focus on the two solicitations outlined in the RFP. The key to an effective procurement begins with a well-developed solicitation, clearly detailing necessary requirements and desired outcomes of the procurement. In addition to the State of West Virginia's and WVOT procurement and contracting laws, regulations, policies, and other guidance and requirements, the solicitation should include a requirements traceability matrix (RTM) with columns to capture vendors' responses to each detailed business requirement.



Requirement ID	Requirement Description
System Requirements (SR Series)	
SR0110	[Product Name] Development, Test, and Production Environments
SR0111	Server Specifications and Architecture per Environment
SR0112	[Product Name] Software Components and Version Requirements
SR0113	High Availability Requirements
SR0114	[Software Name] Service Requirements
SR0120	[Software Name] System Configuration
SR0121	[Software Name] Properties
SR0122	[Software Name] Login Properties
SR0123	System Workgroups and Roles Definitions

Sample Requirements Traceability Matrix

GRC Tool Procurement Support

For the GRC tool solicitations, our team will conduct market research and define specifications and goals based on our understanding of WVOT's needs and gaps and cyber risk program. We have assisted numerous public sector entities with both the solicitation and implementation of a wide range of GRC solutions (Archer, RiskVision, SAP, etc.) giving us deep, in-house awareness of GRC technologies and the vendor landscape. We are tool agnostic and are committed to helping WVOT find the best tool for Program needs. A comprehensive list of GRC tool solicitation considerations and business requirements are included in the Appendix.

Compliance Audit Procurement Support

For the compliance audit solicitation, our team will incorporate feedback from state agency and WVOT stakeholders to compile an extensive set of compliance audit business requirements and evaluation criteria. Our firm brings a deep history of audit and compliance expertise as we were born out of PwC and we will leverage our past performance to develop compliance audit requirements that include:

- Identifying threats, vulnerabilities, and risks
- Quantifying the level of risk based on probability and likely damage to data or systems
- Developing and prioritizing risk mitigation strategies to critical system functions
- Implementing risk mitigation activities to reduce the risks to acceptable levels
- Continually monitoring both identified risks and emerging threats
- Finding the proper balance between meeting industry best practices while preserving the operational functionality required to successfully execute the mission

After the solicitations are issued and responses received, Guidehouse will advise WVOT in evaluating responses. Once vendors are selected and as workstream 1 concludes their pilot activities and transitions to deployment, the team will support WVOT as needed with configuration of the GRC tool and in providing guidance and assistance for agencies to use the compliance audit solicitation for audits of their agencies.

- Develop functional administrator and end user training in Microsoft PowerPoint based on solution accepted via UAT
- Validate GRC tool readiness for functional administrator and end user training, e.g., readiness of the GRC tool and participants' access to the test environment and GRC tool roles
- Coordinate with WVOT management and schedule functional administrator and end user training, including facilities to support onsite training
- Deliver one functional administrator training session and up to three end user training sessions, simultaneously on-site and virtual for training attendees, coordinating with WVOT to support on-site and remote access to the test environment by training participants, validating WVOT production team's and other stakeholders' participation, coordinating communications to stakeholders and scheduling their attendance, and participating as an observer.

Additional considerations and guidance for the GRC tool solicitation and configuration are included in the appendix. Examples of Guidehouse's extensive GRC tool implementation are listed in the Qualifications sections of this proposal.

Phase 4: Transition

Phase 4: Transition

Purpose
To assess performance and conduct knowledge transfer

Key Activities

Ongoing Implementation Support and Performance Assessment

- Continue to refine Program based on full deployment feedback and experience
- Support WVOT with implementation as needed
- Measure performance against KPIs

Knowledge Transfer and Training

- Train WVOT Program staff
- Socialize program materials and activities with WVOT and leadership to transition responsibilities
- Finalize any operational documentation including updating policies and procedures

Outcomes

- Knowledge transfer materials including presentations, training materials, and updated documentation

Ongoing Implementation Support

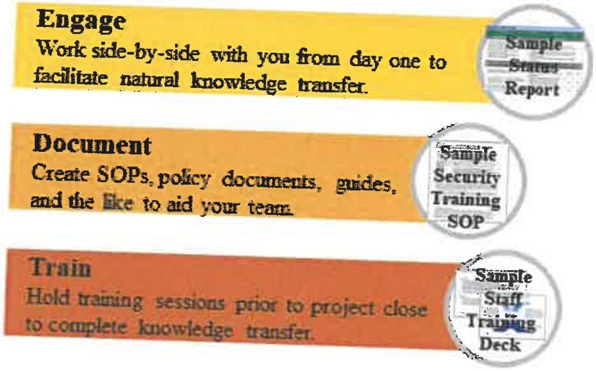
In the final phase of the project, Guidehouse will provide support to operationalize the Program for the long-term including conducting performance measurement and knowledge transfer to the WVOT team. Our team will continue to collect lessons-learned and feedback and revise the Program as needed. We will measure performance against KPIs and leverage the selected GRC tool to observe data on performance.

The Guidehouse team will also support WVOT with additional tasks including updating any materials and documentations and advising on industry frameworks and federal policy guidance.

Knowledge Transfer and Training

We believe helping you build a support organization to operate the Program is critical. Our collaborative approach to the project will ensure socialization and training of WVOT staff occurs from the onset of the Program, but we will dedicate the final weeks of the project to successful transition. Guidehouse will conduct knowledge transfer activities including training Program staff, socializing Program materials, and finalizing any operational documentation including standard operating procedures (SOPs), policies, and Program management materials. We will use our proven tools, templates and accelerators for knowledge transfer and training activities throughout the engagement. Presentations to WVOT and agency leadership will be arranged to formally conclude the engagement.

Our approach to knowledge transfer:



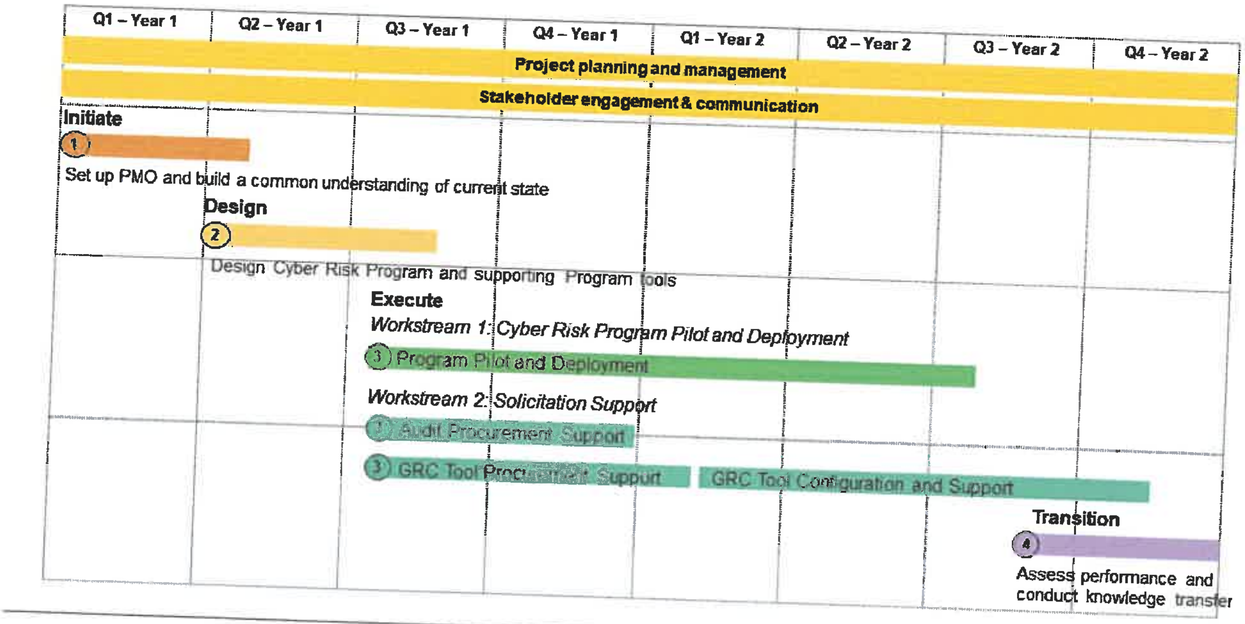
Engage
Work side-by-side with you from day one to facilitate natural knowledge transfer.

Document
Create SOPs, policy documents, guides, and the like to aid your team.

Train
Hold training sessions prior to project close to complete knowledge transfer.

Project Timeline

We have developed the following high-level project timeline based on our understanding of RFP requirements. This timeline will be reviewed in Phase 1 as we develop an understanding of WVOT's needs and requirements and create a comprehensive project plan. We must also review and confirm the scheduling of activities that depend on the WV procurement process. Within the 2-year timeline, the projected schedule of activities may require adjustment to reflect procurement schedules and logistics.

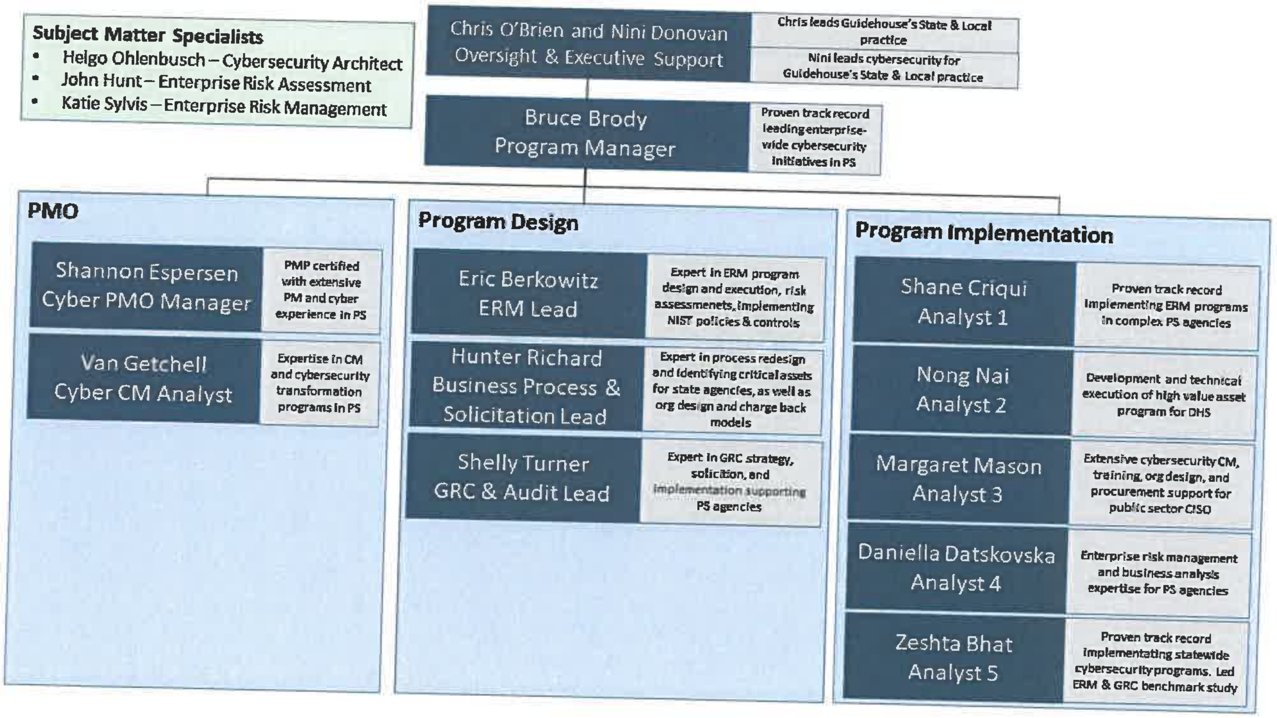


Staffing and Key Staff Qualifications

Proposed Local Organization Structure

Each member of our team has experience successfully providing services of similar nature and complexity required by this engagement, and is highly qualified to help West Virginia Office of Technology. You will also find the intangibles of a quality consultant on our team —personal attention, proactive value-add, fast and accurate responses to questions, frequent and ongoing communication—these are the hallmarks of Guidehouse's approach and commitment.

Nini Donovan will provide oversight for this engagement and Bruce Brody will perform the role of program manager. Our proposed team is depicted below and detailed resumes are provided in the Appendix.[1]



Subject Matter Specialists

- Helgo Ohlenbusch – Cybersecurity Architect
- John Hunt – Enterprise Risk Assessment
- Katie Sylvis – Enterprise Risk Management

Chris O'Brien and Nini Donovan
Oversight & Executive Support
Chris leads Guidehouse's State & Local practice
Nini leads cybersecurity for Guidehouse's State & Local practice

Bruce Brody
Program Manager
Proven track record leading enterprise-wide cybersecurity initiatives in PS

PMO

Shannon Espersen
Cyber PMO Manager
PMP certified with extensive PM and cyber experience in PS

Van Getchell
Cyber CM Analyst
Expertise in CM and cybersecurity transformation programs in PS

Program Design

Eric Berkowitz
ERM Lead
Expert in ERM program design and execution, risk assessmenets, implementing NIST policies & controls

Hunter Richard
Business Process & Solicitation Lead
Expert in process redesign and identifying critical assets for state agencies, as well as org design and charge back models

Shelly Turner
GRC & Audit Lead
Expert in GRC strategy, solicition, and implementation supporting PS agencies

Program Implementation

Shane Criqui
Analyst 1
Proven track record implementing ERM programs in complex PS agencies

Nong Nai
Analyst 2
Development and technical execution of high value asset program for DHS

Margaret Mason
Analyst 3
Extensive cybersecurity CM, training, org design, and procurement support for public sector CISO

Daniella Datskovska
Analyst 4
Enterprise risk management and business analysis expertise for PS agencies

Zeshta Bhat
Analyst 5
Proven track record implementating statewide cybersecurity programs. Led ERM & GRC benchmark study

[1] Final staffing list is dependent on project start date. If any adjustments are required, we will ensure that all staff have the requisite capabilities and experience demanded by the engagement. Furthermore, depending on the GRC tool selection, we are able to deploy additional support staff with specific expertise. Our extensive network of consultants and trained cybersecurity professionals allows us to devote staff rapidly as the needs of the Program evolve.

Project Team Overviews

Staff Member	Expertise Relevant to RFP	Experience Highlights
Chris O'Brien, Executive Oversight	State & Local Government, Cybersecurity, Enterprise-Wide Technology Implementation	Chris leads Guidehouse's State and Local Government Advisory Practice and has over 20 years of experience helping governments and companies embrace new technologies and improve performance. Prior to joining Guidehouse, he served as CIO for the City of Chicago, where he oversaw several large scale technology programs.
Nini Donovan, Oversight and Executive Support	State & Local Government, Cybersecurity, IT Transformation, Stakeholder Engagement	Nini is a Managing Director at Guidehouse and has 19 years of technology and management consulting experience. She leads Guidehouse's cybersecurity practice for state and local governments nationwide. Her recent engagements include leading a statewide cybersecurity transformation program for the state of Massachusetts and an identity governance engagement for the state of Florida.
Bruce Brody, Program Manager	Governance Risk & Compliance (GRC) Tool, Project Management, Cybersecurity Risk Management	Bruce is a certified cybersecurity professional (CISSP, CAP, CISM, CFCP) who has operated as both CISO and an external consultant for public sector agencies, such as the DOD, VA, and DOE. He has a proven track record implementing risk management programs and GRC solutions for public sector agencies.
Shannon Esperson, Cyber PMO Manager	State & Local Government, Project Management, Cybersecurity Solutions	Shannon is a certified Project Management Professional and has a strong balance of cyber, project management and public sector experience. She is currently leading a team that is implementing an identity access and governance system across a major Florida state agency.
Van Getchell, Cyber CM Analyst	State & Local Government, Change Management, Cybersecurity Documentation	Van is a Senior Associate at Guidehouse and has over 8 years of experience working as a project manager and change management lead. She recently led an assessment of a Massachusetts state agency's IT change management process and developed recommendations to improve cybersecurity practices.
Eric Berkowitz, ERM Lead	Enterprise Relationship Management (ERM), Project Management, NIST Compliance	Eric is a Director at Guidehouse with numerous cybersecurity certifications (CAP, RiskVision, etc.) and is also a Project Management Professional. He has led several enterprise-wide cybersecurity and risk assessment programs for the FBI.

Hunter Richard, Business Process & Solicitation Need	State & Local Government, Business Process Redesign (BPR), Charge Back Models	Hunter is a Manager at Guidehouse and brings significant expertise in business process redesign, change management, and charge back models with public sector organizations. His recent engagements have included critical asset discovery and identity access management process assessment for the state of Massachusetts.
Shelly Turner, GRC & Audit Lead	Governance Risk & Compliance (GRC) Tool, Implementation, Assessments	Shelly is a Director at Guidehouse and has over 15 years of experience in IT, including large scale system implementation, IT security, and audit readiness/remediation. She also has proven expertise in implementations of GRC tools to automate IT security controls and processes.
Shane Criqui, Analyst 1	Enterprise Relationship Management (ERM), NIST Compliance, Cybersecurity	Shane is a Senior Associate at Guidehouse with more than seven years of cybersecurity experience within the government, military, and commercial sectors. He is certified in Security+ and has expertise in risk management, regulatory compliance, and cybersecurity culture, training, and awareness.
Nong Nai, Analyst 2	Cybersecurity, High Value Asset, Risk Management	Nong is a Manager at Guidehouse with over ten years of experience in cybersecurity program development and management, as well as data-driven program performance improvement and maturation. He has extensive expertise delivering High Value Asset (HVA) programs to federal agencies.
Margaret Mason, Analyst 3	Cybersecurity, Stakeholder Training, Procurement Support	Margaret is an Experienced Associate at Guidehouse and brings proven expertise in cybersecurity, change management, and organizational redesign. She recently supported the implementation of a Security Awareness and Training program for information system users across a Massachusetts state agency.
Daniella Datskovska, Analyst 4	Enterprise Risk Management (ERM), Compliance, Business Processes	Daniella is a certified Project Management Professional that holds multiple certifications in cybersecurity and risk management (CRMP, etc.). She has served numerous public sector clients, such as the Department of Agriculture, the, DOJ, and DHS, to develop and implement ERM strategies.
Zeshta Bhat, Analyst 5	State & Local Government, Enterprise Relationship Management (ERM), Governance Risk & Compliance (GRC) tool	Zeshta is a Manager at Guidehouse and an experienced cybersecurity professional specializing in development and standardization of processes across different security and IT domains. She is currently providing project management and technical support for the state of Massachusetts's enterprise-wide

		implementation of an identity and access management solution.
Helgo Ohlenbusch, Subject Matter Specialist	Cybersecurity, Enterprise Security, Technical Implementation Support	Helgo is a Senior Information Security Solution Architect at Guidehouse and holds multiple cybersecurity certifications (CCSP, etc.). He has been involved in several Cloud migration projects and has significant experience in enterprise security as a security solution architect and principle security architect.
John Hunt, Subject Matter Specialist	Cybersecurity, Enterprise Risk Assessment, IT Strategy, Information Security Solution Implementation	John is a Partner at Guidehouse with over 20 years of experience assessing and helping mitigate cyber risks across commercial and public sector clients. He has worked a variety of projects designing and evaluating high assurance networking devices, implementing enterprise-wide security solutions, and assessing IT systems for vulnerabilities.
Kate Sylvis, Subject Matter Specialist	Enterprise Risk Management, Cyber Risk Assessment, Governance Risk & Compliance (GRC)	Kate is a Director at Guidehouse and has 17 years of experience in providing governance and compliance services to public and private sector clients, including the U.S. Treasury. Most recently, she led a team performing a cyber risk assessment from an ERM perspective for the Centers for Medicare and Medicaid.

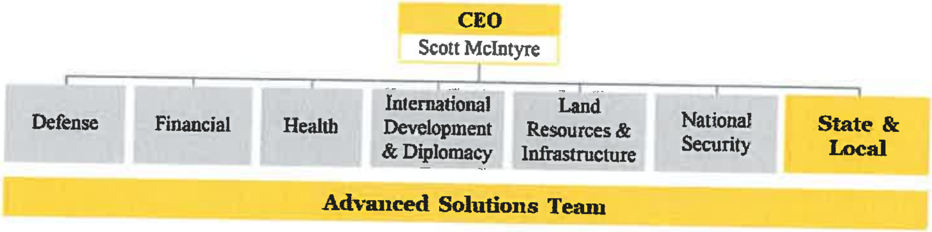
Vendor Background and Company Qualifications

Our Company

Guidehouse (formerly PwC Public Sector) is a national leader in advisory services consulting to the public sector with approximately 1,600 professionals dedicated to serving State, Local, and Federal clients. We have been supporting U.S. government agencies for more than 120 years and are able to cater to the specific needs and nuances of government entities.

We are proud of our track record of successful service to government agencies across the U.S. and, in particular, our reputation for delivering exceptional results and building trust with our clients. We received the 2014 Malcolm Baldrige National Quality Award, presented annually by the President of the United States to organizations that demonstrate performance excellence through innovation, improvement, and visionary leadership. Guidehouse is the only professional services firm to achieve this recognition, and it is a testament to our commitment to quality service.

Guidehouse forms the consulting industry's first large firm dedicated to the needs of government policy makers, project managers and agency heads. The Guidehouse team, and specifically our State and Local Government and Advanced solutions practices support numerous City and State agencies across the U.S.



Guidehouse Organizational Structure

Guidehouse's State and Local Government practice is a leader in helping cities and states execute change. Our consulting practice blends depth and expertise with commercial leading practices. We focus on connecting citizens with government, planning and driving local investments, and increasing efficiency to promote long-term economic, environmental, social, and cultural prosperity. Our services cover strategy through execution for our clients' critical business and information technology needs, including enterprise policy development, program implementation and management, business process redesign, risk assessment, and technology modernization. In addition to our State and Local practice, Guidehouse continues to expand its highly skilled Advanced Solutions team that focuses on cyber, enterprise risk management (ERM), analytics, artificial intelligence (AI), and digital and emerging technologies. These two complementary practices bring a knowledgeable and committed team of both management and technology consultants to support this engagement.

Our Experience and Project References

Our competencies and qualifications

We employ a number of consultants with diverse skill sets in cyber security, and we commit to both quick and sustained responsiveness to WVOT's needs. Guidehouse's depth and breadth of knowledge for this engagement is extensive and our team of experienced professionals understands the nuances of this work. Few firms can match the number and quality of resources we bring to this contract. Our robust revenue growth, recent smooth departure from the PwC network, and subsequent long-term investment and support from our new owner, Veritas Capital, speaks to the strength and stability of our firm and our ability to deliver the terms of this contract.

We identify the following qualifications that demonstrate our experience in **enterprise policy development, program implementation/management, strategic planning,** and **risk assessment** required for this engagement and to successfully carry out the activities of our approach. Our direct cyber security program experience spans critical public organizations at both the national (e.g, the Department of State, the Department of Homeland Security, and the Federal Bureau of Investigation) and the State levels (e.g, the Massachusetts Department of Transportation and the Florida Department of Transportation). The experience outlined below provide us with the tools to successfully ask the right questions to analyze organizational risk postures, develop comprehensive frameworks, and evaluate cyber risk fairly and effectively.

The below table illustrates how previous Guidehouse engagements pertain to this proposal. Full descriptions of these projects including reference contact information is included at the end of this section.

Qualification Overviews

Summary of Education Project Experience	Relevant RFP Requirement
U.S. Department of State – Cyber Risk Management Office The U.S. Department of State engaged Guidehouse to conduct a cybersecurity risk management gap analysis, with the goal of determining where the Department needed to bolster existing cybersecurity risk management processes, policies, procedures, and governance. Guidehouse's Cybersecurity Risk Management Strategy led to the development and approval of a new enterprise cybersecurity risk management office, charged with leading the identification, management, and monitoring of cybersecurity risk for the Department's mission and business processes.	• Enterprise Policy Development • Program Implementation/ Management • Risk Assessment • Strategic Planning
Department of Homeland Security National Protection and Programs Directorate, now Cybersecurity and Infrastructure Security Agency –	• Enterprise Policy Development

Summary of Education Project Experience	Relevant RFP Requirement
Federal Network Resilience, Federal Information Security Modernization Act, and Data Analytics Support Guidehouse supported CyberStat risk posture reviews at CISA throughout all major phases of the risk review process, including the presentation, execution, follow-up, and closure of items tied to the process. Guidehouse also updated and analyzed FISMA cybersecurity performance metrics, which helped agency leadership to visualize the maturity of their organization and provide definitive data in order to make executive decisions on how to protect and defend their agency's cybersecurity initiatives.	• Program Implementation/ Management • Risk Assessment • Strategic Planning
Federal Bureau of Investigation – Cybersecurity Program Management, Implementation, and Administration Guidehouse supported the FBI to provide cybersecurity program management, implementation, and administration for the FBI Cybersecurity Red and Blue Team Program (REBL), which aims to build teams of cyber experts to bolster the Bureau's networks against internal and external threats. Ultimately, Guidehouse helped the FBI to better prevent, detect, respond and contain an advanced targeted attack on the Bureau network and improved organizational design, operating procedures, policies, and communications.	• Enterprise Policy Development • Program Implementation/ Management • Risk Assessment
Massachusetts Department of Transportation – Enterprise Policy Development MassDOT selected Guidehouse to assist in establishing a foundation for maturing its information security posture through enterprise policies. Throughout the life of the project, Guidehouse maintained a Project Management Office (PMO), and helped establish the right measures, structure, and stakeholder involvement to be effective in the implementation and monitoring of enterprise policies across the organization.	• Enterprise Policy Development • Program Implementation/ Management • Risk Assessment
Federal Bureau of Investigation – Risk Review and Prioritization Guidehouse is engaged by the FBI to stand up a Risk Review and Prioritization Program that will assign risk levels to FBI systems to promote better understanding, transparency, and management of IT risks. Through Guidehouse's work, FBI leadership gained awareness of its organizational risks and can leverage a process to allocate resources based on costs relative to mitigating and managing risks, resulting in a mitigation strategy aligned with funding needs.	• Enterprise Policy Development • Program Implementation/ Management • Risk Assessment
Florida Department of Transportation – Cybersecurity Risk Management Benchmarking The FDOT Office of Information Technology (OIT) consulted Guidehouse on best practices and recommendations for assessing and monitoring	• Risk Assessment • Strategic Planning

Summary of Education Project Experience	Relevant RFP Requirement
security-related risks and mitigating other cybersecurity risk management challenges faced by the organization. The findings from this engagement will help FDOT in implementing an effective cybersecurity risk management program/framework across the organization's various functions.	
Massachusetts Department of Transportation – Business Impact Analysis Guidehouse launched a business impact analysis at MassDOT as the first step in developing an IT disaster recovery plan entailing asset discovery and current state analysis, risk identification and business impact analysis, and strategic roadmapping. The project team produced a document that, whether in the case of an infrastructure failure or cybersecurity breach, tiered MassDOT's technical assets according to restoration prioritization.	• Enterprise Policy Development • Risk Assessment • Strategic Planning
Massachusetts Executive Office of Technology Services and Security – Identity and Access Management Statewide Program Development EOTSS engaged Guidehouse to support standing up a statewide Identity & Access Management (IAM) program to ensure that the right people are provided access to the right resources with an appropriate level of authentication across the enterprise. Successful implementation of the IAM technology solution will save significant state resources, streamline operations, integrate state IT security processes, and strengthen the state's overall security posture across the Commonwealth.	• Enterprise Policy Development • Program Implementation/ Management

Detailed Qualifications and Reference Information

We are proud of our track record in serving our clients. The detailed qualifications and reference contact information below provide insight into our performance and are available to substantiate any experience disclosed below:

Name of Client	**U.S. Department of State**	
Engagement Title	Cyber Risk Management Office	
Project Manager and Contact Information	**Name**	Peter Gouldmann
	Telephone Number	(202) 472-8283
	Email Address	gouldmannp@state.gov

Description of Project Goals, Objectives, and Methodology	The U.S. Department of State engaged Guidehouse to conduct a cybersecurity risk management gap analysis, determining where the Department needed to bolster existing cybersecurity risk management processes, policies, procedures, and governance. The Guidehouse team leveraged our experience with the National Institute for Science and Technology (NIST) Risk Management and Cybersecurity Frameworks, as well as the best practices in framing, assessing, monitoring, and responding to risk for our clients. This lead to the development of a comprehensive roadmap to document the implementation and execution activities required to improve cyber risk posture throughout the enterprise. Our teams were able to quickly ramp up and obtain buy-in from executives throughout the Department, including the Chief Information Officer, Chief Information Security Officer, and the Enterprise Cyber Risk Officer, while we simultaneously created an awareness campaign outlining the importance of managing cyber risk to the enterprise. Through this effort we were able to deliver a consistent message that resonated with mission and business owners, creating institutional buy-in and rapidly evolving our ability to collect key data points throughout the organization. Once the gap assessment and roadmap were complete and the final review of the materials had been conducted with our client, the Guidehouse team was asked to continue to support the Department, taking action to implement and execute the creation of a new cyber risk office, and associated cyber risk management program across the Tier 1 (organizational), Tier 2 (mission/business), and Tier 3 (systems) elements of the Department. Our team supported the creation of a Department-wide Cybersecurity Risk Management Strategy document, outlining how and why the organization should address cyber risk, and updated the foundational policy documents within the Department. Our Cybersecurity Risk Management Strategy led to the development and approval of a new enterprise cybersecurity risk management office, charged with leading the identification, management, and monitoring of cybersecurity risk for the Department's mission and business processes. We proposed a structure focused on five key capabilities to help the Department of State better address cyber risk: High Value Assets (HVA) project coordination, cyber risk analysis, cyber risk assessment, governance, and project management. Through the development of new governance and the integration of cyber risk into existing IT and cyber-related boards, Guidehouse enabled the

	Department of State to establish clear information process flows, as well as documented cyber risk equities across elements of the Department. Guidehouse was also able to enhance collaboration across organizational functions by clearly defining appropriate risk management roles and responsibilities, bringing to bear our in-depth understanding of the cybersecurity environment and a rigorous stakeholder analysis approach. Additionally, the project team leveraged existing tools already in the environment, e.g. SharePoint Online, to create a knowledge management reference library of key risk-related material and work product, maintaining the organization's ability to share information and developing a single repository for the enterprise.

Name of Client	**Department of Homeland Security (DHS) National Protection and Programs Directorate (NPPD), now Cybersecurity and Infrastructure Security Agency (CISA)**	
Engagement Title	Federal Network Resilience (FNR), Federal Information Security Modernization Act (FISMA), and Data Analytics Support	
Project Manager and Contact Information	**Name**	Markita Poindexter
	Telephone Number	703-705-6008
	Email Address	markita.poindexter@hq.dhs.gov
Description of Project Goals, Objectives, and Methodology	The Department of Homeland Security's (DHS) Cyber and Infrastructure Security Agency (CISA) plays a central role in the management of cybersecurity across the Federal government, with the responsibility of empowering Departments and Agencies (D/As) with information, assessments, recommendations, and leading practices to strengthen their cybersecurity posture as new threats arise and technology evolves. Guidehouse supported CyberStat risk posture reviews for both Chief Financial Officer (CFO) Act and independent, non-CFO Act agencies. Guidehouse's specialists assisted with all major phases of the CyberStat risk review process including the preparation, execution, follow-up, and closure of items tied to the process. During these reviews, Guidehouse evaluated each agency's cybersecurity strengths, weaknesses, and overall risk posture. The project team also recognized agencies meeting FISMA requirements, highlighted capability areas in need of additional focus, and ultimately helped agencies remove barriers to meeting Federal standards. Guidehouse also built a program management structure to sustain	

	CyberStat review timelines, while incorporating the necessary research and analysis to deliver successful engagements. These deliverables were crucial to driving management-level conversations and leveraged lessons learned across the Federal enterprise in order to improve Federal Information Technology (IT) security from a risk management perspective. Guidehouse also updated and analyzed FISMA cybersecurity performance metrics, working with agencies to measure and report on their cybersecurity program performances. In partnership with a government regulatory agency and Guidehouse support, DHS produced the Annual FISMA Report, which is submitted to Congress and provides insight into the Federal government's overall cybersecurity performance. Guidehouse helped agencies implement performance management strategies which allow for more accurate responses to metrics and a more realistic presentation of cyber risk posture. Guidehouse also leveraged performance management concepts to validate the integrity of the data that agencies report to DHS using quantifiable measurements, such as following up with agencies when responses are outside of a standard deviation or do not meet Federal requirements. Guidehouse updated risk metrics periodically to maintain pace with the rate of innovation and new Federal requirements, with the aim of continuing to improve agency cybersecurity risk posture as well as the resiliency of the Federal enterprise. These metrics allowed agency leadership to visualize the maturity of their organization and provide definitive data in order to make executive decisions on how to protect and defend their agency's cybersecurity initiatives.

Name of Client	**Federal Bureau of Investigation (FBI)**	
Engagement Title	Cybersecurity Program Management, Implementation, and Administration	
Project Manager and Contact Information	**Name**	Matthew J. Smith
	Telephone Number	(202) 651-4029
	Email Address	mjsmith1@fbi.gov
Description of Project Goals, Objectives, and	As a subcontractor to ECS Federal, LLC, Guidehouse supported the Federal Bureau of Investigation (FBI), Office of the Chief Information Officer (OCIO) to provide cybersecurity program management,	

Methodology	implementation, and administration for the FBI Cybersecurity Red and Blue Team Program (REBL). The REBL program aims to build teams of cyber experts to bolster the Bureau's networks against internal and external threats. To achieve this goal, Guidehouse established and led the FBI REBL Project Management Office (PMO) which guided the day-to-day operations of the Red Team, Blue Team, and Mitigation and Support Team (MST). As part of this work, Guidehouse was also tasked with establishing the Enterprise Vulnerability Assessment Program (EVAP), which provided enterprise vulnerability scanning across all FBI system enclaves and classification levels to increase the visibility endpoint security within the FBI IT ecosystem. Other key penetration testing and vulnerability assessment support efforts included leading Red Team penetration testing operations and assessments, leading Red Team exercise communications and coordination with FBI Field Office (FO) stakeholders to scope Rules of Engagement (ROE), managing the procurement, deployment, and hands-on operation of vulnerability scanning tools to automate the enumeration and reporting of vulnerabilities for IT infrastructure components, and developing enterprise wide vulnerability scanning standard operating procedures and vulnerability management policies. Additionally, Guidehouse developed relationships with system stakeholders and executive leadership, and obtained an in-depth understanding of the state of FBI systems, networks, information and criminal and national security missions to provide on-demand vulnerability scans and technical support. They also developed the EVAP Security Assessment and Authorization (SA&A) Team to assist system owners and Information System Security Officers (ISSOs) with performing technical security control assessments based on the NIST SP 800-53 security and privacy controls, identifying and recommending mitigation for vulnerabilities for systems to receive Authority to Operate (ATO). Finally, the team managed communication with FBI executive leadership, reporting of FBI REBL contract status, onboarding of personnel, and training requirements. Ultimately, Guidehouse helped the FBI to better prevent, detect, respond and contain an advanced targeted attack on the Bureau network and improved organizational design, operating procedures, policies, and communications.

Name of Client	**Massachusetts Department of Transportation (MassDOT)**

Engagement Title	Enterprise Policy Development	
Project Manager and Contact Information	**Name**	Gary Foster, Chief Information Officer (CIO)
	Telephone Number	617-222-1905
	Email Address	gfoster@mbta.com
Description of Project Goals, Objectives, and Methodology	MassDOT selected Guidehouse to assist with a series of initiatives to prioritize information security across the organization. The goal of this engagement was to help MassDOT establish a foundation for maturing its information security posture through enterprise policies. A key success factor was building stakeholder support and commitment throughout the organization for improving security, as well as helping stakeholders view security as an organizational issue rather than simply a responsibility of the IT department. To achieve the above objectives, Guidehouse assessed MassDOT's current information security policy landscape for gaps relative best practices and industry-leading standards. Subsequently, the team drafted a new set of standard enterprise security policies addressing these gaps uniformly across the organization. Finally, Guidehouse socialized these policies and developed a governance process, KPIs, and an implementation plan to support MassDOT's successful adoption of these policies. Guidehouse's development of enterprise security policies for MassDOT spanned three phases: 1) Current State Assessment, 2) Future State Policy Development, and 3) Governance Process Development. Throughout the life of the project, Guidehouse maintained a Project Management Office (PMO) in order to develop project plans and reporting templates, provide status reports, document issues and risks, and ensure effective stakeholder engagement. The team focused on governance and helping MassDOT establish the right measures, structure, and stakeholder involvement to be effective in the implementation and monitoring of enterprise policies across the organization.	

Name of Client	**Federal Bureau of Investigation (FBI)**	
Engagement Title	Risk Review and Prioritization	
Project Manager and Contact	**Name**	Vito Ponzio, Acting Unit Chief
	Telephone Number	(202) 203-1766

Information	**Email Address**	vponzio@fbi.gov
Description of Project Goals, Objectives, and Methodology	Guidehouse is engaged by the Federal Bureau of Investigation (FBI) as a part of the Insider Threat and Digital Risk Section assisting with the Risk Review and Prioritization (RRP) Priority Initiative. With this initiative, the FBI is seeking to stand up a Risk Review and Prioritization Program that will assign risk levels to FBI systems to promote better understanding, transparency, and management of IT risks. As part of the initial implementation of RRP, Guidehouse managed the project purpose, scope, and timeline for gathering enterprise-wide Mission Essential definitions and system impact criteria, as well as assisted with prioritizing FBI systems. The project team developed criteria for FBI Division leaders to vet systems by determining the impact of each system on their respective missions. The systems had a relative impact criteria determination that documented each system's impact on the Mission Essential Functions of the FBI. The systems were then assigned vulnerability scores to identify the likelihood of compromise or data loss. With this information, Guidehouse implemented a System Categorization Process workflow in RiskVision, based on NIST 800-60. This automates the process by which System Owners document their systems' data types and information, and automatically assigns the Confidentially, Integrity, and Availability determinations to assist the organization in quickly selecting proper security controls for their information systems. Through Guidehouse's work, FBI leadership gained awareness of its organizational risks and can leverage a process to allocate resources based on costs relative to mitigating and managing risks, resulting in a mitigation strategy aligned with funding needs.	

Name of Client	**Florida Department of Transportation (FDOT)**	
Engagement Title	Cybersecurity Risk Management Benchmarking	
Project Manager and Contact Information	**Name**	Stephanie Tanner, Information Security Manager (ISM)
	Telephone Number	(850) 414-4011
	Email Address	Stephanie.Tanner@dot.state.fl.us

Description of Project Goals, Objectives, and Methodology	The Florida Department of Transportation (FDOT) Office of Information Technology (OIT) consulted Guidehouse on best practices and recommendations for assessing and monitoring security-related risks and mitigating other cybersecurity risk management challenges faced by the organization. As part of the effort, Guidehouse conducted a benchmarking research on peer transportation agencies, including the Massachusetts Bay Transportation Authority (MBTA) and the Southeastern Pennsylvania Transportation Authority (SEPTA). Guidehouse interviewed key Cybersecurity executives at MBTA and SEPTA to gain an understanding of their existing risk management practices, pain points, governance technologies and solutions, and strategy around risk communication to stakeholders. Findings from this benchmarking exercise and recommendations provided by Guidehouse will help FDOT in implementing an effective Cybersecurity risk management program/framework for the organization.

Name of Client	**Massachusetts Department of Transportation (MassDOT)**	
Engagement Title	Business Impact Analysis	
Project Manager and Contact Information	**Name**	Gary Foster, Chief Information Officer (CIO)
	Telephone Number	617-222-1905
	Email Address	gfoster@mbta.com
Description of Project Goals, Objectives, and Methodology	The Massachusetts Department of Transportation (MassDOT) launched a business impact analysis (BIA) as the critical first step in developing an IT disaster recovery plan for the agency. Guidehouse supported MassDOT with this initiative by identifying its core business processes, the applications and systems that support those processes, and current recovery capabilities in the event of a disaster. The project was divided into three phases: discovery and current state analysis, risk identification and business impact analysis, and roadmap. In the current state, the project team mapped which applications, systems, and services support MassDOT's core business processes across all of the agency's departments. With the current state and mapping established, the Guidehouse team then determined disaster scenarios relevant to MassDOT IT's disaster recovery and cyber security efforts. In the second phase, the project team assessed current recovery capabilities and performed a gap analysis between desired and current capabilities, as well	

	as determined criticality tiers of the agency's applications and systems. In the event of a disaster scenario, whether an infrastructure failure or cyber security breach, this document outlined what technological assets should be prioritized when restoring operability. Lastly, the project team provided a roadmap for MassDOT to prioritize disaster recovery planning and assist in business socialization of the BIA.

Name of Client	**Massachusetts Executive Office of Technology Services and Security (EOTSS)**	
Engagement Title	Statewide Identity and Access Management Program Development and Support	
Project Manager and Contact Information	**Name**	Sangit Tamang
	Telephone Number	(617) 626-4630
	Email Address	sangit.tamang@mass.gov
Description of Project Goals, Objectives, and Methodology	The Massachusetts Executive Office of Technology Services and Security (EOTSS) engaged Guidehouse to support standing up a statewide Identity & Access Management (IAM) program to ensure that the right people are provided access to the right resources with an appropriate level of authentication across the enterprise. The program supports over 80 agencies across nine state secretariats including Administration and Finance, Education, Energy and Environmental Affairs, Health and Human Services, Housing and Economic Development, Labor and Workforce Development, Public Safety and Security, Transportation, and Technology Services and Security. Successful implementation of the IAM technology solution will save significant state resources, streamline operations, integrate state IT security processes, and strengthen the state's overall security posture across the Commonwealth. Guidehouse has significantly enhanced the security of various aspects of EOTSS operations through this statewide program. Guidehouse's program has enabled multi-factor authentication on 160+ infrastructure and application servers, and successfully implemented multi-factor authentication for password checkouts on 270+ privileged accounts. Guidehouse also integrated over 40 legacy and modern applications across different agencies supporting critical government functions, and was able to improve the effectiveness of existing identity governance workflows. With Guidehouse's support, EOTSS continues to enhance the security of its enterprise with this IAM program.	

GRC Tool Implementation Experience

Guidehouse has implemented numerous SharePoint solutions to help manage risk and compliance programs for our clients, including the DHS, Department of the Interior, U.S. Coast Guard, U.S. Customs and Border Patrol, FBI, Federal Emergency Management Agency, National Institutes of Health, and U.S. Immigration and Customs Enforcement. For more robust functionality and scalability, including supporting multiple risk and compliance programs and other use cases, we have implemented COTS GRC tools. The table below presents some of our COTS GRC tool implementations.

GRC Tool	Client and Project Description
RiskVision	Implemented a RiskVision GRC solution at the **FBI** for use by the Bureau in managing its Information System Authorization and Accreditation (A&A) and Federal Information Security Modernization Act (FISMA) Compliance programs. This includes maintaining all relevant control documentation, audit findings, and plans of action and milestone (POA&M) and tracking audit finding remediation progress.
RSA Archer	Implemented a RSA Archer GRC solution at the **U.S. Department of Agriculture (USDA)** for use by the department and its 40+ agencies and staff offices. The GRC solution provides an integrated, electronic workflow enabled single solution for the USDA's A-123 and the Office of the Inspector General (OIG) and General Accounting Office (GAO) audit follow up programs.
SAP GRC	Implemented a SAP GRC solution at the **USDA** to monitor automated application key control configurations and high-risk transactions in its SAP financial system. This provides continuous controls monitoring over the process controls operated in the SAP financial system and transactions processed that may violate policy, e.g., duplicate vendor payments, split purchases, etc.
SAP GRC	Implemented a SAP GRC solution at the **U.S. Department of the Navy** to manage its user access over its enterprise-wide SAP financial system. This includes segregation of duties (SOD) and least privilege rules for users of the system to support identification of access conflicts for remediation and to support informed user access provisioning against the SAP GRC access rules.
Oracle GRC	Assessed and identified gaps and made recommendations for enhancing the **DHS's** Oracle GRC SOD and least privilege user access rules to focus on risks at the Oracle financial system function level. Creating SOD and least privilege access rules at the function level of a financial system helps ensure the rules do not operate on false assumptions about the user access design and leave the organization open to undetected violations.
Oracle GRC	Assessed and identified gaps and made actionable recommendations for redesigning the **NIH** Oracle GRC SOD and least privilege user access rules for its Oracle financial system to focus on risks and eliminate irrelevant rules that generate false positives. The changes we proposed to the SOD and least privilege user access rules focus on the relevant user access risks in NIH Oracle financial system.

Use or disclosure of data contained on this page is subject to the restriction on the title page of this document.

Appendix

Developing a GRC tool solicitation

At a high level, the GRC tool solicitation should include detailed business requirements covering the following areas:

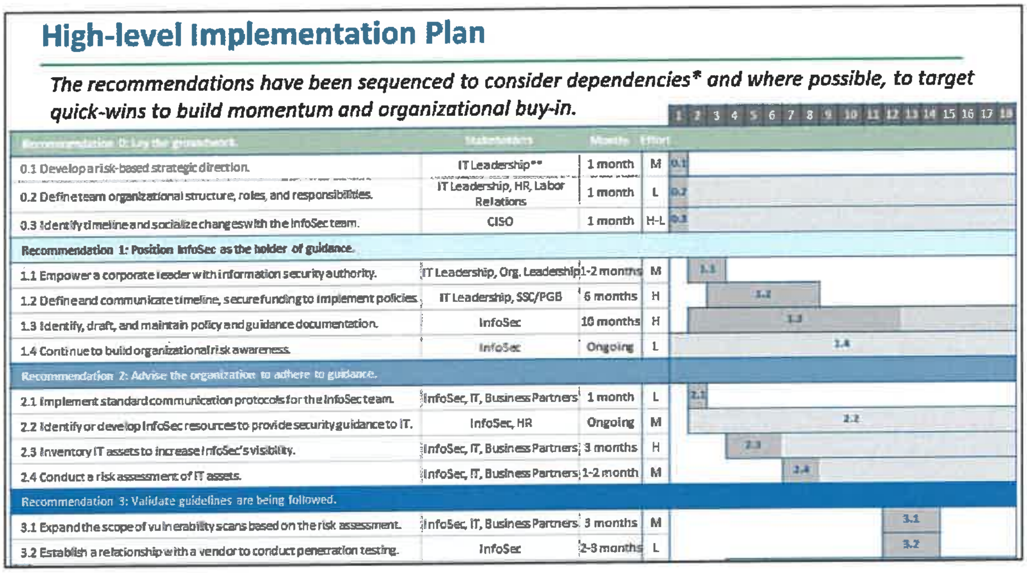
- **Data** - data attributes and entities, data for conversion, data archive, retention, and disposal, and dashboards and reports
- **Interfaces** - requirements for users, hardware, software, and communications, including communications interfaces with devices and other systems
- **Processes** - processes and sub-processes requirements, including process input and output, functional workflows, and sequencing of operations
- **Performance** - performance metrics associated with amount, speed, and other metrics that reflect system behavior under various conditions of operation; also, data validation and error handling, and data retention data capacity and growth capacity
- **Security and Privacy** – requirements for login, identity authentication and authorization, data create/read/update/delete (CRUD) authorizations, and protective and privacy controls
- **Human System Interaction** – graphical user interface (GUI), user skillsets, training, and other requirements pertaining to users' ability to effectively use the new solution, to include both functional administrators and technical administrators and other technical support personnel to operate and maintain it
- **Reliability** – system functioning requirements for operations without system degradation
- **Availability** – the time that the system will be available for operation
- **Maintainability** - the ability of the system to be maintained or restored to its previous condition after the performance of maintenance
- **General** - general system requirements that may not fit under the aforementioned areas or that may fit under more than one area.

The solicitation should also provide for prospective vendors' responses to address the following:

- Information technology (IT) infrastructure requirements to support optimal performance of the GRC tool, including compatible operating systems, application servers, database servers, cloud services, versions, sizing, and other relevant information
- Licensing options for the software, including enterprise licenses, user count-based licenses, and other licensing structures and license agreement terms and conditions
- Vendor technical support service levels available based on licensing agreement options
- Live demonstrations of the software under consideration by WVOT, based on a down-select process in connection with vendors' responses to the business requirements and other evaluation criteria, e.g., client references, price, financial stability/business position as a going concern.

Sample Deliverables

We have included select deliverables and templates as a sample of our past risk assessment and program development work.

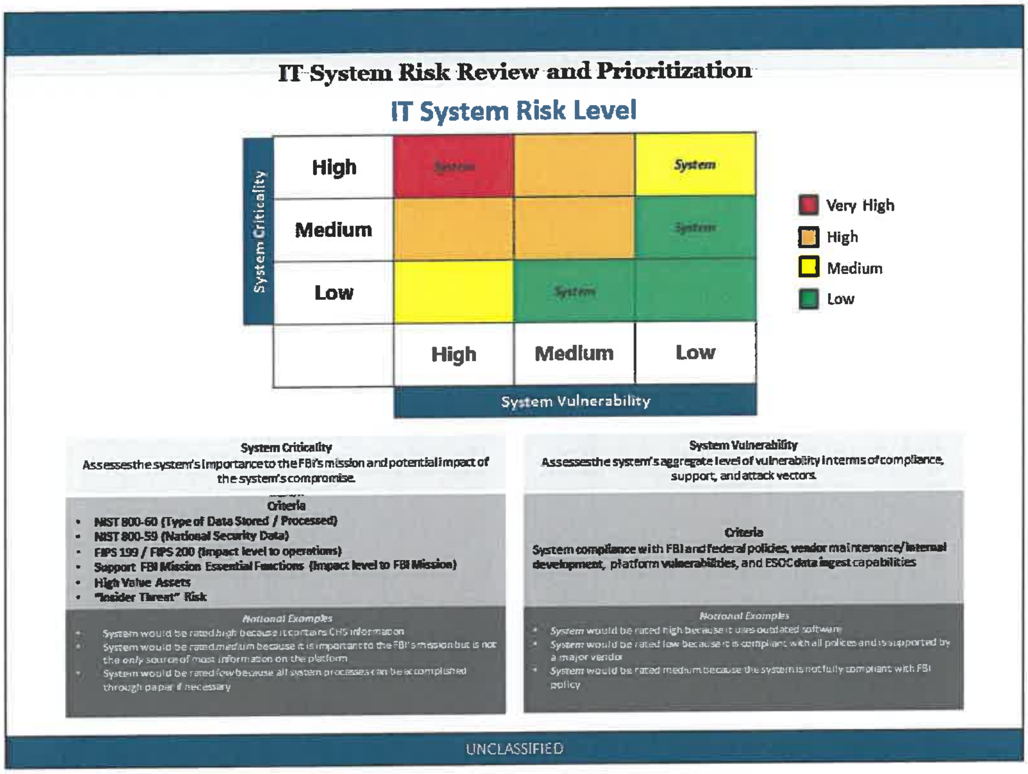


High-level Implementation Plan

The recommendations have been sequenced to consider dependencies and where possible, to target quick-wins to build momentum and organizational buy-in.*

Recommendation 0: Lay the groundwork.	Stakeholders	Months	Effort
0.1 Develop a risk-based strategic direction.	IT Leadership**	1 month	M
0.2 Define team organizational structure, roles, and responsibilities.	IT Leadership, HR, Labor Relations	1 month	L
0.3 Identify timeline and socialize changes with the InfoSec team.	CISO	1 month	H-L
Recommendation 1: Position InfoSec as the holder of guidance.			
1.1 Empower a corporate leader with information security authority.	IT Leadership, Org. Leadership	1-2 months	M
1.2 Define and communicate timeline, secure funding to implement policies.	IT Leadership, SSC/PGB	6 months	H
1.3 Identify, draft, and maintain policy and guidance documentation.	InfoSec	10 months	H
1.4 Continue to build organizational risk awareness.	InfoSec	Ongoing	L
Recommendation 2: Advise the organization to adhere to guidance.			
2.1 Implement standard communication protocols for the InfoSec team.	InfoSec, IT, Business Partners	1 month	L
2.2 Identify or develop InfoSec resources to provide security guidance to IT.	InfoSec, HR	Ongoing	M
2.3 Inventory IT assets to increase InfoSec's visibility.	InfoSec, IT, Business Partners	3 months	H
2.4 Conduct a risk assessment of IT assets.	InfoSec, IT, Business Partners	1-2 month	M
Recommendation 3: Validate guidelines are being followed.			
3.1 Expand the scope of vulnerability scans based on the risk assessment.	InfoSec, IT, Business Partners	3 months	M
3.2 Establish a relationship with a vendor to conduct penetration testing.	InfoSec	2-3 months	L

Sample Implementation Plan



IT System Risk Review and Prioritization

IT System Risk Level

System Criticality			
High	🟥 System	🟧	🟨 System
Medium	🟧	🟧	🟩 System
Low	🟨	🟩 System	🟩
	High	Medium	Low
	System Vulnerability		

🟥 Very High
🟧 High
🟨 Medium
🟩 Low

System Criticality
Assesses the system's importance to the FBI's mission and potential impact of the system's compromise.

Criteria

- NIST 800-60 (Type of Data Stored / Processed)
- NIST 800-59 (National Security Data)
- FIPS 199 / FIPS 200 (Impact level to operations)
- Support FBI Mission Essential Functions (Impact level to FBI Mission)
- High Value Assets
- "Insider Threat" Risk

Notional Examples

- System would be rated *high* because it contains CHS information
- System would be rated *medium* because it is important to the FBI's mission but is not the *only* source of most information on the platform
- System would be rated *low* because all system processes can be accomplished through paper if necessary

System Vulnerability
Assesses the system's aggregate level of vulnerability in terms of compliance, support, and attack vectors.

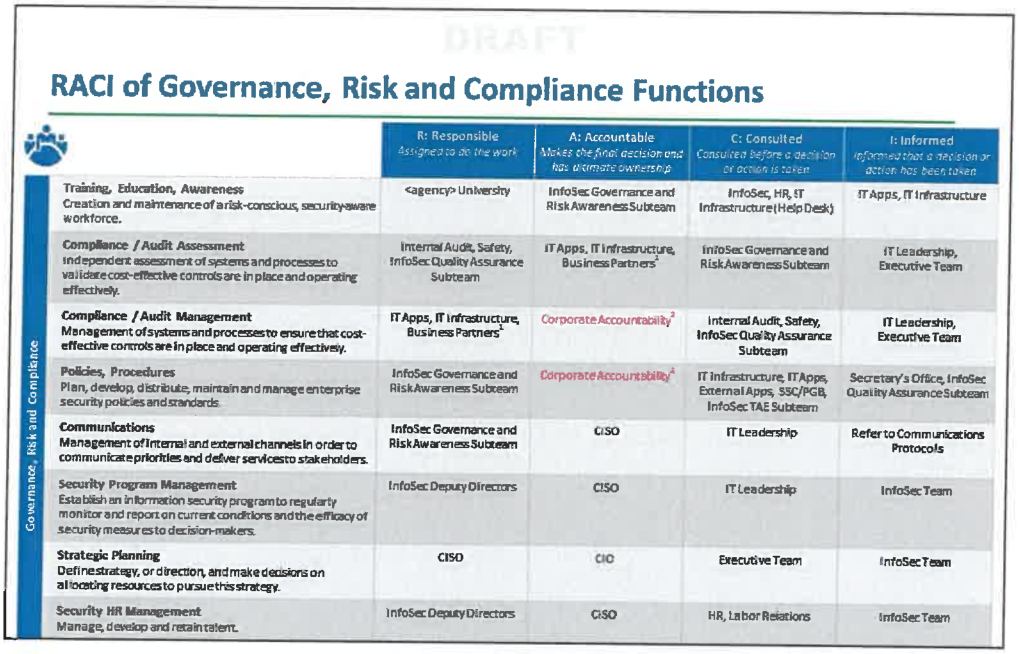
Criteria
System compliance with FBI and federal policies, vendor maintenance/internal development, platform vulnerabilities, and ESOC data ingest capabilities

Notional Examples

- *System* would be rated high because it uses outdated software
- *System* would be rated low because it is compliant with all polices and is supported by a major vendor
- *System* would be rated medium because the system is not fully compliant with FBI policy

UNCLASSIFIED

Sample Risk Prioritization Overview Presentation



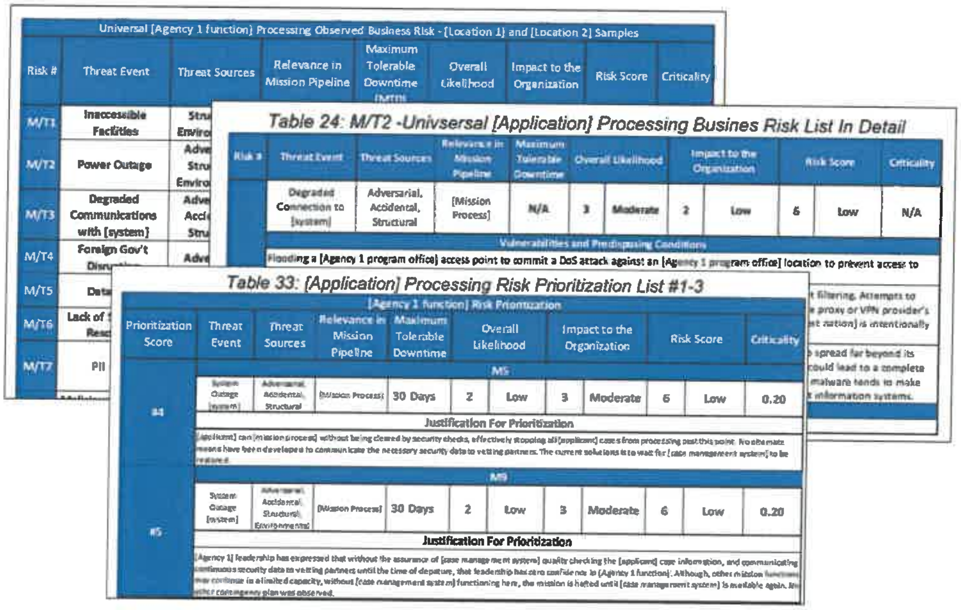
DRAFT

RACI of Governance, Risk and Compliance Functions

Governance, Risk and Compliance

	R: Responsible Assigned to do the work	A: Accountable Makes the final decision and has ultimate ownership	C: Consulted Consulted before a decision or action is taken	I: Informed Informed that a decision or action has been taken
Training, Education, Awareness Creation and maintenance of a risk-conscious, security-aware workforce.	<agency> University	InfoSec Governance and Risk Awareness Subteam	InfoSec, HR, IT Infrastructure (Help Desk)	IT Apps, IT Infrastructure
Compliance / Audit Assessment Independent assessment of systems and processes to validate cost-effective controls are in place and operating effectively.	Internal Audit, Safety, InfoSec Quality Assurance Subteam	IT Apps, IT Infrastructure, Business Partners[1]	InfoSec Governance and Risk Awareness Subteam	IT Leadership, Executive Team
Compliance / Audit Management Management of systems and processes to ensure that cost-effective controls are in place and operating effectively.	IT Apps, IT Infrastructure, Business Partners[1]	Corporate Accountability[2]	Internal Audit, Safety, InfoSec Quality Assurance Subteam	IT Leadership, Executive Team
Policies, Procedures Plan, develop, distribute, maintain and manage enterprise security policies and standards.	InfoSec Governance and Risk Awareness Subteam	Corporate Accountability[2]	IT Infrastructure, IT Apps, External Apps, SSC/PGB, InfoSec TAE Subteam	Secretary's Office, InfoSec Quality Assurance Subteam
Communications Management of internal and external channels in order to communicate priorities and deliver services to stakeholders.	InfoSec Governance and Risk Awareness Subteam	CISO	IT Leadership	Refer to Communications Protocols
Security Program Management Establish an information security program to regularly monitor and report on current conditions and the efficacy of security measures to decision-makers.	InfoSec Deputy Directors	CISO	IT Leadership	InfoSec Team
Strategic Planning Define strategy, or direction, and make decisions on allocating resources to pursue this strategy.	CISO	CIO	Executive Team	InfoSec Team
Security HR Management Manage, develop and retain talent.	InfoSec Deputy Directors	CISO	HR, Labor Relations	InfoSec Team

Stakeholder Analysis and Tasks



Universal [Agency 1 function] Processing Observed Business Risk - [Location 1] and [Location 2] Samples

Risk #	Threat Event	Threat Sources	Relevance in Mission Pipeline	Maximum Tolerable Downtime (MTD)	Overall Likelihood	Impact to the Organization	Risk Score	Criticality
M/T1	Inaccessible Facilities	Stru Enviro						
M/T2	Power Outage	Adve Stru Enviro						
M/T3	Degraded Communications with [system]	Adve Acci Stru						
M/T4	Foreign Gov't Disruption	Adve						
M/T5	Data							
M/T6	Lack of Reso							
M/T7	PII							

Table 24: M/T2 -Univsersal [Application] Processing Busines Risk List In Detail

Risk #	Threat Event	Threat Sources	Relevance in Mission Pipeline	Maximum Tolerable Downtime	Overall Likelihood		Impact to the Organization		Risk Score		Criticality
	Degraded Connection to [system]	Adversarial, Accidental, Structural	[Mission Process]	N/A	3	Moderate	2	Low	6	Low	N/A

Vulnerabilities and Predisposing Conditions

Flooding a [Agency 1 program office] access point to commit a DoS attack against an [Agency 1 program office] location to prevent access to

t filtering. Attempts to e proxy or VPN provider's st nation] is intentionally

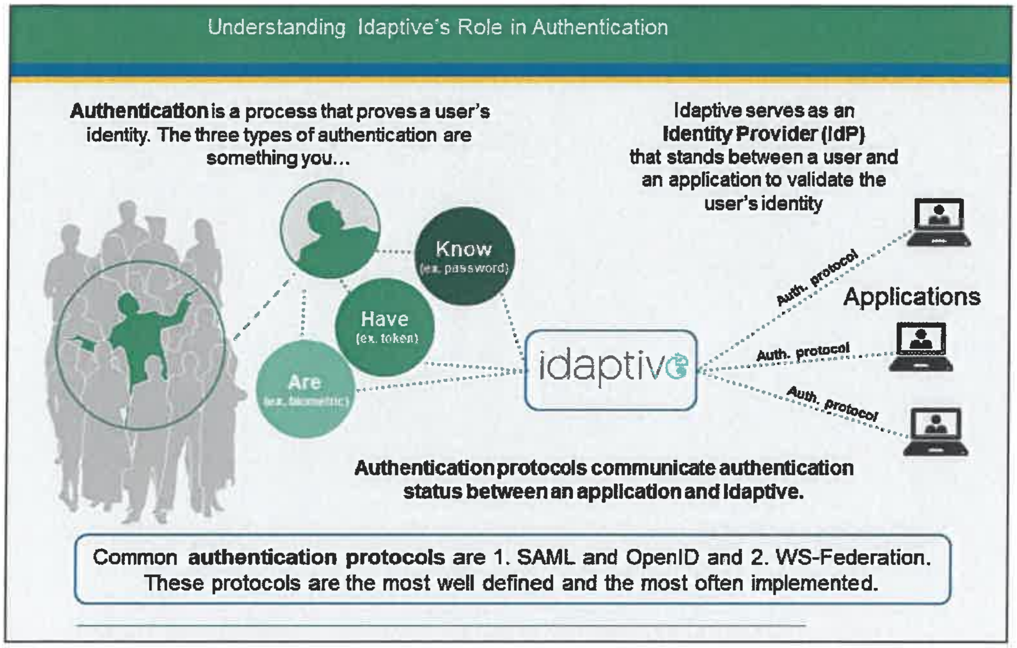
spread far beyond its could lead to a complete malware tends to make information systems.

Table 33: [Application] Processing Risk Prioritization List #1-3

[Agency 1 function] Risk Prioritization

Prioritization Score	Threat Event	Threat Sources	Relevance in Mission Pipeline	Maximum Tolerable Downtime	Overall Likelihood		Impact to the Organization		Risk Score		Criticality
	M5										
#4	System Outage [system]	Adversarial, Accidental, Structural	[Mission Process]	30 Days	2	Low	3	Moderate	6	Low	0.20
	Justification For Prioritization										
	[applicant] can [mission process] without being cleared by security checks, effectively stopping all [applicant] cases from processing past this point. No alternate means have been developed to communicate the necessary security data to vetting partners. The current solutions is to wait for [case management system] to be restored.										
	M9										
#5	System Outage [system]	Adversarial, Accidental, Structural, Environmental	[Mission Process]	30 Days	2	Low	3	Moderate	6	Low	0.20
	Justification For Prioritization										
	[Agency 1] leadership has expressed that without the assurance of [case management system] quality checking the [applicant] case information, and communicating continuous security data to vetting partners until the time of depature, that leadership has zero confidence in [Agency 1 function]. Although, other mission functions may continue in a limited capacity, without [case management system] functioning here, the mission is halted until [case management system] is available again. No other contingency plan was observed.										

Sample Tier 2 Risk Assessment Report



Understanding Idaptive's Role in Authentication

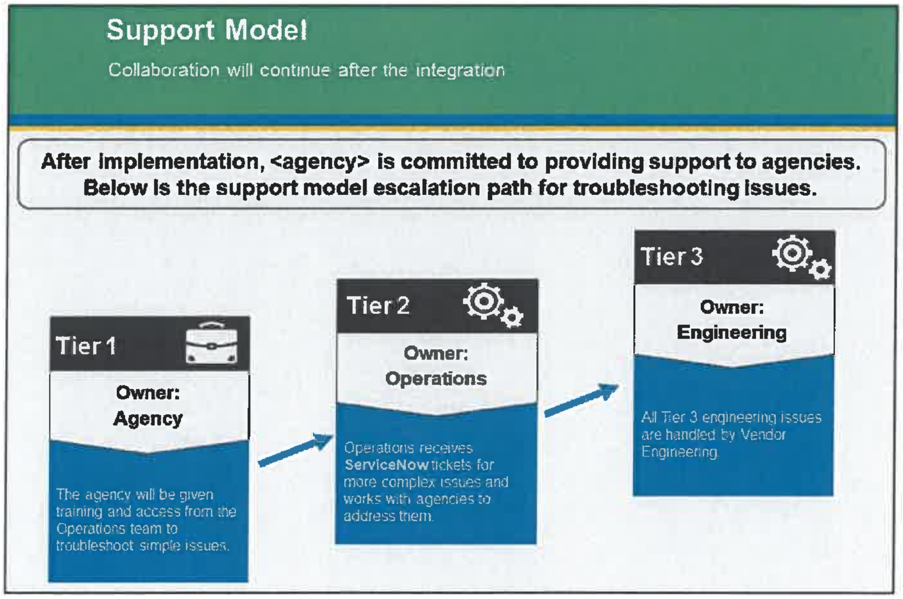
Authentication is a process that proves a user's identity. The three types of authentication are something you…

Idaptive serves as an **Identity Provider (IdP)** that stands between a user and an application to validate the user's identity

Authentication protocols communicate authentication status between an application and Idaptive.

Common **authentication protocols** are 1. SAML and OpenID and 2. WS-Federation. These protocols are the most well defined and the most often implemented.

Sample Training Presentation



Support Model

Collaboration will continue after the integration

After implementation, <agency> is committed to providing support to agencies. Below is the support model escalation path for troubleshooting issues.

Tier 1

Owner: Agency

The agency will be given training and access from the Operations team to troubleshoot simple issues.

Tier 2

Owner: Operations

Operations receives **ServiceNow** tickets for more complex issues and works with agencies to address them.

Tier 3

Owner: Engineering

All Tier 3 engineering issues are handled by Vendor Engineering.

Sample Support Model Communications Materials

Project team resumes

Name	Mr. Christopher O’Brien
Proposed Position	Engagement Partner
Degree/ Education/ Certifications	• MBA, JL Kellogg Graduate School, Northwestern University • BA, Political Science, Catholic University of America

Summary of Qualifications

Mr. O’Brien leads Guidehouse LLP’s State and Local Government Advisory Practice. Mr. O’Brien has more than 20 years of experience helping companies and governments embrace new technologies and improve performance. He has served dozens of US State and Local government clients as they seek to enhance service to constituents, reduce costs, increase efficiency and implement process improvements by enabling technology. Prior to joining Guidehouse, he served as the Chief Information Officer for the City of Chicago, where he oversaw several large scale technology programs, such as the City’s Enterprise Resource Planning (ERP), 311 customer service center and eCommerce platform implementations.

Relevant Experience

- **For the City of New York,** Mr. O’Brien led a project team through the completion of a Broadband Strategy to improve the digital infrastructure and capabilities of the City and its residents. The effort inventoried, at an address-by-address level, the broadband services available to citizens and businesses in an effort to determine whether market interventions were necessary to improve access. The study results indicated a significant problem with digital literacy among residents and recommended a significant program of investing in education and infrastructure for low-income New Yorkers. Guidehouse helped the City obtain more than $50 million in federal funding to implement the program, which has become a national model for broadband adoption programs.
- **For New York City's Metropolitan Transportation Authority**, Chris led an IT assessment of the applications, infrastructure and service delivery for this $11B organization. The fact base and inventory created led to an IT consolidation and application rationalization that will yield more than $20M in annual savings.
- **For the State of Minnesota**, Mr. O’Brien led the statewide IAM program, which began with an assessment of the Identity programs within each agency, an inventory of risks and issues and the development of a statewide program and strategy for IAM. The team then stood up an enterprise IAM program and currently assists the state on overseeing and operating this function.
- **For the City of Seattle,** Mr. O’Brien led an engagement to design and implement the City’s data center strategy that migrated the City from over 15 outdated Data Center facilities to 2 modern centers with world-class resiliency and redundancy. As part of this project, he led a team to collect and validate business requirements, develop future state scenarios for consideration, and implement key recommendations.

Name	**Ms. Nini Donovan**
Proposed Position	Engagement Director
Degree/Education	• MS, Engineering Management, Dartmouth College • BS, Engineering, Dartmouth College

Summary of Qualifications

Ms. Donovan is a Managing Director at Guidehouse LLP's State and Local Government Advisory Practice. She has more than 19 years of experience in technology and management consulting, stakeholder engagement, program management, and building of high-performing operations. Mrs. Donovan has worked extensively with a wide range of public and private sector organizations on complex business and IT transformation efforts. Her skills includes Stakeholder Engagement, Program Management, Cybersecurity, IT Strategy and Execution, and Business Process Improvement.

Relevant Experience

- **For the Massachusetts Executive Office of Technology Services & Security,** Mrs. Donovan is currently leading development of a statewide Identity & Access Management (IAM) program and implementation of their IAM solution. Ms. Donovan oversaw her team's effort to introduce a centralized identity and access management platform, on-board all critical and public facing applications into Single Sign On platform, integrate cloud and infrastructure servers into privileged access management component, introduce additional layer of security to all privileged users, implement alert & monitoring services and allow end users to reset their passwords to improve productivity.
- **For the State of Massachusetts's Department of Transportation**, Ms. Donovan led a cybersecurity and change management initiative to ensure that information security is an enterprise-wide priority for the organization. After conducting a needs assessment, Mrs. Donovan led the mapping of MassDOT staff's current interactions with information security and developed detailed recommendations for improvement. As part of this engagement, the team developed standard enterprise security policies, a five year roadmap and implementation plan, and a Security Awareness and Training Program that was successfully rolled out to 7,000+ MassDOT and MBTA information system users.
- **For the Commonwealth of Massachusetts Human Resources Division (HRD)**, Ms. Donovan lead the team in a shared services center evaluation to identify detailed recommendations to improve business processes and meet the needs of their customers across the state following a large HR consolidation. She oversaw a team of consultants who conducted a current state analysis across people, processes, and technology to determine appropriate staffing models, call routing processes, customer journey maps, performance management, and technology adoption. Ms. Donovan lead the team to produce detailed recommendations to address gaps identified in the current state, along with an actionable and detailed roadmap to reach the organization's target state.

Name	**Mr. Bruce Brody**
Proposed Position	Program Manager
Degree/Education	• MA, Information Security, Eastern Michigan University • BA, Mid-East and Military Studies, Franklin and Marshall College

Summary of Qualifications

Mr. Brody is a Director at Guidehouse LLP's Federal Advisory Practice and has over 25 years of information assurance and cybersecurity leadership and executive roles with the Department of Defense, Department of Veterans Affairs (VA), Department of Energy (DOE), and commercial private industry. Mr. Brody has implemented Department-wide and enterprise-wide cybersecurity programs at VA and DOE, as well as DRS Technologies and Cubic Corporation. He established and ran large ICAM programs such as the Authentication and Authorization Infrastructure Program (AAIP) at the VA, and the HSPD-12 Program at DOE. Certifications include Information Systems Security Professional (CISSP), Authorization Professional (CAP); Information Security Manager (CISM); FISMA Compliance Professional (CFCP), Advanced Program Management Professional, Level III

Relevant Experience

- **As a Director within the Cyber Security Solutions team at Guidehouse LLP,** Mr. Brody provides high-end mentoring, consulting, advice and transformation to enterprises in cybersecurity best practices, and provide mentoring to Chief Information Officers(CIOs) and Chief Information Security Officers (CISOs) on how best to implement a cybersecurity program across all of Governance, Risk and Compliance (GRC); risk strategy and risk management; incident management and response; information security; resilience; infrastructure protection; personnel security, authentication and authorization; and security architecture.
- **Mr. Brody has served as CISO for a Defense Industrial Base corporation,** while at the same time performing internal and external support for compliance programs such as Department of Defense Directive 8570.01, NIST controls, National Information Assurance Partnership (NIAP) Common Criteria certifications, technology evaluations and threat intelligence information sharing with partner companies and formal bodies.
- **As Vice President and Global CISO at DRS Technologies Inc.,** Mr. Brody drove continuing improvement in the protection and risk management of the company's information assets from the enterprise to the individual level. He also served as a trusted advisor and strategic partner to the company's C-level management and external oversight bodies. Mr. Brody monitored and assessed the overall compliance of DRS with information security policies, programs and procedures to meet regulatory requirements. Mr. Brody published and enforced the enterprise-wide policy framework and risk management guidelines, established and oversaw the governance process and ran the enterprise-wide information security compliance program. Mr. Brody also established and maintained an enterprise-wide vision, strategy, architecture and program that ensured implementation of the highest levels of information and cyber security.

Name	**Ms. Shannon Espersen**
Proposed Position	Cyber PMO Manager
Degree/ Education	• MBA, American University • BS, Business Management, Pennsylvania State University

Summary of Qualifications

Ms. Espersen is a Manager in Guidehouse LLP's State and Local Government Advisory Practice. She has over 18 year of experience working as a project manager, financial advisor and process improvement consultant managing or participating in various projects. Her experience includes project/portfolio management, system implementation, financial management, process improvement and international projects. She is a certified Project Management Professional.

Relevant Experience

- **For the State of Florida's Department of Transportation (FDOT),** Ms. Espersen is leading a team to implement an identity access and governance system (SailPoint Identity IQ) to automate and streamline processes. Ms. Espersen manages project deliverables, client and subcontractor relationships and leads the change management activities. SailPoint will automate lifecycle events such as: onboarding, transfers, access changes, name changes, and off-boarding, and provide attestation and recertification of user accesses based on risk, rule, or attribute settings. Implementation of this solution will provide FDOT with many core identity governance capabilities, but most primarily will allow personnel to focus on mission-critical tasks and save them time, money and resources.
- **For the Department of Defense (DoD),** Ms. Espersen was the Program Manager in support of the Task Force for Business and Stability Operations - Iraq (TFBSO) located in the International Zone in Baghdad, Iraq. She managed a team that created a process for and implemented the monitoring, control and closeout of investment projects initiated by TFBSO. She also worked with potential investors to help them start-up, research and analyze potential investment opportunities within Iraq. She supported the Iraqi National Investment Commission by supporting investment initiatives and growing capacity.
- **For the Federal Transit Administration,** Ms. Espersen was the Project Manager to update FTA's guidance to transit agencies how to report its financial data into the National Transit Database that complied with the Government Accounting Standards Board. The project also included performing cost-benefit analysis and determining cost allocation techniques.
- **For the Department of State,** Ms. Espersen was the Lead Budget Analyst, overseeing the financial reporting on over twenty (20) key, large-scale IT projects with an annual budget of ~$10M. She identified more efficient ways to report data and corrected errors from mismanaged systems.
- **For a government agency,** Ms. Espersen was the Project Manager to support the Audit Unit during the implementation of an Asset Management System, which included providing an internal control perspective, analyzing 'to-be' internal controls, test plans and results for the following areas: Transaction Processing, Reporting, Accounting Entries for Depreciation, Data Migration, Segregation of Duties and Access Controls.

Name	**Ms. Van Getchell**
Proposed Position	Cyber CM Analyst
Degree/Education	• MBA, University of Massachusetts Boston • BA, Communications and American Studies, Boston College

Summary of Qualifications

Van is a Senior Associate at Guidehouse LLP's State and Local Government Advisory Practice. She has over 8 years working as a project manager, business process analyst, and change management lead. She has significant experience working with public sector agencies including the Massachusetts Department of Transportation (MassDOT), Department of Education, Department of Labor, and Department of Transportation. She has led current state assessments identified gaps, reviewed cybersecurity risks, and developed recommendations for process improvements for her clients.

Relevant Experience

- **For the Massachusetts Executive Office of Technology Services & Security,** Ms. Getchell is currently the Business Analyst for the Identity and Access Management implementation. She is tasked with creating communications materials, gathering requirements for application integration, and interviewing stakeholders.
- **For the Massachusetts Department of Transportation (MassDOT)**, Ms. Getchell conducted a business applications analysis across the agency. She led a current state assessment of the agency's IT change management process, identifying gaps and developing recommendations for process improvements. She also analyzed MassDOT applications and systems and interviewed stakeholders to determine dependencies between applications and business processes. Her team's proposed solution, an application Guidebook for change implementation, enabled MassDOT to create better lines of communication and facilitate information sharing between various stakeholders and siloed departments.
- **For a Massachusetts private university**, Ms. Getchell served as a Business Process Analyst. In this role, she worked with six internal client departments comprised of over 70 employees to identify and understand business requirements and provide process improvement recommendations to ensure consistency and best practices across the department. Additionally, she led the integration of two new technologies and four applications for staff by creating business requirement specifications, writing and executing test plans, and collaborating with the Business Intelligence team to set a release schedule. Lastly, Ms. Getchell streamlined data management processes by identifying issues, proposing solutions, and securing an external vendor to build a functional and collaborative database.
- **For a continuing medical education company**, Ms. Getchell oversaw the accreditation and compliance department. She developed policies and procedures for live and online activity planning, grant support, development, marketing, delivery, and ensured compliance with industry standards.

Name	**Mr. Eric Berkowitz**
Proposed Position	ERM Lead
Degree/Education	• B.S., Finance, Virginia Tech

Summary of Qualifications

Mr. Berkowitz is a Director at Guidehouse LLP's Federal Advisory Practice currently supporting the FBI's Federal Bureau of Investigation's reorganization of their IT Security services under the FBI's OCIO. He is supporting the organization develop and document their strategy, new organizational design, and develop key service offerings for the FBI. Mr. Berkowitz also manages Guidehouse's support of the FBI's SAA Management program, ICAM deployment, and Business Process Improvement services for IT related programs. Certification includes Professional (CAP), (ISC)2, RiskVision, and Project Management Professional (PMP).

Relevant Experience

- **For the FBI EIACSS Task Order(TO) 18**, Mr. Berkowitz is responsible for driving FBI-wide programs for improved Risk Management for FBI Mission Essential Divisions and systems. He works directly with FBI CISO and CIO on designing the FBI's new IT Security Organization, to include the development and deployment of new services and resources to support the FBI's IT Security program. He leads a team tasked to develop the Continuous Monitoring Strategy and Continuous Monitoring Program Plan for FBI, deploy the strategy to System and IT Security Personnel within the Agency, and deploy a previously implemented Continuous Monitoring/Governance, Risk and Compliance (GRC) tool.
- **For the FBI Enterprise Technology Transformation Officer (ETTO)**, Mr. Berkowitz leads the integration of Office of Chief Information Officer (OCIO) and Cyber Security organization, to include cyber security service improvement and development, organizational design and redesign activities, performance of a workforce assessment, and resource and function allocation. He has assisted in the development and deployment of the Intelligence Agency's Identity, Credential, and Access Management (ICAM) program to include developing their ICAM strategy, compliance and governance model, communication plan, and schedule. Subsequently executing ICAM strategic deployment plan.
- **For the FBI IAPS Task Order(TO) 18,** Mr. Berkowitz led a team tasked to develop the Continuous Monitoring Strategy and Continuous Monitoring Program Plan for FBI, deploy the strategy to System and IT Security Personnel within the Agency, and deploy a previously implemented Continuous Monitoring/Governance, Risk and Compliance (GRC) tool.
- **For the FBI's FY08 A-123 Assessment**, Mr. Berkowitz collaborated with the FBI's FD and the Information Technology Operations Division (ITOD) on the FY09 A-123 IT Assessment. He documented and tested IT controls as they pertain to the financial process, including general computer controls, application access controls, and user security roles. He also created a matrix designed to identify weaknesses in FBI's IT internal control structure, identify control gaps in newly implemented IT systems and databases, and determine new ways for the team to assist in remediation of IT deficiencies as they relate to IT processes.

Name	**Mr. Hunter Richard**
Proposed Position	Business Process & Solicitation Lead
Degree/Education	• MBA, Harvard Business School • BA, Government, Harvard University

Summary of Qualifications

Mr. Richard is a Manager at Guidehouse LLP's State and Local Government Advisory Practice. He brings significant experience working with cities and state government agencies on strategies to increase economic development, introduce enabling technology, and manage change. He is an expert in BIA, project management, strategy development, and process and change management.

Relevant Experience

- **For the Massachusetts Department of Transportation (MassDOT),** Mr. Richard served as the project manager of the team conducting a business impact analysis of critical business and IT functions across the agency. He led over 60 stakeholder interviews with leaders across MassDOT from HR and Legal to Highway Operations and RMV Licensing to identify critical business processes and recovery needs in the event of a disaster. His team analyzed MassDOT applications and systems in light of business requirements to assess current recovery capabilities, determine key dependencies and criticalities, and enable MassDOT to prioritize disaster recovery resources.
- **For the Commonwealth of Massachusetts,** Mr. Richard led the development of a current state assessment, gap analysis, and strategy roadmap to improve a state agency's HR department identity and access management processes. Specifically, Mr. Richard analyzed business processes and requirements in the agency's employee lifecycle from recruitment and onboarding through to off-boarding. His work identified process changes to ensure data security is a priority and to introduce automation into manual IT and HR processes across several state secretariats.
- **For the Harvard Kennedy School Urban Field Lab**, Mr. Richard analyzed municipal business processes and delivered a policy proposal identifying strategies to reduce overcrowding and introduce social services into the city's Inspectional Services Department. Mr. Richard worked alongside a 6-person multi-disciplinary Harvard team to interview municipal workers, tenants, landlords, and social workers and present key findings to the City Manager of Chelsea. Contents of the policy proposal were included in the city's Bloomberg Mayor's Challenge grant proposal.
- **For the Commonwealth of Massachusetts**, Mr. Richard designed strategies and managed projects to attract businesses to the Massachusetts economy. Mr. Richard coordinated partnerships between foreign companies, state, federal, and quasi-agencies, industry associations, and senior corporate leaders, led overseas trade missions, and organized over 70 roundtables, seminars, and workshops for diplomats and the local business community.

Name	**Ms. Shelly Turner**
Proposed Position	GRC & Audit Lead
Degree/ Education	• B.S.B.A., Accounting, West Virginia University

Summary of Qualifications

Ms. Turner is a Director at Guidehouse LLP's Federal Advisory Practice and has over 15 years of experience in information technology (IT). Her experience includes large scale system implementation, IT security and audit readiness/remediation, as well as conducting audits. Her experience also includes implementations of governance, risk, and compliance (GRC) tools to automate IT security controls and processes. She has led projects for Federal agencies in the Department of Justice, Department of Homeland Security, and other civilian agencies and the Department of Defenses. Certifications include ScrumMaster (CSM), Internal Controls Auditor (CICA), Information Systems Auditor (CISA), Risk and Information Systems Control (CRISC), Oracle Advanced Controls Applications Certified Implementation Specialist, Defense Financial Management (CDFM)

Relevant Experience

- **For the Department of Homeland Security (DHS), Continuous Diagnostics and Mitigation (CDM),** Ms. Turner leads the GRC and training teams in connection with implementation of the DHS CDM initiative. This includes assessing agencies' as-is environments, measuring readiness for DHS CDM processes and technology, to include RSA's Archer GRC dashboard for monitoring hardware, software, configuration, and vulnerabilities, and recommending changes to encourage organizational adoption.
- **For the Department of Justice (DoJ), Federal Bureau of Investigation (FBI) Audit Unit Support,** Ms. Turner leads a team providing support to the Audit Unit in the areas of information security and controls for FBI's financial statement. Her team also is assisting the Audit Unit with in-sourcing its OMB A-123 assessment program. This includes delivering training on all activities for the A-123 assessment and supporting their execution of the assessment. Previously, Ms. Turner led two teams providing RiskVision GRC technology implementation services and information assurance support services. This includes advising FBI executives on leading practices and providing project oversight and management of team resources.
- **For the Defense Security Service (DSS)**, Financial Statement Audit Readiness Support, Oracle Security and Controls, Ms. Turner led a team for information security controls supporting the Agency's financial statement audit readiness program. She served as a Subject Matter Specialist to DSS in connection with its use of the Defense Agency Initiative (DAI) Oracle EBS financial system hosted by the Defense Logistics Agency (DLA). Ms. Turner advised on user access security, automated process controls and configurations, and interface controls with respect to DSS's A-123, SSAE 16, and FISCAM audit readiness project. Additionally, she served as an advisor to DSS on IT controls for non-Oracle systems and applications and on operational matters pertaining to the DAI Oracle financial system, Memoranda of Understanding (MOU) with DOD service provider Agencies, policies, and SOPs.

Name	**Mr. Shane Criqui**
Proposed Position	Analyst 1
Degree/ Education	• BS, Political Science, Kansas State University

Summary of Qualifications

Mr. Criqui a Senior Associate at Guidehouse LLP's Federal Advisory Practice with more than seven years working within the government, military, and commercial sectors. He has expertise in communications security, risk management, regulatory compliance, as well as cybersecurity culture, training, and awareness. Mr. Criqui was previously a Cyber Security Operator for the Air National Guard's 190th Air Refueling Wing, responsible for combat crew communications security enabling the KC-135 tanker critical domestic and war zone missions. Mr. Criqui managed and trained aircrew in the use of crypto systems, maintained regulatory compliance, and handled communications security. He is certified in Security+.

Relevant Experience

- **For the Department of State (DOS) Bureau of Information Risk Management (IRM),** Mr. Criqui currently serves as a cybersecurity risk analyst. He led and executed IRM's first Bureau-level Cyber Risk Assessment, established IRM's Information Risk Program's risk assessment capability and built the Information Risk Program's first risk assessment methodology for conducting risk assessments.
- **For the Department of Defense (DOD)**, United States Air Force (USAF) CISO program development, Mr. Criqui led the culture, training, and awareness team in revising the existing risk management framework (RMF) policies, communications, and training to provide for an enhanced and efficient RMF initiative. During the project, he optimized the RMF Next knowledge management through the creation of a RMF Knowledge Management Strategy, developed a RMF role-specific qualification matrix for evaluating candidates for risk management positions, and organized the testing of faux phishing, counter-social engineering/phishing reporting, and training tools to build requirements for new Air Force capabilities to maintain and surpass FISMA regulatory compliance.
- **For the Kansas Air National Guard,** Mr. Criqui served as a Cyber Security Operator filling the role of a Communications Security Responsible Officer (CRO), holding a Top Secret (SCI) clearance, managing hundreds of pieces of secret communications critical for Air Force aerial refueling missions. He has obtained extensive exposure and training in leadership and management through his experience in the Air Force in both real world and training environments. Mr. Criqui conducted military training exercises and real world operational missions routinely solving time sensitive problems by assessing the situation, defining the problem, developing alternatives, evaluating possible solutions, and selecting the best option in an expeditious manner.

Name	**Mr. Nong Nai**
Proposed Position	Analyst 2
Degree/ Education	• MBA, Georgetown University • MA, Johns Hopkins University • BA, George Mason University

Summary of Qualifications

Mr. Nai is a Manager at Guidehouse LLP with over with over 10 years of experience in strategy development and execution, cybersecurity program development and management, and data-driven program performance improvement and maturation. He has led teams to deliver strategic advisory, cybersecurity, and program management support to many of his clients. He has extensive experience delivering High Value Asset (HVA) programs to federal agencies.

Relevant Experience

- **For the Cybersecurity and Infrastructure Security Agency (CISA) *(formally Department of Homeland Security)* and Federal Network Resilience (FNR),** Mr. Nai delivered cybersecurity services to improve the Federal Civilian Government's cybersecurity posture. He managed the day-to-day operations of the High Value Asset (HVA) Program Management Office (PMO) alongside the client to ensure cybersecurity service efficiency and effectiveness of CAB's Security Architecture Review (SAR) and the National Cybersecurity Assessments and Technical Services' (NCATS) Risk and Vulnerability Assessment (RVA), resulting 170% and 30% increase in efficiency of the SAR and RVA service delivery respectively
- **For the Cybersecurity and Infrastructure Security Agency (CISA) *(formally Department of Homeland Security)* and Federal Network Resilience (FNR),** Mr. Nai planned and executed High Value Asset (HVA) strategy development effort, and drafted a five-year plan in collaboration with OMB and the National Institute of Standards and Technology (NIST) by leveraging the program operational lessons learned and insights to establish the baseline, identify gaps, and drive the establishment of HVA Program's vision, mission, goals, and objectives to mature the program to full operational capability
- **For a not-for-profit organization,** Mr. Nai led a team of four Multi-Disciplined Engineers with strategic support to US Cyber Command (USCYBERCOM) Chief Knowledge Officer (CKO) to develop Command-wide Knowledge Management (KM) Strategy to establish direction for the KM Program and its chartered KM Working Group. He also conducted impact assessments of DISA re-organization on its acquisition policies, processes, and workforce with respect to program oversight, management, and execution, and make cost-effective, executable recommendations to the Office of Component Acquisition Executive to address identified risks accordingly
- **For the Department of Defense,** Mr. Nai served as the contracting specialist. In this role, he managed a variety of large, sole-source and evaluated procurements for the Agency from the pre-solicitation phase through solicitation, evaluation, negotiation, award, and contract performance.

Name	**Ms. Margaret Mason**
Proposed Position	Analyst 3
Degree/Education	• BA, Economics and Government, University of Virginia

Summary of Qualifications

Ms. Mason is an Experienced Associate at Guidehouse LLP's State and Local Government Advisory Practice. She brings expertise in cybersecurity, change management, communications, stakeholder management, and organizational design. Her most recent engagements include performance management and communications for the NYC Mayor's Office, change management and training for MassDOT, and strategy and process improvement for MA HRD.

Relevant Experience

- **For the Massachusetts Department of Transportation**, Ms. Mason supported the implementation of a Security Awareness and Training Program that was successfully rolled out to 7,000+ MassDOT and MBTA information system users. She managed relationships across departments, produced individualized training assignments, drafted communications, and monitored compliance. In a previous engagement, Ms. Mason also assessed existing structures, processes and resources in the agency's information security structure. She performed a gap analysis between existing functionalities, business need and best practices. Her work also involved designing the new team structure, defining the functions and responsibilities of new roles, documenting tasks, identifying training needs for each role, and developing an onboarding deck.
- **For the Massachusetts Human Resources Division (HRD),** Ms. Mason assessed the current state of people, processes, and technology within the shared service center. She supported the team to identify recommendations, and develop a detailed implementation roadmap. Additionally, she designed a communications strategy to promote the call center's services and change management guide to assist HRD during the implementation phase.
- **For New York City's Mayor's Office of Operations**, Margaret supported an assessment of the Office's citywide performance management function with a specific focus on an annual performance report, the Mayor's Management Report (MMR). To develop the current state, Margaret conducted interviews with Operations, City Hall, and agency staff, reviewed existing documentation, conducted leading practices research, and designed and distributed a survey to collect feedback from 45 agencies across the city. In addition, Margaret worked with the team to develop a vision for the future of the MMR and Operations' role in city-wide performance management, identify detailed recommendations based on current state gaps and opportunities, and develop an implementation plan to achieve these goals.
- **For New York City's Department for the Aging,** Ms. Mason supported the organization as it looked to transition the Home Delivered Meals program to a new model. Ms. Mason helped to develop a comprehensive implementation plan including key steps, activities, and investments. To inform the plan, she conducted market research, surveyed peer cities to assess potential roadblocks, supported stakeholder workshops, and drafted a communications and marketing strategy.

Name	**Ms. Daniella Datskovska**
Proposed Position	Analyst 4
Degree/Education	• MBA, Finance and Marketing, Texas Christian University • BBA, International Business, Wartburg College

Summary of Qualifications

Ms. Datskovska is a Director at Guidehouse LLP's Federal Advisory Practice. She is a recognized Enterprise Risk Management practitioner with over eighteen years of commercial and government and public sector consulting experience in enterprise and operational risk management, communication, program and change management. Ms. Datskovska has served numerous public sector clients like the Department of Agriculture, Department of Justice, and Department of Homeland Security to develop and implement ERM strategies. She is a certified PMP, CISA, and CRMP.

Relevant Experience

- **For the Small Business Administration, the United States Department of Agriculture and its agencies**, Ms. Datskovska led ERM program design and implementation, including structuring and conducting risk assessments, facilitating the definition of agencies' risk appetite and tolerance in alignment with the organization's strategy and mission, assessing ERM program maturity to establish agencies' ERM, risk management and compliance processes current state level of effectiveness and efficiency, and identifying the desired future state and roadmap to achieve it.
- **For the Department of Justice, Department of Commerce/USPTO, Department of Homeland Security/ICE, Millennium Challenge Corporation and U.S. Export-Import Bank teams**, Ms. Datskovska led the development of an ERM framework, policy and operational ERM elements, including risk appetite, communication and stakeholder management plans and training. She worked to identify these clients' risk universe and risk profile – most critical strategic and operational risks; prioritizing the risk universe and developing strategic response plans, including external, political, operational, reputational, compliance, human capital and other pertinent risk categories.
- **For the Department of Energy,** Ms. Datskovska led the assessment of current state of compliance, risk management and internal control program. The goal of the assessment was to develop high-level business requirements for replacing the current suite of customized risk management and internal controls processes and tools to enhance risk management.
- **For the Office of Financial Policy and Operations at the General Services Administration (GSA),** Ms. Datskovska led an ERM assessment project to identify the future state vision for improved risk management within the organization. As a result of the project, the Office received a phased implementation roadmap for developing an integrated ERM program as well as the assessment of their key risks areas (entity-wide and program specific) with accompanying recommendations.

Name	**Ms. Zeshta Bhat**
Proposed Position	Analyst 5
Degree/ Education	• MS, Engineering Management, University of Southern California, Los Angeles • B.E., Information Science Engineering, Ramaiah Institute of Technology, India

Summary of Qualifications

Ms. Bhat is a Manager at Guidehouse LLP's State and Local Government Advisory Practice. Ms. Bhat is an experienced Cybersecurity professional specializing in development and standardization of processes across different security and IT domains such as Identity & Access Management (IAM), Application Security, Cloud Security, and Threat and Vulnerability Management. Ms. Bhat has worked with clients in public sector, retail, healthcare, and finance to provide cybersecurity strategy and technology implementation services. Most recently, she has provided project management for the Identity and Access Management implementation effort for the Commonwealth of Massachusetts.

Relevant Experience

- **For the Massachusetts Executive Office of Technology Services & Security,** Ms. Bhat is currently providing project management and technical support for the Identity and Access Management implementation for the State of Massachusetts, managing multiple workstreams, day-to-day project execution, and client interactions.
- **For the State of Massachusetts**, Ms. Bhat has successfully led the implementation of Privileged Access Management services for critical infrastructure resources and systems. The implementation included enabling multi-factor authentication on password checkouts for privileged accounts across multiple agencies and Active Directory domains. Ms. Bhat also implemented multi-factor authentication on login to authorize and manage access to critical on premise / Cloud servers and workspaces. As part of the project, Ms. Bhat has supported testing of multi-factor authentication and development of operations support model for O365 access.
- **For a mid-sized technology client**, Ms. Bhat designed governance model, target operating model, RACI, and stakeholder engagement methodology as part of their IAM program. Ms. Bhat also helped the client with IAM tool selection through detailed vendor analysis. To perform data cleanup in preparation for the implementation, she lead the analysis of user access data across client's several databases, Linux servers, and Active Directory to identify active accounts belonging to terminated users and to identify users with privileged access (e.g., sysadmin, root etc.).
- **For a large manufacturing client**, Ms. Bhat conducted a current state analysis of client's application development processes, identified gaps and pain points in the process from a security standpoint, and developed a target operating model to introduce mandatory security checks and touchpoints in client's application development lifecycle. She also developed an Excel based risk assessment tool to help application teams assess project risk and determine high level security requirements projects are subject to in the development lifecycle.

- **For a large consumer product client**, Ms. Bhat developed and standardized security standard operating processes covering areas such as vulnerability assessment and management, security logging / monitoring and integration with SIEM, and risk exception and acceptance.

Name	**Mr. Helgo Ohlenbusch**
Proposed Position	Subject Matter Specialist
Degree/Education	• MBA., MIT Sloan School of Business • MA, Computer Science, Worcester Polytechnic Institute • BA, Computer Science, University Louis Pasteur

Summary of Qualifications

Mr. Ohlenbusch is a Senior Information Security Solution Architect at Guidehouse LLP. He works with public sector clients providing cybersecurity strategy and technical implementation support. He has been involved in many Cloud migration projects and has significant experience in enterprise security working with various organizations including large multi-national software companies, industry-leading security firms, and start-up companies as a security solution architect and principle security architect. Certifications include CCSP, CISA, TOGAF, CISSP, and SCEA.

Relevant Experience

- **Mr. Ohlenbusch has supported two major Office 365 migration projects.** As an Office 365 architect in the healthcare sector, he helped migrate users to Office 365 including Azure Active Directory migration and mailboxes migration in a hybrid environment. He also developed the Security Architecture of the Office 365 migration in the retails sector. Additionally, Mr. Ohlenbusch was responsible for the Enterprise Security Architecture of a major migration to AWS and ensured the migration enhanced the company's security posture while reinforcing and adapting existing security policies.
- **Mr. Ohlenbusch, prepared, evaluated and presented security solutions, proof of concepts, architectures and recommendations to senior leaders for a multi-national technology firm.** He developed security architecture, vision and guiding principles at macro & micro level across all security initiatives including Identity Management, single sign on, federation, authentication, authorization, etc.
- **Mr. Ohlenbusch led and managed a technical team through an iterative development process from system concept, requirements and use cases analysis, architectural design, detail design to coding & debugging for a leading IT security organization.** He promoted and ensured the proper usage of best software engineering and specified, designed, implemented and deployed the Enterprise LDAP Directory, Central Profile Database and the close integration with other company systems.
- **Mr. Ohlenbusch is currently leading Identity & Access Management application integrations for multiple public sector agencies** including driving business and technical

requirements, defining architecture and design in complex environments, and leading implementation efforts.

- **For RSA**, Mr. Ohlenbusch was a senior technical architect responsible for implementation support of the security and identity and access management product suite including strong authentication, SingleSign-On, federation, auditing, data, file and database encryption, knowledge and risk based authentication, virtual and meta directory, data leakage solution, PKI infrastructure and compliance solutions.

Name	**Mr. John Hunt**
Proposed Position	Subject Matter Specialist
Degree/ Education	• MS, Computer Science, Johns Hopkins University • BS, Engineering, Math, and Computer Science, University of Louisville

Summary of Qualifications

Mr. Hunt is a Partner at Guidehouse LLP with over 20 years of assessing and helping mitigate cyber risks across commercial and public sector clients. He leads the Guidehouse Advanced Solutions Team which includes Cybersecurity, Advanced Analytics, Artificial Intelligence, Open Source Solutions, IT Strategy, and Digital and Emerging Technologies. As an expert in discussing cyber risk at the executive level, he has spent many years building IT Security consulting practices where he delivered IT security solutions to large Fortune 500 companies and a diverse network of Federal agencies to include DHS, DoJ, FBI, the IC, USDA, State Department, and several other Federal departments and agencies. He has worked a variety of projects designing and evaluating high assurance networking devices, implementing enterprise wide security solutions, assessing IT systems for vulnerabilities, evaluating IT controls to support financial and non-financial audits, and building compliance programs. Certifications include $(ISC)^2$ and Certified Information Systems Security Professional (CISSP).

Relevant Experience

- **For the Federal Bureau of Investigation**, Mr. Hunt provided leadership, planning, and support for a GRC implementation, policies and procedures design work, FISMA liaison support, and audit remediation support.
- **For the United States Corps of Engineers (USACE) and the Department of Health and Human Services,** Mr. Hunt performed IT security audits of predetermined data centers and systems to evaluate the protection of information technology (IT) assets (data, systems, and processes) in networked computing environments, with an emphasis on the effectiveness of logical access and systems software controls in support of the financial audit.
- **For the United States Government Agency,** Mr. Hunt supervised the IT Security tests in support of the General Controls portion of the financial audit for a large Government Agency. He reviewed and provided input into the General Controls sections of the Audit report and participated in the overall audit planning, and interfaced directly with the Inspector General (IG) and specific departments within the Agency on IT Security and

Name	Mr. John Hunt

General Controls testing and results. He also supervised the Federal Information Security Modernization Act (FISMA) Audit.

- **For the Social Security Administration,** Mr. Hunt has led numerous audits and reviews that have included diagnostic testing of Windows, and UNIX variations, and network devices, such as routers and firewalls. While supporting a SSA engagement; Mr. Hunt worked in a complex IT environment that encompassed 60 UNIX, 300 NT, 25 AS 400, 25 WANG servers, and 14 mainframe systems. His team tested eight Unix servers, six Windows servers, one database server, two firewalls, and one web server. The network penetration testing consisted of both internal and external penetration testing. SSA uses these systems to pay more than $400 billion in annual benefits to approximately 45 million beneficiaries across the country.

Name	Ms. Kate Sylvis
Proposed Position	Subject Matter Specialist
Degree/ Education	• BS, Accounting and Finance, University of Richmond

Summary of Qualifications

Ms. Sylvis is a Director at Guidehouse LLP's Federal Advisory Practice. She has 17 years of experience in providing governance, risk and controls, compliance, operational, and auditing services to public and private-sector clients, including the U.S. Treasury, government sponsored entities, investment banks and credit unions. She offers significant technical experience in areas such as governance, risk management, internal controls, compliance, operations, financial reporting, and investment accounting. She has provided advice and support to new program start-ups that cross organizational and operational design, governance, risk, compliance, and internal controls assessments under Sarbanes Oxley and OMB A-123 Appendix A. Certifications include Certified Public Accountant (CPA) and RIMS-CRMP-FED.

Relevant Experience

- **For the Centers for Medicare and Medicaid (CMS),** Ms. Sylvis led a team performing a cyber risk assessment from an ERM perspective with the objective of identifying how information relating to cybersecurity risk was utilized in decision-making. The project included the design of an assessment framework, facilitated interviews and risk assessment and reporting through to senior leadership.
- **For COSO ERM,** Integrating with Strategy and Performance, Ms. Sylvis was a member of the Principal Authorship Team responsible for the development of the 2017 COSO ERM – Integrating with Strategy and Performance Framework. She led a team to develop the Compendium of Examples to the Framework. Ms. Sylvis is a regular speaker at various forums and conferences on topics such as the changes to the Framework and how federal agencies can implement those changes.
- **For the Internal Revenue Service (IRS).** Ms. Sylvis has served as the Director providing advice and support to the IRS in the design and implementation of an ERM Program. She

<table>
<tr><th>Name</th><th>Ms. Kate Sylvis</th></tr>
<tr><td colspan="2">developed a Concept of Operations for the ERM Program based on the COSO ERM Framework, provided advice around the design and implementation; of roles and responsibilities for components of the operating model, processes around risk identification, assessment and mitigation. She supported the initial high level risk assessment, analysis of performance measures and key risk indicators (KRIs), development of KRI guidance to be used by business units for implementation, developed ERM training for: 25 program liaisons, 300 executives, manager general awareness, and topical podcasts (e.g., Basics of Risk Identification, Basics of Risk Assessment, Basics of Risk Response), and an enterprise wide risk identification reporting channel.
• <b>For the U.S. Department of Treasury,</b> Ms. Sylvis led a team at the Small Business Lending Fund (SBLF) in assisting with the development of a Concept of Operations for the Compliance Risk and Controls (CRC) function within the program office to document the governance structures and roles and responsibilities for CRC during the asset management and disposition activities in the transaction lifecycle. She assisted in standing up the compliance function as well as the development of an analytics process that allows SBLF to monitor the accuracy of participant submissions.</td></tr>
</table>

REQUEST FOR PROPOSAL
CRFP ISC2000000001
WVOT – Cyber Security Program

By signing below, I certify that I have reviewed this Request for Proposal in its entirety; understand the requirements, terms and conditions, and other information contained herein; that I am submitting this proposal for review and consideration; that I am authorized by the bidder to execute this bid or any documents related thereto on bidder's behalf; that I am authorized to bind the bidder in a contractual relationship; and that, to the best of my knowledge, the bidder has properly registered with any State agency that may require registration.

Guidehouse LLP
(Company)

Chris O'Brien , Partner
(Representative Name, Title)

(773) 909-4360
(Contact Phone/Fax Number)

8/27/2019
(Date)

West Virginia Ethics Commission

Disclosure of Interested Parties to Contracts

Pursuant to *W. Va. Code* § 6D-1-2, a state agency may not enter into a contract, or a series of related contracts, that has/have an actual or estimated value of $1 million or more until the business entity submits to the contracting state agency a Disclosure of Interested Parties to the applicable contract. In addition, the business entity awarded a contract is obligated to submit a supplemental Disclosure of Interested Parties reflecting any new or differing interested parties to the contract within 30 days following the completion or termination of the applicable contract.

For purposes of complying with these requirements, the following definitions apply:

"Business entity" means any entity recognized by law through which business is conducted, including a sole proprietorship, partnership or corporation, but does not include publicly traded companies listed on a national or international stock exchange.

"Interested party" or *"Interested parties"* means:

(1) A business entity performing work or service pursuant to, or in furtherance of, the applicable contract, including specifically sub-contractors;
(2) the person(s) who have an ownership interest equal to or greater than 25% in the business entity performing work or service pursuant to, or in furtherance of, the applicable contract. (This subdivision does not apply to a publicly traded company); and
(3) the person or business entity, if any, that served as a compensated broker or intermediary to actively facilitate the applicable contract or negotiated the terms of the applicable contract with the state agency. (This subdivision does not apply to persons or business entities performing legal services related to the negotiation or drafting of the applicable contract.)

"State agency" means a board, commission, office, department or other agency in the executive, judicial or legislative branch of state government, including publicly funded institutions of higher education: Provided, that for purposes of W. Va. Code § 6D-1-2, the West Virginia Investment Management Board shall not be deemed a state agency nor subject to the requirements of that provision.

The contracting business entity must complete this form and submit it to the contracting state agency prior to contract award and to complete another form within 30 days of contract completion or termination.

This form was created by the State of West Virginia Ethics Commission, 210 Brooks Street, Suite 300, Charleston, WV 25301-1804. Telephone: (304)558-0664; fax: (304)558-2169; e-mail: ethics@wv.gov; website: www.ethics.wv.gov

STATE OF WEST VIRGINIA
Purchasing Division

PURCHASING AFFIDAVIT

CONSTRUCTION CONTRACTS: Under W. Va. Code § 5-22-1(i), the contracting public entity shall not award a construction contract to any bidder that is known to be in default on any monetary obligation owed to the state or a political subdivision of the state, including, but not limited to, obligations related to payroll taxes, property taxes, sales and use taxes, fire service fees, or other fines or fees.

ALL CONTRACTS: Under W. Va. Code §5A-3-10a, no contract or renewal of any contract may be awarded by the state or any of its political subdivisions to any vendor or prospective vendor when the vendor or prospective vendor or a related party to the vendor or prospective vendor is a debtor and: (1) the debt owed is an amount greater than one thousand dollars in the aggregate; or (2) the debtor is in employer default.

EXCEPTION: The prohibition listed above does not apply where a vendor has contested any tax administered pursuant to chapter eleven of the W. Va. Code, workers' compensation premium, permit fee or environmental fee or assessment and the matter has not become final or where the vendor has entered into a payment plan or agreement and the vendor is not in default of any of the provisions of such plan or agreement.

DEFINITIONS:

"Debt" means any assessment, premium, penalty, fine, tax or other amount of money owed to the state or any of its political subdivisions because of a judgment, fine, permit violation, license assessment, defaulted workers' compensation premium, penalty or other assessment presently delinquent or due and required to be paid to the state or any of its political subdivisions, including any interest or additional penalties accrued thereon.

"Employer default" means having an outstanding balance or liability to the old fund or to the uninsured employers' fund or being in policy default, as defined in W. Va. Code § 23-2c-2, failure to maintain mandatory workers' compensation coverage, or failure to fully meet its obligations as a workers' compensation self-insured employer. An employer is not in employer default if it has entered into a repayment agreement with the Insurance Commissioner and remains in compliance with the obligations under the repayment agreement.

"Related party" means a party, whether an individual, corporation, partnership, association, limited liability company or any other form or business association or other entity whatsoever, related to any vendor by blood, marriage, ownership or contract through which the party has a relationship of ownership or other interest with the vendor so that the party will actually or by effect receive or control a portion of the benefit, profit or other consideration from performance of a vendor contract with the party receiving an amount that meets or exceed five percent of the total contract amount.

AFFIRMATION: By signing this form, the vendor's authorized signer affirms and acknowledges under penalty of law for false swearing (*W. Va. Code* §61-5-3) that: (1) for construction contracts, the vendor is not in default on any monetary obligation owed to the state or a political subdivision of the state, and (2) for all other contracts, that neither vendor nor any related party owe a debt as defined above and that neither vendor nor any related party are in employer default as defined above, unless the debt or employer default is permitted under the exception above.

WITNESS THE FOLLOWING SIGNATURE:

Vendor's Name: Guidehouse LLP

Authorized Signature: ______________________ Date: 8/22/19

State of Washington

County of District of Columbia, to-wit:

Taken, subscribed, and sworn to before me this 22 day of August, 20___.

My Commission expires 11/14/23, 20___.

AFFIX SEAL HERE

KAIKEE H. ROBINSON
NOTARY PUBLIC
MY COMMISSION EXPIRES 11/14/2023
DISTRICT OF COLUMBIA

NOTARY PUBLIC ______________________

West Virginia Ethics Commission

Disclosure of Interested Parties to Contracts

(Required by *W. Va. Code* § 6D-1-2)

Name of Contracting Business Entity: Guidehouse LLP **Address:** 1800 Tysons Blvd, 7th Floor
McLean, VA, 22102

Name of Authorized Agent: ______________ **Address:** ______________

Contract Number: CRFPISC2000000001 **Contract Description:** Cyber Security Program

Governmental agency awarding contract: State of West Virginia, Department of Administration, Purchasing Division

□ **Check here if this is a Supplemental Disclosure**

List the Names of Interested Parties to the contract which are known or reasonably anticipated by the contracting business entity for each category below *(attach additional pages if necessary)*:

1. **Subcontractors or other entities performing work or service under the Contract**
   □ Check here if none, otherwise list entity/individual names below.

2. **Any person or entity who owns 25% or more of contracting entity (not applicable to publicly traded entities)**
   ☒ Check here if none, otherwise list entity/individual names below.

   Guidehouse Holding Corporation, parent (99%), 1800 Tysons Blvd, 7th Floor, McLean, VA 22102

3. **Any person or entity that facilitated, or negotiated the terms of, the applicable contract (excluding legal services related to the negotiation or drafting of the applicable contract)**
   □ Check here if none, otherwise list entity/individual names below.

Signature: ______________ Date Signed: 8/22/2019

Notary Verification

State of Washington, , County of District of Columbia :

I, Kanekee M. Robinson, the authorized agent of the contracting business entity listed above, being duly sworn, acknowledge that the Disclosure herein is being made under oath and under the penalty of perjury.

Taken, sworn to and subscribed before me this 22 day of August, 2019

Kanekee M.
Notary Public's Signature

To be completed by State Agency:
Date Received by State Agency: ______________
Date submitted to Ethics Commission: ______________
Governmental agency submitting Disclosure: ______________

KANEKEE M. ROBINSON
NOTARY PUBLIC
DISTRICT OF COLUMBIA
MY COMMISSION EXPIRES 11/14/2023

Guidehouse LLP respectfully requests the State modify the following provision to align with our contracting policies.

28. WARRANTY: The Vendor expressly warrants that the goods and/or services covered by this Contract will: (a) substantially conform to the specifications, drawings, samples, or other description furnished or specified by the Agency; (b) be merchantable and fit for the purpose intended; and (c) be free from defect in material and workmanship for 365 days following acceptance of the goods or services by the State.

Guidehouse LLP respectfully requests the State modify the following provision to align with our contracting policies.

36. INDEMNIFICATION AND LIMITATION OF LIABILITY: The Vendor agrees to indemnify, defend, and hold harmless the State and the Agency, their officers, and employees form and against: (1) Any claims or losses for services by any subcontractor, person, or firm performing or supplying services, materials, or supplies in connection with the performance of this Contract; (2) ~~any claims or losses resulting to any person or entity injured or damaged by the Vendor, its officers, employees, or subcontractor by the publication, translation, reproduction, delivery, performance, use, or disposition of any data used under the Contract in a manner not authorized by the Contract, or by Federal or State statutes or regulations~~ death or bodily injury; or (3) damage to real or tangible property ~~any failure of the Vendor, its officers, employees, or subcontractors to observe State and Federal laws including, but not limited to, labor and wage and hour laws.~~

Except to the extent finally determined to be prohibited by law, Vendor's aggregate liability for all claims, losses, liabilities, or damages in connection with this agreement or its subject matter, whether as a result of breach of contract, tort (including negligence), or otherwise, regardless of the theory of liability asserted, is limited to no more than the total amount of fees paid to Vendor for the particular Service giving rise to the liability under this agreement. In addition, Vendor will not be liable for any lost profits, consequential, indirect, punitive, exemplary, or special damages. Also, Vendor shall have no liability arising from or relating to any third-party hardware, software, information, or materials selected or supplied by the State.

Guidehouse

Submission of this proposal is not an indication of Guidehouse LLP's willingness to be bound by all of the terms presented in the State of West Virginia's (the "State") Request for Proposal for WVOT Cyber Security Program (the "RFP"). This proposal in response to the State's RFP does not constitute a contract to perform services and cannot be used to award a unilateral agreement. Final acceptance of this engagement by Guidehouse is contingent upon successful completion of Guidehouse's acceptance procedures. Any engagement arising out of this proposal will be subject to negotiation of a mutually satisfactory vendor contract including modifications to certain RFP terms and conditions (including, without limitation, the RFP's Section 3 General Terms and Conditions) and including our standard terms and conditions and fees and billing rates established therein.

Given our past history of successfully negotiating mutually agreeable terms with similar public sector agencies, we do not anticipate any difficulty in reaching a contractual agreement that will enable us to provide the professional services which you are requesting, while protecting the interests of both parties.

Guidehouse LLP respectfully requests the State delete the following provision to align with our contracting policies:

~~**11. LIQUDATED DAMAGES:** This clause shall in no way be considered exclusive and shall not limit the State or Angecy's right to pursue any other available remedy. Vendor shall pay liquidated damages in the amount specified below or as described in the specifications:~~

- ~~______________ for __________________.~~
- ~~Liquidated Damages Contained in the Specifications.~~

Guidehouse LLP respectfully requests the State modify the following provision to align with our contracting policies.

13. PRICING: The pricing set forth herein is firm for the life of the Contract, unless specified elsewhere within this Solicitation/Contract by the State. A Vendor's inclusion of price adjustment provisions in its bid, without the express authorization from the State in the Solicitation to do so, may result in bid disqualification. ~~Notwithstanding the foregoing, Vendor must extend any publicly advertised sale price to the State and invoice at the lower of the contract price or the publicly advertised sale price.~~

Guidehouse LLP respectfully requests the State modify the following provision to align with our contracting policies.

19. CANCELLATION: The Purchasing Division Director reserves the right to cancel this Contract immediately upon written notice to the vendor if the materials or workmanship supplied do not substantially conform to the specification contained in the Contract , provided, however, the State allows the Vendor the opportunity to cure any failure in a timely manner. The Purchasing Division Director may also canel any purchase or Contract upon 30 days written notice to the Vendor in accordance with West Viriginia Code of State Rules § 148-1-5.2b.

Guidehouse LLP respectfully requests the State delete the following provision to align with our contracting policies.

~~**20. TIME:** Time is of the essence with regard to all matters of time and performance in this contract.~~

ADDENDUM ACKNOWLEDGEMENT FORM

SOLICITATION NO.: 15C2000000001

Instructions: Please acknowledge receipt of all addenda issued with this solicitation by completing this addendum acknowledgment form. Check the box next to each addendum received and sign below. Failure to acknowledge addenda may result in bid disqualification.

Acknowledgment: I hereby acknowledge receipt of the following addenda and have made the necessary revisions to my proposal, plans and/or specification, etc.

Addendum Numbers Received:
(Check the box next to each addendum received)

☒ Addendum No. 1
☒ Addendum No. 2
□ Addendum No. 3
□ Addendum No. 4
□ Addendum No. 5
□ Addendum No. 6
□ Addendum No. 7
□ Addendum No. 8
□ Addendum No. 9
□ Addendum No. 10

I understand that failure to confirm the receipt of addenda may be cause for rejection of this bid. I further understand that any verbal representation made or assumed to be made during any oral discussion held between Vendor's representatives and any state personnel is not binding. Only the information issued in writing and added to the specifications by an official addendum is binding.

Guidehouse LLP
Company

Chris O'Brien
Authorized Signature

8/27/2019
Date

NOTE: This addendum acknowledgement should be submitted with the bid to expedite document processing.

Revised 6/8/2012