

**PROPOSAL TO PROVIDE CYBERSECURITY PROGRAM SERVICES FOR:
West Virginia Office of Technology**



**CRFP ISC200000001
WVOT – Cyber Security Program**

**Dixon Hughes Goodman LLP
500 Virginia Street, Suite 800
Charleston WV 25301
T 304.343.0168 | F 304.343.1895**

**4350 Congress Street, Suite 900
Charlotte NC 28209
T 704.367.7020 | F 704.367.7760**

Tom Tollerton | Managing Director | tom.tollerton@dhg.com

A handwritten signature in black ink, appearing to read "Tom Tollerton".

August 27, 2019

Signed

Date

RECEIVED

2019 AUG 29 AM 9:19

WV PURCHASING
DIVISION

TECHNICAL PROPOSAL

table of contents

4.2.1 goals and objectives.....	1
4.2.2. Mandatory Requirements.....	11
4.3.1 qualifications and experience.....	12
4.3.2. Mandatory qualifications and experience.....	21

ADDENDUM ACKNOWLEDGEMENT FORM
SOLICITATION NO.: _____

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)

- | | |
|--|--|
| <input checked="" type="checkbox"/> Addendum No. 1 | <input type="checkbox"/> Addendum No. 6 |
| <input checked="" type="checkbox"/> Addendum No. 2 | <input type="checkbox"/> Addendum No. 7 |
| <input type="checkbox"/> Addendum No. 3 | <input type="checkbox"/> Addendum No. 8 |
| <input type="checkbox"/> Addendum No. 4 | <input type="checkbox"/> Addendum No. 9 |
| <input type="checkbox"/> Addendum No. 5 | <input type="checkbox"/> 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.

RECEIVED

2019 AUG 27 AM 9:36

WV PURCHASING
DIVISION

Dixon Hughes Goodman LLP
Company

Authorized Signature

9/26/2019

Date

NOTE: This addendum acknowledgment should be submitted with the bid to expedite document processing.
Revised 6/8/2012



Purchasing Division
 2019 Washington Street East
 Post Office Box 50130
 Charleston, WV 25305-0130

State of West Virginia
 Request for Proposal
 10 - Consulting

Proc Folder: 609025

Doc Description: Cyber Security Program RFP (OT19152)

Proc Type: Central Master Agreement

Date Issued	Solicitation Closes	Solicitation No	Version
2019-07-26	2019-08-29 13:30:00	CRFP 0210 ISC2000000001	1

BID RECEIVING LOCATION

BID CLERK
 DEPARTMENT OF ADMINISTRATION
 PURCHASING DIVISION
 2019 WASHINGTON ST E
 CHARLESTON WV 25305
 US

VENDOR

Vendor Name, Address and Telephone Number:

Dixon Hughes Goodman LLP
 500 Virginia Street, Suite 800
 Charleston WV 25301
 304.343.0168

FOR INFORMATION CONTACT THE BUYER

Jessica S Chambers
 (304) 558-0246
 jessica.s.chambers@wv.gov

Signature X

FEIN # 56-0747981

DATE

8/26/19

All offers subject to all terms and conditions contained in this solicitation



Purchasing Division
 2019 Washington Street East
 Post Office Box 50130
 Charleston, WV 25305-0130

State of West Virginia
 Request for Proposal
 10 – Consulting

Proc Folder: 609025

Doc Description: Addendum 1-Cyber Security Program RFP (OT19152)

Proc Type: Central Master Agreement

Date Issued	Solicitation Closes	Solicitation No	Version
2019-07-30	2019-08-29 13:30:00	CRFP 0210 ISC2000000001	2

BID RECEIVING LOCATION

BID CLERK
 DEPARTMENT OF ADMINISTRATION
 PURCHASING DIVISION
 2019 WASHINGTON ST E
 CHARLESTON WV 25305
 US

VENDOR

Vendor Name, Address and Telephone Number:

Dixon Hughes Goodman LLP
 500 Virginia Street, Suite 800
 Charleston WV 25301
 304.343.0168

FOR INFORMATION CONTACT THE BUYER

Jessica S Chambers
 (304) 558-0246
 jessica.s.chambers@wv.gov

Signature X

FEIN # 56-0747981

DATE

8/26/2019

All offers subject to all terms and conditions contained in this solicitation



Purchasing Division
 2019 Washington Street East
 Post Office Box 50130
 Charleston, WV 25305-0130

State of West Virginia
 Request for Proposal
 10 - Consulting

Proc Folder: 609025

Doc Description: Addendum 2-Cyber Security Program RFP (OT19152)

Proc Type: Central Master Agreement

Date Issued	Solicitation Closes	Solicitation No	Version
2019-08-21	2019-08-29 13:30:00	CRFP 0210 ISC2000000001	3

BID RECEIVING LOCATION

BID CLERK
 DEPARTMENT OF ADMINISTRATION
 PURCHASING DIVISION
 2019 WASHINGTON ST E
 CHARLESTON WV 25305
 US

VENDOR

Vendor Name, Address and Telephone Number:

Dixon Hughes Goodman LLP
 500 Virginia Street, Suite 800
 Charleston WV 25301
 304.343.0168

FOR INFORMATION CONTACT THE BUYER

Jessica S Chambers
 (304) 558-0246
 jessica.s.chambers@wv.gov

Signature X

FEIN # 56-0747981

DATE

8/26/19

All offers subject to all terms and conditions contained in this solicitation

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 exceeds 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: Dixon Hughes Goodman LLP

Authorized Signature: [Signature] Date: 8/26/19

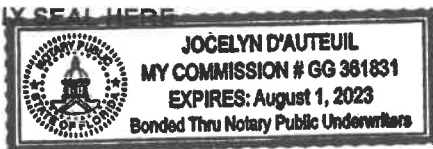
State of Florida

County of Orange, to-wit:

Taken, subscribed, and sworn to before me this 26 day of August, 2019

My Commission expires August 1, 2023

AFFIX SEAL HERE

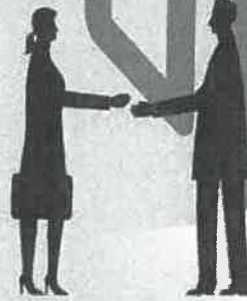


NOTARY PUBLIC

[Signature]
Purchasing Affidavit (Revised 01/19/2018)

DHG | IT advisory

PROPOSAL TO PROVIDE CYBERSECURITY SERVICES FOR:
West Virginia Office of Technology



CRFP ISC2000000001
WVOT – Cyber Security Program

Dixon Hughes Goodman LLP
500 Virginia Street, Suite 800
Charleston WV 25301
T 304.343.0168 | F 304.343.1895

4350 Congress Street, Suite 900
Charlotte NC 28209
T 704.367.7020 | F 704.367.7760

Tom Tollerton | Managing Director | tom.tollerton@dhg.com

Signed

Date

A handwritten signature in black ink, appearing to read "Tom Tollerton", written over a horizontal line.

8/26/2019

ORIGINAL SIGNATORY FORMS

West Virginia Ethics Commission
Disclosure of Interested Parties to Contracts

(Required by W. Va. Code § 6D-1-2)

Dixon Hughes Goodman

Name of Contracting Business Entity LLP Address: 500 Virginia Street, Suite 800; Charleston WV 25301

Name of Authorized Agent: Tom Tollerton Address: 4350 Congress Street, Suite 900, CLT NC

Contract Number: TBD Contract Description: _____

Governmental agency awarding contract: WV Office of Technology

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.

Soteria LLC
Charleston SC

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.

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: 8/26/2019

Notary Verification

State of Florida, County of Orange:

I, Thomas Burleigh Tollerton, 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 26 day of August, 2019

Notary Public's Signature

To be completed by State Agency:

Date Received by State Agency: _____

Date submitted to Ethics Commission: _____

Governmental agency submitting Disclosure: _____



REQUEST FOR PROPOSAL
CRFP ISC2000000001
WVOT – Cyber Security Program

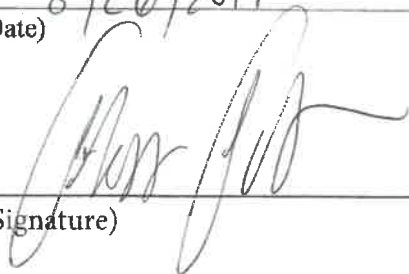
By signing below, I certify that I have reviewed this Request for Proposal in its entirety; understand the requirements, terms and conditions, and other information contained herein; that I am submitting this proposal for review and consideration; that I am authorized by the bidder to execute this bid 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.

Dixon Hughes Goodman LLP
(Company)

Tom Tollerton, Managing Director
(Representative Name, Title)

704-367-7020 / 704-367-7760
(Contact Phone/Fax Number)

8/26/2017
(Date)



(Signature)

DESIGNATED CONTACT: Vendor appoints the individual identified in this Section as the Contract Administrator and the initial point of contact for matters relating to this Contract.

Tom Tollerton, Managing Director
(Name, Title)
Tom Tollerton, Managing Director
(Printed Name and Title)
4350 Congress Street, Suite 900, Charlotte NC 28209
(Address)
704-367-7020 704-367-7760
(Phone Number) / (Fax Number)
Tom.Tollerton@dhg.com
(email address)

CERTIFICATION AND SIGNATURE: By signing below, or submitting documentation through wvOASIS, I certify that I have reviewed this Solicitation in its entirety; that I understand the requirements, terms and conditions, and other information contained herein; that this bid, offer or proposal constitutes an offer to the State that cannot be unilaterally withdrawn; that the product or service proposed meets the mandatory requirements contained in the Solicitation for that product or service, unless otherwise stated herein; that the Vendor accepts the terms and conditions contained in the Solicitation, unless otherwise stated herein; that I am submitting this bid, offer or proposal for review and consideration; that I am authorized by the vendor to execute and submit this bid, offer, or proposal, or any documents related thereto on vendor's behalf; that I am authorized to bind the vendor in a contractual relationship; and that to the best of my knowledge, the vendor has properly registered with any State agency that may require registration.

Dixon Hughes Goodman LLP
(Company)


(Authorized Signature) (Representative Name, Title)

Tom Tollerton, Managing Principal
(Printed Name and Title of Authorized Representative)

8/26/2019
(Date)

704-367-7020 704-367-7760
(Phone Number) (Fax Number)

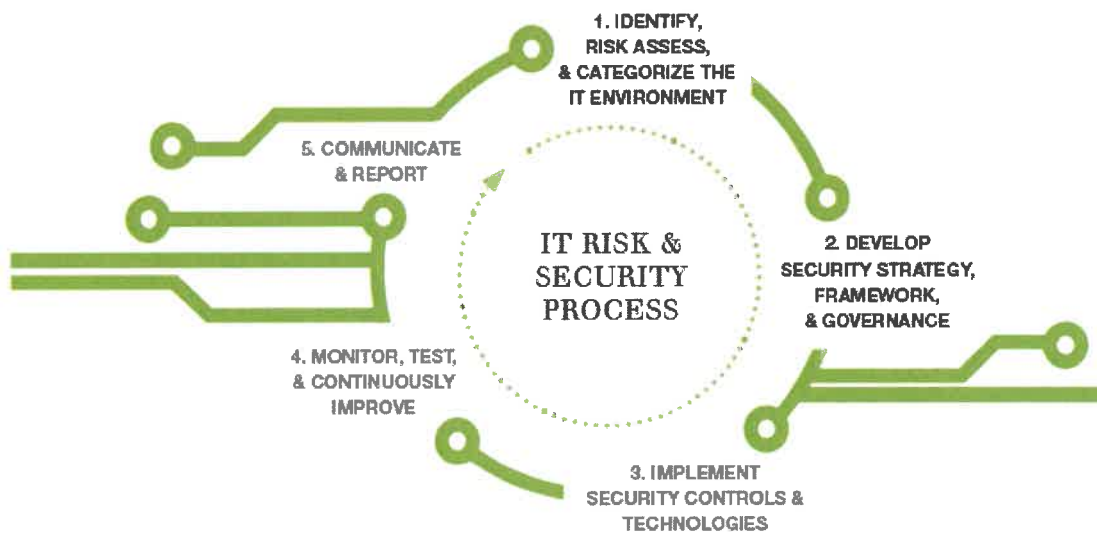
4.2.1 goals and objectives

The objective of the engagement is to assist the West Virginia Office of Technology (WVOT) in establishing a Cyber Security Risk Program to support state agencies as described in West Virginia code §5A-6B. On the following pages we outline our approach and methodology for providing the services, addressing the issues, and completing the projects as described in the RFP for each of the items in scope. As part of the engagement, we will plan for, create, implement and provide to WVOT personnel the Cyber Risk Program, as well as develop two solicitations on behalf of WVOT for auditing and compliance tools.

We will utilize guidance published by the National Institute of Standards and Technology (NIST); ISO 22301 Societal Security – Business Continuity Management Systems; and policies and standards of WVOT as well as other guidance that may be applicable.

4.2.1.1. FRAMEWORK DEVELOPMENT

We recommend the framework be adopted from the NIST Cybersecurity framework and supplemental publications for risk management and security controls, aligned with WVOT's business needs. The Risk Management Policy will be the initial policy in the WVOT Cyber Risk Program upon which the framework and all other policies will be developed. The Risk Management Policy will provide guidance to the WVOT and agencies in identifying and assessing information security risks and mitigating risk to an acceptable level. The framework will be leveraged in this first phase, identifying WVOT's most critical assets and proposing a prioritized roadmap and timeline for all agencies to be assessed.



DHG IT RISK ASSESSMENT PROCESS

4.2.1.1.1 Identify most critical information assets and align to applications and agencies

Through interviews with key agencies and WVOT individuals, we will gain a thorough understanding across the supported state agencies as to the business and technical environment supporting critical functions, processes and data.

Step 1: Perform an enterprise risk assessment interviewing state leadership, which includes Cabinet Secretaries and Agency Leadership, to understand and confirm critical information assets and asset categories across all WV state

agencies, establishing a risk management strategy based on organizational risk tolerance. The risk tolerance will be input in determining the organization's risk framing strategy, or how it assesses, responds to, and monitors risk. Develop a prioritized timeline for assessing and classifying the inventory of critical assets. Note that critical assets may include operational technology, as well as information technology, as key government functions may rely on such systems. Assign identifying attributes to all inventory assets to further prioritize them. Attributes will be developed, such as essential to security, maintains order in the economy, ensures general public health and safety, delivers essential public or private sector services, or must meet compliance requirements. Potential critical information assets could include:

- Automated data and systems
 - Citizen data (examples): personal health information, criminal records, tax information, driving records, adoption records
 - Sensitive agency data (examples): financial data, third party contracts, strategic planning, business disputes
 - Sensitive technology design (examples): network and infrastructure architecture design, security baselines and configurations, proprietary software
 - Sensitive building design information (examples): Department of Corrections, public infrastructure, data center facilities
- Facilities and equipment
 - Technology support: support of information technology assets, people, business continuity functions
 - Essential services: facilities that provide key services, essential to the state
- Operation technology
 - Surveillance and video: cameras, equipment such as used by the departments of Transportation or Public Safety
 - Industrial control systems (ICS) or supervisory control and data acquisition (SCADA) systems
- Non-automated data
 - Paper archives: records that are regulatorily retained in storage

Step 2: Provide a draft listing of critical agencies and associated assets to the Cyber Risk Committee for review and approval. Finalize the timeline for detailed asset inventory assessments within the critical agencies.

Step 3: With the approved critical Agency listing, work with each Agency to determine where critical information may be stored in the IT environment (e.g. physical documents, network file shares, applications, databases, and interfaces). Also work to determine which systems support critical functions, if these are distinct functions.

Step 4: Provide draft listing of each Agency's mapping of critical information and/or functions to the IT environment (e.g. physical documents, network file shares, applications, databases, and interfaces).

Step 5: Finalize the list and provide the deliverables to the Cyber Risk Committee.

4.2.1.1.2 Evaluate agencies with the highest risk exposure based off their assets and any mandated compliance requirements

All compliance requirements will be documented and assigned to assets, as applicable, to include regulations of West Virginia, the federal government, international, and specific industries. Examples are assets regulated by HIPAA, GDPR, FISMA, CJIS, CMS, FERPA, and others.

We will perform risk assessments on each of the previously identified critical agencies following the NIST Risk Management Framework. Associated with the risk assessment, the information gathered through interviews will be supplemented by the

use of automated asset inventory collection tools to capture all hardware, software, and operating systems. We will develop for each agency a Risk Register that catalogs risks. Each risk is assigned an occurrence impact, probability for the overall impact, and risk value. These risks values will be recorded in the Risk Register and provided to each agency for confirmation of the results. The Risk Register results for each agency can subsequently be captured and quantitatively managed in a governance, risk, and compliance (GRC) platform, providing WVOT full visibility.

4.2.1.1.3 Develop and consolidate evaluation framework

We will develop a tiered evaluation framework that guides the agency assessment for the state, with consideration of the critical assets and infrastructure, agency size, the maturity levels of security functions within the agencies, and the compliance requirements in alignment with state policies. The tiers will be defined and each agency assigned to tiers in accordance with the level of cybersecurity maturity, integrated with the agency's risk management processes. The NIST framework has four tiers ranging from low maturity to high and they are: 1) partial, 2) risk informed, 3) repeatable, and 4) adaptive. The tiers shall be defined according to WVOT goals, to include the compliance requirements and a baseline goal that all agencies should strive to achieve. Tiers will be developed keeping mindful that many of the agencies are in the initial stages of a cybersecurity program and funding program improvements is often a barrier to advancing beyond Tier 1. Tier definitions and goals are often adjusted upward after several years of implementation, providing the agencies with achievable progression when initiating a program of this magnitude. Most importantly, the state's goals for the program will form the basis of the tier definitions. The baseline standards for all agencies will be developed and agencies will be assigned a timeline for achieving the baseline. The baseline standards may be updated in the future, as well, reflecting the agencies' maturing individual programs.

Each of the agencies formerly identified as critical will be assigned to the tiers, once developed. The draft listing of the tiered phases and agencies in each tier will be provided to the Cyber Risk Committee for review and approval.

4.2.1.1.4 Establish a Risk Profiling Procedure and pilot the results of the risk profile

The risk profile is a compilation of the asset inventory previously identified and effectively classified according to its sensitivity, criticality to the organization, value, and regulation requirements. A threat modeling process will be performed, forming the strategic cyber risk profile from the adversaries' perspective of the high value assets. From this strategic risk profile, we will quantify the value for all risks and develop the tactical risk profile for each agency. The tactical risk profile will consider all policies, procedures, and technical controls that mitigate risk to improve the risk profile.

We will classify processes and assets by critical criteria and analyze, inventory and document the business applications, processes and data.

With the approved critical information listing, work with each Agency to determine where critical information may be stored in the IT environment (e.g. physical documents, network file shares, applications, databases, and interfaces).

4.2.1.2 CYBER RISK PROGRAM DOCUMENTATION / CREATION

The Cyber Risk Program will be comprised of a full suite of documentation, templates, policies, and procedures to be used by Agencies in the pilot program. All documentation will be revised and improved as the pilots are implemented and feedback is solicited and applied. The existing WVOT policies will be reviewed, modified, and included in the updated framework, to the extent that they meet WVOT's target goals.

4.2.1.2.1 Develop Policies and operations procedures, reporting templates, and program roadmap

Cybersecurity policies and procedures are foundational to the security framework. The policies will be specific enough to meet WVOT's baseline goals and provide structure and substance for those agencies with more advanced programs, those with mature and repeatable processes. The policies will be achievable by the less mature agencies, providing the structure needed to advance the state collectively.

Procedures will include processes and technical controls that are recommended as industry best practices and aligned with

the state's goals for all programs. The procedures should be tailored for each agency according to the agency's specific business needs.

Policies that may be developed or modified include:

- Information Security Governance
- Risk Management
- Asset Management
- Data Protection and Privacy
- Access Control / Passwords
- Acceptable Use
- Threat Vulnerability Management
- Business Continuity / Disaster Recovery Management
- Change Management
- Mobile Security / Remote Access
- Human Resources and Security Awareness
- Physical and Environmental Security
- Third Party / Supply Chain Risk
- Incident Response

The depth and breadth of policies to be created or further developed from the existing ones will be determined following completion of the initial WVOT assessment of critical assets. These are key policies needed for all security programs, but they can be modified and expanded as needed.

Procedures will be developed for each of the policies and include baseline technical controls that should be implemented and maintained by each Agency. The agencies will need to tailor all procedures, more extensively than the policies, to apply them to their actual and targeted practices, in alignment with business requirements.

4.2.1.2.2 Define roles and responsibilities between central teams and agencies

The roles and responsibilities of key security functions at the WVOT level and within the agencies will be defined as the resources implementing and maintaining the WVOT security program. On the WVOT organizational level, the Cyber Security Office will be instrumental in communicating with and guiding agencies and their implementation of the framework. Roles and responsibilities to be defined for the agencies include Agency Leadership, Information Security Officer, Information Owner, Security Administrator, and IT Management. Other roles and responsibilities will be defined and may be tailored for use by the agencies. Those roles are key to the incident response plan, business continuity, and also apply to policies with employee governance. They include but are not limited to: Senior Leadership, Human Resources, Legal, Communications, Public Relations and Internal Audit. A Responsibility Assignment Matrix (RAM) or Responsible Accountable Consulted Informed (RACI) chart will be developed for use by WVOT and within the agencies.

4.2.1.2.3 Document approach, tools, and templates for agencies to apply framework and manage audit and assessment activities

The security program documentation will be compiled in a handbook for use by the agencies. The documentation will include:

- WVOT state legislation and purpose for a cybersecurity program;
- Contact list of all resources available for implementation assistance, with the RACI chart of WVOT roles and responsibilities;
- Cybersecurity policies and procedures;
- The security framework worksheet that maintains all controls to be tracked and monitored;
- Reporting templates, both internally to the agencies and to the WVOT, such as for update to the annual risk exceptions report, security incidents, and a self-assessment of the program progress;
- Audit and compliance requirements, reportable externally and to the WVOT.

4.2.1.2.4 Pilot the program with at least one small and one large agency

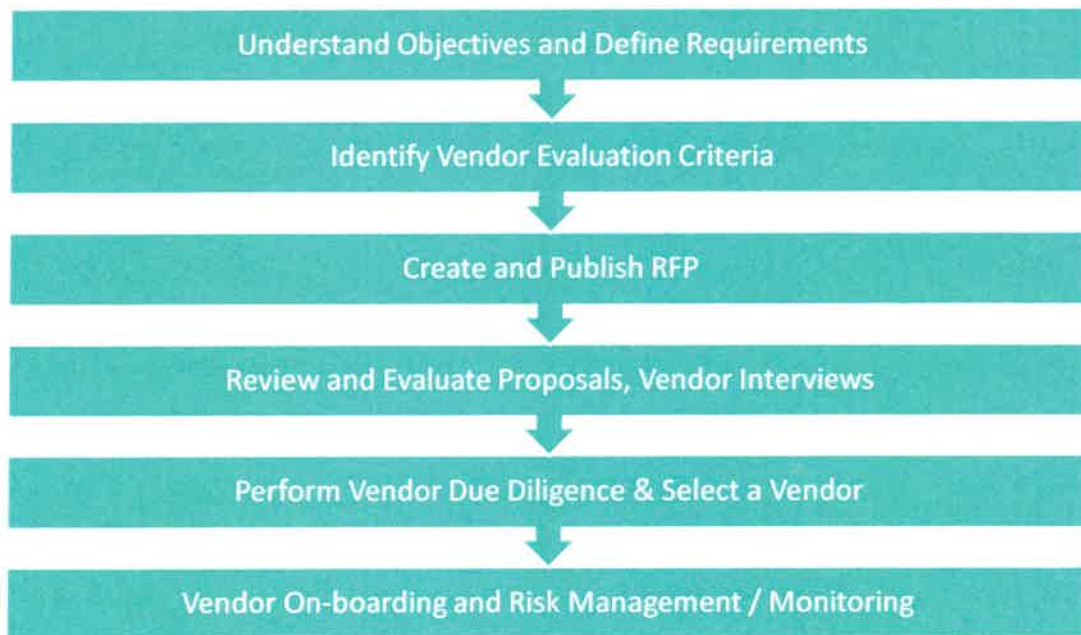
We will develop a project schedule with detailed tasks to be performed by WVOT, external consultants, and two agencies in the pilot phase. The two agencies should be those identified with critical assets and business diversification to test all aspects of the security program. The project schedule and resource requirements must be approved by WVOT and the agencies. Parallel implementations will make the most efficient use of WVOT resources and provide effective feedback to update processes or documentation immediately, as needed.

4.2.1.2.5 Assess the results and document lessons learned from Pilot program. Remediation of issues should be accounted for in the milestones and deadlines

Capturing and effectively applying the lessons learned during the pilot phase is critical for WVOT implementing further to all agencies. The input to this process and subsequent report will be reviewed by all stakeholders and adjustments made, as necessary.

4.2.1.3 COMPLIANCE AUDIT SOLICITATION

4.2.1.3.1 Assist WVOT in developing solicitation for a governance tool



4.2.1.3.2 Vendor should provide expertise in identifying, analyzing and evaluating agency risk and applying the appropriate security controls relevant to the information custodians

Leveraging our outlined approach to cybersecurity risk management, we will assist agency management in identifying, analyzing, and evaluating unique risks in agency operations and data use. The identified and prioritized risks will inform the security controls required to mitigate risk and drive development of requirements to be included in the solicitation.

4.2.1.3.3 Review vendor responses and advise reviewers

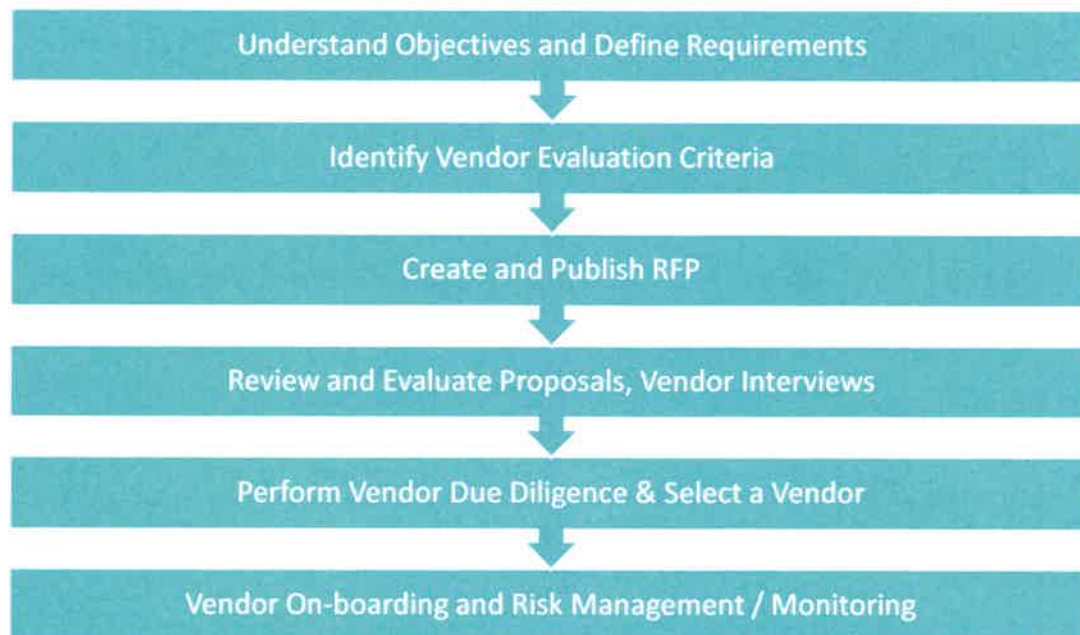
We will collect, compile, and provide initial review of vendor responses. We will prepare summary documentation, allowing state reviewers to perform a cost/benefit analysis for each proposing vendor and select a vendor.

4.2.1.3.4 Provide guidance and assistance to WVOT to process and assist agencies in using the solicitation

DHG has assisted various organizations with identifying and documenting key solution requirements and prioritizing prospective vendors. We will provide advisory assistance to WVOT in the use of solicitation documentation and vendor response information.

4.2.1.4 GOVERNANCE, RISK & COMPLIANCE (GRC) TOOL SOLICITATION

4.2.1.4.1 Assist WVOT in developing a solicitation for a governance tool



We will perform the following for this portion of the project:

- Interview stakeholders and document functional requirements
 - Provide draft requirements to stakeholders for review, approval, and ranking
 - Finalized requirements, with ranking / prioritization
- Provide draft vendor evaluation criteria to stakeholders for review and approval
 - Finalize vendor evaluation criteria
- Develop draft RFP document
 - Finalize RFP document
- Identify potential vendors
- Solicit vendors
 - Receive and collect proposals.
 - Evaluate and compare the proposals, compiling key criteria for WVOT Management to perform a cost-benefit analysis
- Recommend a selection of vendors and a high-level implementation plan, based upon our understanding of WVOT requirements defined in the solicitation.

4.2.1.4.2 Implement the governance tool to support future assessment

We anticipate that the GRC vendor selected by WVOT will have its own implementation team. However, there are many tasks that WVOT will need to be involved with and provide oversight for. DHG will work with WVOT management in a project management and project support role for those tasks. Examples of ways DHG can be strategic project partner, include:

- Assistance with the design of user access rights
- Assistance with the tracking and mapping of requirements throughout the process
- Assistance with the review of software company questions and decision points
- Assistance with the review of draft user acceptance testing scenarios
- Assistance with the executing user acceptance test steps
- Assistance with the monitoring progress, budget, and status
- Assistance with the design of processes and procedures
- Assistance with the documentation of processes

4.2.1.4.3 Establish baseline security and use procedures for the tool

We will assist WVOT, the appropriate agency personnel, and the selected vendor to define desired requirements for the use, administration, and management of the selected GRC tool. We will work with vendor personnel to establish these guidelines.

4.2.1.4.4 Customize the tool to align with state specific requirements established during programs development

The selected vendor would be expected to customize the tool to align with state specific requirements and work with the state and agencies to implement the tool appropriately.

4.2.1.4.5 Train users to utilize the governance tool and develop policies and procedures for the governance tool

DHG can provide some guidance with the selected vendor to provide training on the use and ongoing maintenance of the selected GRC tool. The training and education should require an annual refresher and be comprised of various forms of delivery methods such as in person and online offerings. The vendor may consider a stratified approach to provide relevant training to daily users, and education to those in more of a supervisory role.

4.2.1.5 FULL IMPLEMENTATION / ROLL OUT PLAN TO DEPLOY FRAMEWORK TO AGENCIES

4.2.1.5.1 Include a communications plan



4.2.1.5.2 Include education and enablement of tools

DHG will design an education plan for a broad audience which may include the following:

- Training Sessions
- Town Halls
- Webinars

4.2.1.5.3 Incrementally expand pilot program

We will facilitate the identification and definition of priorities and develop a plan for implementation across the State agencies. First, we will obtain approval from WVOT on a high level implementation roadmap, estimated resource needs, and training timelines. Once we have a repeatable execution we can determine the next phase in the roll out once the initial pilot is complete and WVOT is satisfied with the outcomes. Establishing and agreeing to the roadmap and ensuring management can assess what resources are needed as part of the implementation process across a wider selection of agencies will be an important step.

4.2.1.5.4 Plan for framework deployment and audit execution across the enterprise

4.2.1.5.5 Include the performance of audit of enterprise services

4.2.1.5.6 Support agencies with utilizing the third-party vendor awarded a contract to perform assessments

During deployment, we will plan for testing of the newly deployed framework to a select sample of agencies/departments. For this testing we will measure outcomes, issues, and identify gaps in controls, documenting inherent and residual risks. We will work with WVOT and key stakeholders identified at the agency level to plan for remediation, discuss the root cause analysis and control enhancement opportunities.

Importance and Value of Assessing Inherent Risk and Residual Risk:

The assessment of both Inherent Risk and Residual Risk highlights and provides insight and transparency to important management information not otherwise readily available, including:

- Risks where management relies heavily on the continued and effective operation of key controls (high inherent risk/low residual risk)
- Risks whose nature does not significantly alter following the application of controls, indicating that certain controls may be ineffective (high inherent risk/high residual risk)
- Risks that may be over-controlled (low inherent risk/low residual risk)

4.2.1.6 ONGOING SUPPORT / SUPPORTABLE BUSINESS MODEL

4.2.1.6.1 Ensure that its Cyber Risk Program services are trackable in accordance with WVOT charge back model

We will review WVOT's chargeback model and propose rates for the cybersecurity services offered to the agencies. The pricing should be based upon the resources assigned to the tasks in determining the appropriate charges.

4.2.1.6.2 Identifying appropriate points for fee assessment

We assume that fee assessment would be consistent with the current service rates and charge methods. Fees should be assessed as services are provided. General fee assessments for program support may be assessed as agencies use the cyber program services, which should be soon after the pilot phase. WVOT will need to assess the need for additional staffing to sufficiently deliver all services, including advisory services such as a Virtual Chief Information Security Officer

offering to lead efforts in agencies lacking technical support.

4.2.1.6.3 Assist WVOT in establishing pricing for various aspects of the Cyber Risk Program

We would outline the security program tasks to be performed by the agencies, working with the WVOT Cyber Security Office to determine which ones they would want to offer to the agencies. WVOT might want to augment resources with external service providers to maintain control and consistency in service delivery and having visibility into the status of all programs. Services provided could include:

- Review and develop agency policies and procedures;
- Perform agency risk assessments, developing the roadmap for program implementation;
- Perform vulnerability assessments; internal network, application, external web application, and wireless network penetration testing services;
- Perform security awareness training and tabletop exercises;
- Deliver social engineering exercises, such as phishing campaigns;
- Provide fractional or virtual Chief Information Security Officer services;
- Provide incident response support, containment and eradication, and forensics services.

4.2.1.6.4 Recommendations would recommend Enterprise cybersecurity risk services based on services which directly addresses state-wide critical cyber risks

The services listed above would address critical cyber risks, as well as those facing all agencies. Additional technical controls may be needed for those agencies specifically handling CJIS or PHI data, as examples. single sign-on, network access control, privileged access management, mobile device management, static or dynamic code analysis, leveraging cloud services for backups or redundancy such as through AWS or Azure, email protection with Microsoft O365 Advanced Threat Protection: these are but a few examples of technical controls that may be used to protect agencies with critical or highly sensitive data.

We will provide guidance for WVOT's vetting of products and services that may be offered in the services catalog or developed as a list of trusted and supported products maintained by WVOT.

4.2.1.6.5 Recommendations should take into consideration leveraging cost sharing and economies of scale opportunities to drive cost- efficiencies

All services can be provided in full by WVOT resources or the tasks and costs shared between the agency and WVOT. For example, vulnerability testing may be performed by an agency using a scanning tool, such as Nessus, with an enterprise license procured by WVOT. Agencies may need assistance with their vulnerability management initially, then choose to use the enterprise license at a discounted price to perform regular scans and take ownership of the assessments. As agencies mature in their security programs, services can be transitioned to the agencies as they receive training and education for the new tasks. WVOT can leverage vendor training for products and provide at minimal or no cost to the agencies.

4.2.1.6.6 implemented and delivered as an enterprise/managed service, addressing cyber workforce challenges

Cyber workforce challenges can be met through staff augmentation. Additionally, offering preferred vendors to deliver the requested security services and managing the allocation of those services to ensure consistency will provide the resources needed to implement the security program while ensuring the program's goals are being addressed. Once the scope of the full project implementation and resource requirements have been determined, we will assess options for workforce development and leveraging external resources to ensure that WVOT can meet its enterprise project goals while supporting the agencies in their implementation.

4.2.1.7 COMMUNICATION PLAN

4.2.1.7.1 The State can apply custom branding to all documents and materials

Our agreement with the state would be structured as such to allow branding on all of our deliverables. WVOT management would be responsible for reviewing and accepting deliverables provided as part of this engagement.

4.2.1.7.2 Vendor should establish regular communications to discuss project status at a minimum of every two (2) weeks

It will be critical for the success of the development of the Cyber Security Risk Program that our team establishes a detailed project plan with WVOT stakeholders to include status updates at appropriate times throughout the work. We will commit to a project status update communication at the minimum of every two weeks. The final project plan will be accepted by both parties prior to the commencement of work.

4.2.1.7.3 Vendor should provide communications to different levels of stakeholders identified in the project proposal

Our teams strive to develop and maintain quality relationships with the management and stakeholders of our clients to work efficiently and effectively on projects, and as issues arise. Each phase of our engagement requires proactive communication between the engagement team and the WVOT stakeholders identified in the project plan. Personal contact will be essential to the overall success of the engagement.

4.2.1.7.4 Vendor should provide on-site support for major milestones and project initiatives

Effective project management and communication are the keys to a successful engagement. DHG's project management methodology effectively addresses the objectives of cost, time, and quality. Specifically, our team will coordinate with you through use of the following tools:

- Identification of Key Contacts – Identifying key stakeholders from WVOT with whom our team members can form a project committee will be helpful. The committee will be responsible for formation of planning activities, deadlines and decisions to ensure a successful engagement.
- Status Reporting – Regular visibility to progress and issues identified in the execution of the engagement activities; Real-time reporting of findings in person for major milestones and project initiative planning.
- Risk and Issue Escalation – Continuous maintenance of and focus on resolution of project issues
- Providing Updates – Clear and appropriate project status and issue escalation to stakeholders as well as planned in person meetings
- Change Management Control Process – Agreement of required changes to schedule, scope, and budget
- Financial Management – A 'no surprise' approach, achieved by sharing the budget template as needed, which includes: actual versus expected hours & cost; projections for expected hours & cost; analysis of the remaining hours & costs left at any given point in time.

4.2.2. Mandatory Requirements

4.2.2.1. Timeline

Prior to beginning any onsite work, our engagement leadership will meet with WVOT's management to devise a detailed schedule to include major milestones, the timing of deliverables that DHG will provide throughout the engagement, onsite meetings, task progress updates and other important steps in the project. Developing a full project plan and the ensuing process will help ensure we meet WVOT's expectations while clearly outlining the timing of each major component of the engagement.

4.2.2.2. - The Plan will be developed to comply with applicable West Virginia state and federal laws

It is our intention to create a plan that complies with all applicable West Virginia, state and local laws regarding cyber security programs.

4.2.2.3. – We agree that the program will adhere to the following:

- 4.2.2.3.1. The program must enable a 3-tiered organizational hierarchy allowing for cyber risk ownership
- 4.2.2.3.2. The program must account for the standardization of the impact risk variable.
- 4.2.2.3.3. The program must include the capability to leverage both qualitative and quantitatively risk assessments and provide recommendations how to effectively and efficiently leverage both.

4.2.2.4 We agree that all documentation and materials associated with the project will be owned by the State of West Virginia.

Any deliverables prepared as a result of the engagement will become the property of the State of West Virginia. Any workpapers prepared by DHG in support of this engagement will remain in the possession of DHG for seven years.

4.2.2.5 As stated in this proposal, we agree to base the project on industry framework such as NIST and will work with the management of WVOT to select the appropriate frameworks and guidance.

4.3.1 qualifications and experience

For this project, DHG is partnering with Soteria, a subcontractor who compliments DHG's services and who is experienced in the services requested by WVOT. All future references to the Supplier will represent the DHG and Soteria team.

ABOUT DHG

Dixon Hughes Goodman LLP ("DHG") is a Top 20 firm with national clients and a local Charleston, WV presence. We have more than 2,000 professionals in 13 states and we focus on a number of industries, including Advisory Services for State Government. **Over the past 5 years, the DHG team has served over 20 state agencies.**

DHG's IT Advisory practice uses a risk-based approach to evaluate the people, processes, and technology that affect your organization's success. We advise our clients on best practices with the aim of protecting the security and integrity of the data, networks, and technology that are at the very heart of your organization. Our thorough analyses help clients who rely on Internet technology or software applications identify risk and implement strategies to minimize exposure.

Our dedicated team brings years of industry and professional services experience, plus critical certifications, to each of our engagements. We serve clients in a variety of industries including state and local governments, technology, financial services, insurance, nonprofits, hosting and application service providers, and third-party services.

ABOUT SOTERIA

Soteria is headquartered in Charleston, South Carolina and **has served more than 22 state agencies in the past three years.** They were founded by former members of US government agencies tasked with exploitation and attack of nation-state level adversaries. In addition to serving state and local government organizations, Soteria provides expert security advisory, consulting, and services to clients in the financials, global logistics, insurance, and technology sectors.

Soteria's team is well-versed in developing strategies for defending national infrastructure from cyber threats and attacks. Soteria's expertise in the cybersecurity domain is predicated upon its cybersecurity professionals serving in leading national security positions within the US military, intelligence community, and private industry.

Soteria is one of only a few providers on the state of South Carolina's Information Security and Privacy Services contract for security assessments and consulting, incident response management, and security monitoring analytics services. During the term of this contract, Soteria has competed for and won business at an increasing rate, primarily due to the firm's stellar track record for service delivery.

4.3.1.1. OUR EXPERIENCE

DHG generally does not share client lists out of consideration for our clients' confidentiality. We can share with you that our team has experience providing IT Consulting Services to various governmental agencies and state entities. For these clients, we have performed:

- Project Management, Requirements Analysis, and Implementation Support
- Using Governance, Risk, and Compliance (GRC) Solutions
- Cybersecurity Consulting
- IT Security Framework Consulting
- Cloud Security Consulting
- Network and Infrastructure Design

- Vulnerability Management
- Security Operations Center (SOC) Design & Monitoring
- Incident Response & Forensics
- Identity & Access Management
- Process and Organizational Design
- Training for Security Awareness, Incident Response, Business Continuity

4.3.1.2. REFERENCES

DHG

Ed Miller
Director IT Security Governance
Virginia Information Technologies Agency (VITA)
edward.miller@vita.virginia.gov
(804) 416-6027

Brian Gibbs-Wilson
Chief Information Security Officer
Virginia Department of Education
brian.gibbs-wilson@doe.virginia.gov
(804) 225-4209

Soteria

Richard Makla
Chief Strategy Officer
South Carolina Department of Administration, Office of Technology and Information Services
richard.makla@admin.sc.gov
(803) 896-8958

James Brown
Chief Information Security Officer
South Carolina Department of Administration
james.brown@admin.sc.gov
(803) 896-8958

Brian Leach
Information Technology Director
South Carolina State Election Commission
bleach@elections.sc.gov
(803) 734-9059

4.3.1.3. OUR PROFESSIONALS

Our philosophy is to have significant Principal, Director and Manager involvement on our engagements. Overall, this program delivers:

- A better understanding of your needs, objectives and expectations
- The ability to assess our performance meeting your expectations
- The development and implementation of a collaborative communication structure for reporting purposes

The following professionals will make up your engagement team, with other staff engaged as necessary to meet the goals of this project. Our firms have the skills and staffing capabilities to ensure a successful engagement.



Rodney Murray | Managing Principal | 704.367.7062 | rodney.murray@dhg.com

Rodney Murray is based out of the Charlotte office and leads the firm's IT Advisory practice. Rodney has more than 30 years of experience in information technology and business applications, including providing internal audit and risk management services. His risk and advisory experience includes managing and performing technology risk and controls assessments, Sarbanes-Oxley compliance, HIPAA and GLBA privacy compliance, business process analysis, SOC reporting and assistance to internal audit functions. Rodney's client base includes financial institutions, hospitals and health care providers, state and local governments, manufacturers, hosting and application service providers and third party services providing financial transaction processing.

Prior to joining DHG, Rodney worked for a Big Four accounting firm for more than six years delivering IT risk and advisory services across all industry segments. His client base included community, regional and national banks, third-party service providers to financial institutions, manufacturers, retailers, and state and local governments.

LICENSES & CERTIFICATIONS

- Certified Information Systems Auditor
- Certified in Risk and Information Systems Control

EDUCATION

- University of North Carolina Chapel Hill, BS, Business Administration

**Ben Sady | Principal | 804.474.1267 | ben.sady@dhg.com**

Ben is a Principal in the Risk and IT Advisory Services practice in the DHG Atlantic region. Ben has over 15 years of professional experience providing Consulting services to public and private companies across a wide range of industries, including significant experience serving State Agencies.

Ben has services to over 50 organizations. He began his career at a Big Four firm and later, he held a leadership position at a firm providing Consulting services. In these roles, Ben managed every aspect of the consulting process, including scoping, risk assessment, project management, managing fieldwork and deliverables, and reporting results to client senior management.

Ben's project experience includes leading teams in:

- Cyber Consulting (GRC, Framework Design and Strategy, Control Mapping, Information Security, Data Privacy, Technology Change, Third Party Risk Management, Disaster Recovery, Cloud Technologies, Application Risks, Tools & Technologies)
- Technology Consulting (Vendor Selection Criteria, PMO Formation, Project Management, Requirements Gathering, Data Mapping & Quality, User Acceptance Testing, Project Documentation, End User Training)
- Business Process Improvement Consulting (Process Documentation, Process Design Evaluation, Control Identification, Gap Identification, Re-engineering, Performance Metrics & Dashboards)
- Internal Audit and IT Audit (Outsourcing/Co-sourcing, Financial Process Reviews, Business Process Reviews, IT Process Reviews)

LICENSES & CERTIFICATIONS

- Certified Information Systems Auditor
- Certified Internal Auditor
- Certified in Risk and Information Systems Control
- Project Management Professional

EDUCATION

- Virginia Tech, BS, Business Technology



Paul Ihme | Co-founder and President Consulting Services | 843.510.0538 | pihme@soteria.io

Paul has 14 years of experience in advanced cybersecurity offensive operations and defense of large multi-layered networks. He leads Soteria's security solutions and vCISO practice for clients and provides advisory services to C-suite and board level clients from multi-billion dollar global companies to small sized business, both government and corporate. He has significant experience in risk assessments, developing security programs and incident response, as well as SOC analysis with federal government agencies and global financial institutions. He is experienced in working with NIST, ISO, CoBIT, PCI, HIPAA, CIS Top 20. He spent 10 years in the Air Force with roles focused on software development, network defense, and offensive cyber operations.

LICENSES & CERTIFICATIONS

- Certified Information Systems Security Professional
- GIAC Reverse Engineering Malware (GREM)

EDUCATION

- Community College of the Air Force, AAS, Cyber Security, Communications Technology
- University of Maryland University College, BS, Computer Science
- Eastern Michigan University, MS, Technical Studies, Offensive Computer Security



Tom Tollerton | Managing Director | 704.367.7061 | tom.tollerton@dhg.com

Tom has over 15 years of experience in the cybersecurity industry and manages the firm's cybersecurity and data privacy compliance services. Tom specializes in cyber risk management, data privacy compliance, SOC reporting, and PCI compliance assessments, and his experience includes performance of cybersecurity risk assessments, data privacy assessment and consulting projects, and compliance audits for a variety of clients, including multiple public-sector and municipality clients. Leveraging deep technical experience, Tom's experience with specific frameworks includes DFARS, NIST 800-53, and NIST 800-171 Compliance. His clients include organizations of all sizes in the governmental sector, fintech, dealership, communications, insurance, and software industries, including multiple Fortune 500 corporations.

Tom has had multiple articles published in national publications and is a regular speaker on current cybersecurity and privacy topics at various firm and industry events.

LICENSES & CERTIFICATIONS

- Certified Information Systems Security Professional
- Certified Information Systems Auditor
- Payment Card Industry Qualified Security Assessor

EDUCATION

- Florida State University, Master of Business Administration
- Florida State University, BS



Pam Everitt | Senior Security Consultant | 843.514.3955 | peveritt@soteria.io

Pam has 18 years of experience as CIO in a large, quasi-state agency with global support of multiple locations that provided significant economic impact to the state. She has 25 years of IT leadership for government and corporate enterprises. She has led several complex infrastructure and enterprise systems implementations incorporating IoT, cybersecurity and physical security controls and achieving required compliance with federal and state entities. Pam has also led multi-site business continuity and disaster recovery projects. She leveraged her consulting services experience to develop a 10-year technology strategy, which led to more managed services and cloud computing and shifted the IT cost model from capital to operating with clear business value metrics.

LICENSES & CERTIFICATIONS

- Certified Information Systems Security Professional

EDUCATION

- The Citadel, MBA and BS, Business Administration



Douglas Jambor | Senior Manager | 704.367.5987 | douglas.jambor@dhg.com

Douglas has 13 years of full-time penetration testing experience in the information technology field focusing on information systems security and information security risk management. He is DHG's cybersecurity subject leader and manager over all of the firm's technical cybersecurity services, which includes Internal, External, Wireless, and Web Application Security Assessments (Penetration Testing). Other cybersecurity services also include testing end-user awareness levels via Social Engineering Assessments from email-based (phishing), phone-based (vishing), fake website (online), and building access walkthroughs (physical) attack vectors. Over the last decade, Douglas has performed hundreds of both penetration testing and IT audit engagement for clients located in every industry. He has also performed many incident response engagements and acted as the lead digital forensics investigator.

LICENSES & CERTIFICATIONS

- Certified Information Systems Security Professional (ISC)²
- Certified Computer Examiner

EDUCATION

- DeVry University, Bachelor Computer Information Systems, Digital Forensics



Jim Buda | Manager | 404.215.7540 | jim.buda@dhg.com

With 5 years of experience, Jim focuses on IT audits, information system security audits, SOX, SOC reporting and PCI Compliance assessments. He also performs network security assessments for clients in a variety of industries. His experience includes IT internal auditing, information security co-sourcing, internal control evaluation and effectiveness training.

LICENSES & CERTIFICATIONS

- Certified Information Systems Auditor
- Certified Public Accountant
- Security + (CompTIA)

EDUCATION

- University of North Carolina, Wilmington, Masters Accountancy, Systems Accountancy
- University of North Carolina, Wilmington, Bachelors, Business Administration, Accounting & Information Systems



John Richardson | Manager | 804.474.1221 | john.richardson@dhg.com

John has more than 15 years of experience in Information Technology across multiple industries. His particular areas of expertise include understanding business strategy, culture and goals to align proper technology and security controls to match business needs. John's experience includes:

- Created and implemented IT policies and procedures and performed risk assessment for 200+ systems for a state agency
- Aligned Information Technology (IT) with strategic plan and mission to facilitate efficiency, productivity and profitability for a national logistics company
- Provided continuous auditing of information security governance and risk management for legal, regulatory and compliance requirements
- Designed and implemented a business continuity and disaster recovery program
- Consolidated multiple standalone servers into enterprise virtual environment
- Initiated, developed and implemented operational security policies, procedures, guidelines and awareness training

LICENSES & CERTIFICATIONS

- Certified Information Systems Auditor
- Certified Information Systems Security Professional
- Certified Ethical Hacker
- Payment Card Industry Qualified Security Assessor

EDUCATION

- Virginia Commonwealth University Masters Business Administration
- Old Dominion University Bachelors Business Administration



Deidre Tompkins | Manager | 804.474.1234 | deidre.tompkins@dhg.com

With 25+ years of experience in cyber risk and compliance advisory, Deidre recently joined DHG from a global cybersecurity company where she was Director of Cyber Advisory Services. While there, she designed custom solutions to protect critical information assets and manage risk for a variety of clients. Her experience includes the design and implementation of custom enterprise security programs for commercial and government entities. She has delivered comprehensive enterprise cybersecurity risk management programs, security governance and policy design/development/implementation, enterprise cybersecurity risk assessments and compliance audits, security program maturity reviews, security awareness programs, architecture reviews, pen testing and compromise assessments, incident response consultation, physical security control implementations, and managed SOCaaS, and onsite custom SOC implementations.

LICENSES & CERTIFICATIONS

- Certified Information Security Manager
- Certified Information Systems Security Professional (ISC)²
- Certified Information Systems Auditor
- Certified Scrum Master
- Project Management Professional
- Six Sigma Green Belt and Black Belt

EDUCATION

- Mercer University Masters Management Information Systems
- Mercer University Bachelors Business Administration

4.3.1.4. EXPERIENCE OF ENGAGEMENT TEAM

Our team members were selected as a reflection of this particular project's needs and objectives, and its members bring relevant experience, knowledge, and credentials. After reviewing the requirements, we believe our team's experience in the following areas are of greatest importance to you:

- Experience Providing Consulting Services to governmental agencies and state entities
- Project Management, Requirements Analysis, and Implementation Support
- Using Governance, Risk, and Compliance (GRC) Solutions
- Cybersecurity Consulting
- IT Security Framework Consulting
- Cloud Security Consulting
- Network and Infrastructure Design
- Vulnerability Management
- Security Operations Center (SOC) Design & Monitoring
- Incident Response & Forensics
- Identity & Access Management
- Process and Organizational Design
- Training for Security Awareness, Incident Response, Business Continuity

4.3.2. Mandatory qualifications and experience

4.3.2.1 Our Direct Experience with Implementing a Cyber Risk Management Program

PROJECT / SERVICE	PROJECT
<p>IT Framework Mapping & Implementation</p>	<p>DHG has assisted many complex and regulated organizations with identifying a common control framework and then mapping it against NIST, ISO, SSAE 18 / SOC Controls, PCI DSS Controls, HIPAA Security Controls, Cloud Controls Matrix from CSA, CIS Top 20, and many more.</p> <p>We have also helped organizations with the implementation of the common control framework by identifying existing controls, control gaps, and an implementation roadmap.</p>
<p>Private Equity IT Framework Design and Implementation</p>	<p>Soteria recently completed a project with a private equity firm to design and implement an information security framework to be applied to the firm, as well as its portfolio of companies. This proved to be a complex and challenging project, as the portfolio companies varied in size, complexity, and regulatory requirements. For example, while many portfolio companies were healthcare providers with requirements to protect PHI, PII, and payment card information, others were niche manufacturing companies with less than 50 employees and very limited information technology resources or requirements.</p> <p>Soteria worked with the parent company and representatives from the portfolio to design a security framework that instills the appropriate level of rigor and process to each firm, based on their level of risk, resources, and regulatory requirements. This framework has since been deployed and Soteria participates in ongoing working groups with representatives from the portfolio companies to assist with strategy and guidance as needed.</p>

REQUEST FOR PROPOSAL
CRFP ISC200000001
WVOT – Cyber Security Program

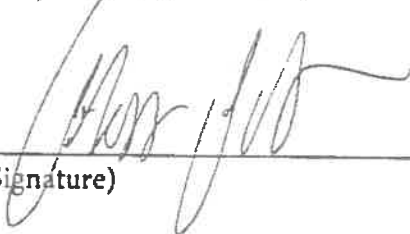
By signing below, I certify that I have reviewed this Request for Proposal in its entirety; understand the requirements, terms and conditions, and other information contained herein; that I am submitting this proposal for review and consideration; that I am authorized by the bidder to execute this bid 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.

Dixon Hughes Goodman LLP
(Company)

Tom Tollerton, Managing Director
(Representative Name, Title)

704-367-7020 / 704-367-7760
(Contact Phone/Fax Number)

8/26/2017
(Date)

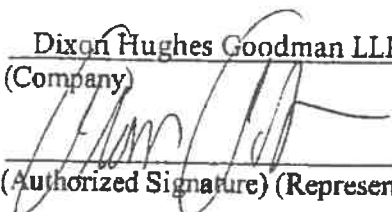

(Signature)

DESIGNATED CONTACT: Vendor appoints the individual identified in this Section as the Contract Administrator and the initial point of contact for matters relating to this Contract.

Tom Tollerton, Managing Director
(Name, Title)
Tom Tollerton, Managing Director
(Printed Name and Title)
4350 Congress Street, Suite 900, Charlotte NC 28209
(Address)
704-367-7020 704-367-7760
(Phone Number) / (Fax Number)
Tom.Tollerton@dhg.com
(email address)

CERTIFICATION AND SIGNATURE: By signing below, or submitting documentation through wvOASIS, I certify that I have reviewed this Solicitation in its entirety; that I understand the requirements, terms and conditions, and other information contained herein; that this bid, offer or proposal constitutes an offer to the State that cannot be unilaterally withdrawn; that the product or service proposed meets the mandatory requirements contained in the Solicitation for that product or service, unless otherwise stated herein; that the Vendor accepts the terms and conditions contained in the Solicitation, unless otherwise stated herein; that I am submitting this bid, offer or proposal for review and consideration; that I am authorized by the vendor to execute and submit this bid, offer, or proposal, or any documents related thereto on vendor's behalf; that I am authorized to bind the vendor in a contractual relationship; and that to the best of my knowledge, the vendor has properly registered with any State agency that may require registration.

Dixon Hughes Goodman LLP
(Company)


(Authorized Signature) (Representative Name, Title)

Tom Tollerton, Managing Principal
(Printed Name and Title of Authorized Representative)

8/26/2019
(Date)

704-367-7020 704-367-7760
(Phone Number) (Fax Number)

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 exceeds 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: Dixon Hughes Goodman LLP

Authorized Signature: [Signature]

Date: 8/26/19

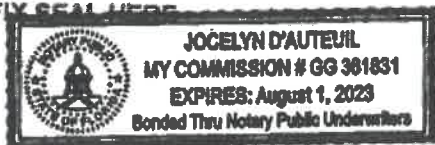
State of Florida

County of Orange, to-wit:

Taken, subscribed, and sworn to before me this 26 day of August, 2019

My Commission expires August 1, 2023

AFFIX SEAL HERE



NOTARY PUBLIC

[Signature]

Purchasing Affidavit (Revised 01/19/2018)

West Virginia Ethics Commission
Disclosure of Interested Parties to Contracts

(Required by W. Va. Code § 6D-1-2)

Dixon Hughes Goodman

Name of Contracting Business Entity LLP Address: 500 Virginia Street, Suite 800; Charleston WV 25301

Name of Authorized Agent: Tom Tollerton Address: 4350 Congress Street, Suite 900, CLT NC

Contract Number: TBD Contract Description: _____

Governmental agency awarding contract: WV Office of Technology

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.

Soteria LLC
Charleston SC

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.

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: 8/26/2019

Notary Verification

State of Florida, County of Orange:

I, Thomas Burleigh Tollerton, 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 26 day of August, 2019

Notary Public's Signature

To be completed by State Agency:

Date Received by State Agency: _____

Date submitted to Ethics Commission: _____

Governmental agency submitting Disclosure: _____



Revised June 8, 2018

ADDENDUM ACKNOWLEDGEMENT FORM
SOLICITATION NO.: _____

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)

- | | |
|--|--|
| <input checked="" type="checkbox"/> Addendum No. 1 | <input type="checkbox"/> Addendum No. 6 |
| <input checked="" type="checkbox"/> Addendum No. 2 | <input type="checkbox"/> Addendum No. 7 |
| <input type="checkbox"/> Addendum No. 3 | <input type="checkbox"/> Addendum No. 8 |
| <input type="checkbox"/> Addendum No. 4 | <input type="checkbox"/> Addendum No. 9 |
| <input type="checkbox"/> Addendum No. 5 | <input type="checkbox"/> 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.

Dixon Hughes Goodman LLP
Company

[Handwritten Signature]
Authorized Signature

9/26/2019
Date

NOTE: This addendum acknowledgment should be submitted with the bid to expedite document processing.
Revised 6/8/2012



Purchasing Division
 2019 Washington Street East
 Post Office Box 80130
 Charleston, WV 25305-0130

State of West Virginia
 Request for Proposal
 10 - Consulting

Proc Folder: 609025

Doc Description: Cyber Security Program RFP (OT19152)

Proc Type: Central Master Agreement

Date Issued	Solicitation Class	Solicitation No	Version
2019-07-26	2019-08-29 13:30:00	CRFP 0210 ISC2000000001	1

BID CLERK

DEPARTMENT OF ADMINISTRATION

PURCHASING DIVISION

2019 WASHINGTON ST E

CHARLESTON

WV 25305

US

Vendor Name, Address and Telephone Number:

Dixon Hughes Goodman LLP
 500 Virginia Street, Suite 800
 Charleston WV 25301
 304.343.0168

FOR INFORMATION CONTACT THE BUYER

Jessica S Chambers

(304) 558-0246

jessica.s.chambers@wv.gov

Signature X

FEIN # 56-0747981

DATE

8/26/19

All offers subject to all terms and conditions contained in this solicitation



Purchasing Division
 2019 Washington Street East
 Post Office Box 50130
 Charleston, WV 25305-0130

State of West Virginia
 Request for Proposal
 10 - Consulting

Proc Folder: 609025

Doc Description: Addendum 1-Cyber Security Program RFP (OT19152)

Proc Type: Central Master Agreement

Date Issued	Solicitation Closes	Solicitation No	Version
2019-07-30	2019-08-29 13:30:00	CRFP 0210 ISC2000000001	2

BID RECEIVING LOCATION

BID CLERK
 DEPARTMENT OF ADMINISTRATION
 PURCHASING DIVISION
 2019 WASHINGTON ST E
 CHARLESTON WV 25305
 US

VENDOR

Vendor Name, Address and Telephone Number:

Dixon Hughes Goodman LLP
 500 Virginia Street, Suite 800
 Charleston WV 25301
 304.343.0168

FOR INFORMATION CONTACT THE BUYER

Jessica S Chambers
 (304) 558-0246
 jessica.s.chambers@wv.gov

Signature X

FEIN # 56-0747981

DATE

8/26/2019

All offers subject to all terms and conditions contained in this solicitation



Purchasing Division
 2019 Washington Street East
 Post Office Box 50130
 Charleston, WV 25305-0130

State of West Virginia
 Request for Proposal
 10 - Consulting

Proc Folder: 609025

Doc Description: Addendum 2-Cyber Security Program RFP (OT19152)

Proc Type: Central Master Agreement

Date Issued	Solicitation Closes	Solicitation No	Version
2019-08-21	2019-08-29 13:30:00	CRFP 0210 ISC2000000001	3

BID RECEIVING LOCATION

BID CLERK
 DEPARTMENT OF ADMINISTRATION
 PURCHASING DIVISION
 2019 WASHINGTON ST E
 CHARLESTON WV 25305
 US

VENDOR

Vendor Name, Address and Telephone Number:

Dixon Hughes Goodman LLP
 500 Virginia Street, Suite 800
 Charleston WV 25301
 304.343.0168

FOR INFORMATION CONTACT THE BUYER

Jessica S Chambers
 (304) 558-0246
 jessica.s.chambers@wv.gov

Signature X

All offers subject to all terms and conditions contained in this solicitation

FEIN # 56-0747981

DATE

8/26/19