Wharton County Junior College

Board of Trustees
Agenda Item

Date of Board Meeting: February 20, 2024

Subject: Cybersecurity Staff Augmentation

Recommendation: Approve the contract with Strata Information Group to continue using staff augmentation services for Cybersecurity.

Background and Rationale:

In compliance with Texas DIR requirements, each institution of higher education must have staff that is dedicated to the oversight and management of cybersecurity efforts. In recent years, the College has utilized contract services with third-party vendors to attend to the cybersecurity needs of the institution. In preparation for the initial contract, the College solicited and received information from two (2) vendors regarding their cybersecurity services: Strata Information Group and Columbia Advisory Group. Both Strata Information and Columbia Advisory currently have cooperative purchasing contracts that would allow us to sign an agreement without going out for formal bids.

The services quoted by each party include:

- SIG: vCISO Services @ $6,720/month for 6 months = $40,320
- CAG: vCISO Services @ $5,750/month for 12 months = $69,000

The services provided through SIG have been superior and include designated staff support, comprehensive documentation development for upcoming FY 24 cybersecurity audit, and monitoring of all systems. The IT team recommends the continuation of services with SIG for the remainder of the fiscal year.

Cost and Budgetary Support: $40,320 (Current operating budget)

Strategic Priority Alignment:

- ☐ Student Success
- ☐ Community Impact
- ☑ Resource Optimization
- ☑ Institutional Excellence

Resource Person(s): Amanda Allen, Ed.D.; Vice President of Strategy, Enrollment Mgmt, and Technology

Signatures:

Cabinet-Level Supervisor — Date: 02/08/24

02/08/2024

President's Approval:

President — Date: 2-12-24

POLICY DB (LOCAL)
08/01/2020

PROPOSAL FOR SERVICES

Strata Information Group, Inc.
3935 Harney Street, Suite 203
San Diego, CA 92110
United States

Prepared By	Kyle Bork	Created Date	2/7/2024
Email	bork@sigcorp.com	Expiration Date	4/30/2024
		Quote Number	00000105

2024 vCISO

Quote To Name	Wharton County Junior College	Contact Name	Amanda Allen
Address	911 Boling Highway Wharton, TX 77488-3298	Phone	(979) 532-4560
		Email	allena@wcjc.edu

Proposed Services

Service	Sales Price	Quantity	Total Price	Line Item Description
Cybersecurity Strategic Consulting	$6,720.00	6.00	$40,320.00	vCISO Services

**Total Price shown is an estimated amount unless the Scope of Services below indicates an alternative basis.*

Total Price $40,320.00

Scope of Services

Under the terms of this Statement of Work, Strata Information Group, Inc. (SIG) will provide services for the staff of Wharton County Junior College (WCJC), as directed to perform the work outlined below. WCJC, as a member of the Educational and Institutional Cooperative Services (E&I), will utilize E&I's Master Agreement Contract number CNR01502, dated May 1, 2020. SIG Cyber supports internal teams with key security initiatives and program development, however, it should be noted that internal teams at WCJC are ultimately responsible for the security of the WCJC environment (in alignment with FTC Safeguard requirements) as they provide hands on management of security controls and budgeting for internal security initiatives.

Description of Work:

The proposed service is for 6 hours of engagement (24 hours per month) per week for 6 months. Wharton County Junior College will have the option to extend the service for an additional 6 months at their discretion provided they give 6 weeks' notice before the end of the agreement (to allow SIG to staff for the engagement).

The engagement is to be conducted via remote connection.

These services are subject to change depending on WCJC's priorities, needs, and availability of staff and systems.

Detailed tasks:
SIG Cyber proposes a six-month extension (from 2/26 to 8/31) to its existing agreement to continue assisting Wharton County Junior College (WCJC) with vCISO services that provide strategic direction for its security program. Our continued focus for this engagement will be around compliance with the recently announced FTC Safeguard rule requirements as well as Texas Administrative Code 202 for higher education. SIG Cyber will continue working with WCJC staff to analyze compliance with the FTC Safeguards and Texas Administrative Code 202 and assist with development of policies and procedures to align with these frameworks. SIG Cyber supports internal teams with key security initiatives and program development, however, it should be noted that internal teams at WCJC are ultimately responsible for the security of the WCJC environment as they provide hands on management of security controls and budgeting for internal security initiatives.

A prioritized roadmap of security projects has been created during our previous statement of work and SIG Cyber will continue to support WCJC staff with completion of these projects. SIG Cyber will also continue working with internal teams and third parties to address technical gaps in the WCJC program. Regular cadence and status calls will be held with WCJC staff to review status and adjust priorities. This will ensure that SIG Cyber is in alignment with internal team members on security projects. SIG will continue working to remediate gaps in compliance against the 9 elements that the

Strata Information Group, Inc.
3935 Harney Street, Suite 203
San Diego, CA 92110
United States

FTC has stipulated must be included in an organization written information security program (WISP). Those 9 elements are highlighted here (the C.F.R. numbers referenced below are direct references to the FTC Safeguards rule published online):

• Element 1: Designates a qualified individual responsible for overseeing and implementing the institutions or servicer's information security program and enforcing the information security program (16 C.F.R. 314.4(a)).

• Element 2: Provides for the information security program to be based on a risk assessment that identifies reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information (as the term customer information applies to the institution or servicer) that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information, and assesses the sufficiency of any safeguards in place to control these risks (16 C.F.R. 314.4(b)).

• Element 3: Provides for the design and implementation of safeguards to control the risks the institution or servicer identifies through its risk assessment (16 C.F.R. 314.4(c)). At a minimum, the written information security program must address the implementation of the minimum safeguards identified in 16 C.F.R. 314.4(c)(1) through (8).

• Element 4: Provides for the institution or servicer to regularly test or otherwise monitor the effectiveness of the safeguards it has implemented (16 C.F.R. 314.4(d)).

• Element 5: Provides for the implementation of policies and procedures to ensure that personnel can enact the information security program (16 C.F.R. 314.4(e)).

• Element 6: Addresses how the institution or servicer will oversee its information system service providers (16 C.F.R. 314.4(f)).

• Element 7: Provides for the evaluation and adjustment of its information security program considering the results of the required testing and monitoring; any material changes to its operations or business arrangements; the results of the required risk assessments; or any other circumstances that it knows or has reason to know may have a material impact the information security program (16 C.F.R. 314.4(g)).

• Element 8: For an institution or servicer maintaining student information on 5,000 or more consumers, addresses the establishment of an incident response plan (16 C.F.R. 314.4(h)).

• Element 9: For an institution or servicer maintaining student information on 5,000 or more consumers, addresses the requirement for its Qualified Individual to report regularly and at least annually to those with control over the institution on the institution's information security program (16 C.F.R. 314.4(i)).

Key Assumptions & Project Completion Criteria

SIG will fulfill its obligation described in this Proposal for Services when the first of the following occurs:

- SIG completes and delivers the tasks described in the "Scope of Services" above
- SIG provides the number of hours of services specified in this Proposal for Services
- The service period specified in a mutually-agreed Statement of Work ends

- The price(s) quoted in this proposal are valid for 90 calendar days.
- Costs are based on client current contract rates; rates may increase based on the term of the underlying contract.
- SIG will bill monthly for services. Payments are due Net 30 days.
- Costs exclude all state taxes, if applicable, unless otherwise noted.
- Includes engagement management, preparation time, labor, and the development of engagement reports.
- All prices are quoted in USD, unless otherwise noted.

This Proposal for Services is for discussion or budgeting purposes only and shall not be binding unless subject to a written agreement executed between SIG and Client. The price(s) included in this proposal are good through the expiration date shown above.
If you are ready to receive an executable agreement, contact the individual listed in the Prepared By section above.