

D.1.1. Evaluation of Network Security / D.1.2. Audit of Network Security / D.1.3. Vulnerability Testing								
Milestone Description	Number of Devices	Duration	Hours	Hourly Rate	Year 1	Year 2	Year 3	Total Cost - 3 Years
Project Kick-Off (One Time Effort)		5 - 8 days	24	\$124.00	\$2,976.00	\$2,976.00	\$2,976.00	\$8,928.00
Project Award		3 - 5 days						
Kickoff Meeting		Kickoff Date	2					
Project Schedule, RoE (Rules of Engagement) document review and sign-off		2 - 3 days	12					
Establish a VA and PT Environment		0.5 Day	10					
A. Agency / Department - wide Information Technology Risk Assessment*		25-30 days	320	\$124.00	\$39,680.00	\$37,696.00	\$36,565.12	\$113,941.12
Comprehensive Assessment								
• Identify hazards and risk factors that have the potential to cause harm (hazard identification).								
• Analyze and evaluate the risk associated with that hazard (risk analysis, and risk evaluation).								
• Determine appropriate ways to eliminate the hazard or control the risk when the hazard cannot be eliminated (risk control).								
B. Penetration Testing								
Option A - Small Size Agency / Department		8-10 days	120	\$124.00	\$14,880.00	\$14,136.00	\$13,711.92	\$42,727.92
External vulnerability testing - the ability of an attacker to penetrate systems and network externally, without providing any additional information that would be available to a bad actor	Up to 25 External IPs							
Internal Network Pentest - the ability to perform lateral movement once inside the network to identify and document anomalies within the network such as missing patches, configuration flaws, use of default or weak passwords and password policies, identifiable vulnerabilities	Up to 2000 Internal IPs							
Hosted Application Pen Testing – review the security level internally hosted applications, including the accessibility both internally and externally to test the application security and code vulnerability.	Up to 5 Web Applications							

D.1.1. Evaluation of Network Security / D.1.2. Audit of Network Security / D.1.3. Vulnerability Testing

Milestone Description	Number of Devices	Duration	Hours	Hourly Rate	Year 1	Year 2	Year 3	Total Cost - 3 Years
Social Engineering - Phishing campaign that will span across multiple pools of users. The campaign will begin with a baseline and ease of identification increasing in difficulty throughout the engagement to complex identification. Phishing campaign that will span across multiple pools of users.	Up to 25 Users							
All other SOWs items including Password cracking, Network Packets Capture Assessment/Review, Workstation and Server hardening tests, Monitoring tools assessment, and any other tests that mutually agreed upon discussion with Agency / Department and security stakeholders								
B. Training: A critical component of this RFP is to provide quality cross-training of the security team. This follows the model of mixing red and blue teams to form something the industry is calling a purple team. To facilitate that security teams would like to participate in the actual pen test. This includes but is not limited to using conference software (Zoom or Webex) to watch as tests are run, communicating with pen testers about their methodology and reasoning, and knowledge transfer from pen tester to the security team.	Up to 4 Hours (Remote Training Session) Up to 5 Technical Team Members							
C. Reporting and Documentation Requirements a. Scoping sessions to determine breadth, depth, and rules of engagement of each type of test laying out mutual understanding of the assessment b. Impact and Comprehensive and timely outcomes report i. Audit trail of all tests including outcomes ii. Path and Methods for all successful attacks iii. Remediation/Fix Report for exposures and best practice recommendations c. Recommendations for risk mitigation, industry-standard fixes, and retesting process d. All reports must be visibly marked as "Confidential" e. All documentation beyond the initial RFP is to be considered confidential. This includes all reports whether compiled or generated by a tool. f. An executive summary of the testing, findings, and recommendations								
Option B - Medium Size Agency / Department**		16-20 days	300	\$122.00	\$36,600.00	\$34,770.00	\$33,726.90	\$105,096.90
External vulnerability testing - the ability of an attacker to penetrate systems and network externally, without providing any additional information that would be available to a bad actor	Up to 250 External IPs							

D.1.1. Evaluation of Network Security / D.1.2. Audit of Network Security / D.1.3. Vulnerability Testing								
Milestone Description	Number of Devices	Duration	Hours	Hourly Rate	Year 1	Year 2	Year 3	Total Cost - 3 Years
Internal Network Pentest - the ability to perform lateral movement once inside the network to identify and document anomalies within the network such as missing patches, configuration flaws, use of default or weak passwords and password policies, identifiable vulnerabilities	Up to 8000 Internal IPs							
Hosted Application Pen Testing – review the security level internally hosted applications, including the accessibility both internally and externally to test the application security and code vulnerability.	Up to 10 Web Applications							
Social Engineering - Phishing campaign that will span across multiple pools of users. The campaign will begin with a baseline and ease of identification increasing in difficulty throughout the engagement to complex identification. Phishing campaign that will span across multiple pools of users.	Up to 100 Users							
All other SOWs items including Password cracking, Network Packets Capture Assessment/Review, Workstation and Server hardening tests, Monitoring tools assessment, and any other tests that mutually agreed upon discussion with Agency / Department and security stakeholders								
B. Training: A critical component of this RFP is to provide quality cross training of the security team. This follows the model of mixing red and blue teams to form something the industry is calling a purple team. To facilitate that security teams would like to participate in the actual pen test. This includes but is not limited to using conference software (Zoom or Webex) to watch as tests are run, communicating with pen testers about their methodology and reasoning, and knowledge transfer from pen tester to security team.	Up to 8 Hours (Remote Training Session) Up to 10 Technical Team Members							

D.1.1. Evaluation of Network Security / D.1.2. Audit of Network Security / D.1.3. Vulnerability Testing								
Milestone Description	Number of Devices	Duration	Hours	Hourly Rate	Year 1	Year 2	Year 3	Total Cost - 3 Years
C. Reporting and Documentation Requirements a. Scoping sessions to determine breadth, depth, and rules of engagement of each type of test laying out mutual understanding of the assessment b. Impact and Comprehensive and timely outcomes report i. Audit trail of all tests including outcomes ii. Path and Methods for all successful attacks iii. Remediation/Fix Report for exposures and best practice recommendations c. Recommendations for risk mitigation, industry standard fixes and retesting process d. All reports must be visibly marked as "Confidential" e. All documentation beyond the initial RFP is to be considered confidential. This includes all reports whether compiled or generated by a tool. f. An executive summary of the testing, findings, and recommendations								
Option C - Large Size Agency / Department**		35-40 days	500	\$119.00	\$59,500.00	\$56,525.00	\$54,829.25	\$170,854.25
External vulnerability testing - the ability of an attacker to penetrate systems and network externally, without providing any additional information that would be available to a bad actor	Up to 500 External IPs							
Internal Network Pentest - the ability to perform lateral movement once inside the network to identify and document anomalies within the network such as missing patches, configuration flaws, use of default or weak passwords and password policies, identifiable vulnerabilities	Up to 15000 Internal IPs							
Hosted Application Pen Testing – review the security level internally hosted applications, including the accessibility both internally and externally to test the application security and code vulnerability.	Up to 50 Web Applications							
Social Engineering - Phishing campaign that will span across multiple pools of users. The campaign will begin with a baseline and ease of identification increasing in difficulty throughout the engagement to complex identification. Phishing campaign that will span across multiple pools of users.	Up to 250 Users							
All other SOWs items including Password cracking, Network Packets Capture Assessment/Review, Workstation and Server hardening tests, Monitoring tools assessment, and any other tests that mutually agreed upon discussion with Agency / Department and security stakeholders								

D.1.1. Evaluation of Network Security / D.1.2. Audit of Network Security / D.1.3. Vulnerability Testing								
Milestone Description	Number of Devices	Duration	Hours	Hourly Rate	Year 1	Year 2	Year 3	Total Cost - 3 Years
B. Training: A critical component of this RFP is to provide quality cross training of the security team. This follows the model of mixing red and blue teams to form something the industry is calling a purple team. To facilitate that security teams would like to participate in the actual pen test. This includes but is not limited to using conference software (Zoom or Webex) to watch as tests are run, communicating with pen testers about their methodology and reasoning, and knowledge transfer from pen tester to security team.	Up to 16 Hours (Remote Training Session) Up to 15 Technical Team Members							
C. Reporting and Documentation Requirements a. Scoping sessions to determine breadth, depth, and rules of engagement of each type of test laying out mutual understanding of the assessment b. Impact and Comprehensive and timely outcomes report i. Audit trail of all tests including outcomes ii. Path and Methods for all successful attacks iii. Remediation/Fix Report for exposures and best practice recommendations c. Recommendations for risk mitigation, industry standard fixes and retesting process d. All reports must be visibly marked as "Confidential" e. All documentation beyond the initial RFP is to be considered confidential. This includes all reports whether compiled or generated by a tool. f. An executive summary of the testing, findings, and recommendations								
C. On-Demand Services***								
1. Consultation (Remote, for onsite - travel charges will be additional)				\$134.00	TBD	TBD	TBD	TBD
2. Small-scale testing services, as needed, to augment ongoing audits or testing				\$134.00	As per scope	As per scope	As per scope	As per scope
3. Ability to use firm during normal business hours				\$134.00	Yes	Yes	Yes	
Optional Cost - Estimated Travel Cost (1 Trip - 3 to 4 days) - If required				\$1,250.00	TBD	TBD	TBD	TBD
Total Cost (Varies based upon selected options)					TBD	TBD	TBD	TBD

Assumptions:

*Based upon publicly available information, we have estimated the scope for "A. Comprehensive Assessment" for Year 1. If the Comprehensive Assessment scope will be reduced to limited for Year 2 and Year 3 then we will adjust our pricing accordingly once, we know an exact limited scope. Meanwhile, we will offer 5% discount for Comprehensive scope for year 2 and an additional 3% discount as long as scope and size remain same as year 1.

** Due to the lack of exact assets/devices information about each Agency / Department, GSG would like to propose Three Options for "B. Penetration Testing" based upon size/scope of each Agency / Department. Each Option for Agency / Department size included with ceiling limits from numbers of devices/users. However, if these options are not the best fit then we are open to consider other option as well. Above hours are based upon scope and clarification response provided in RFP and Q&A document. If any of the scope and/or quantities of devices increases, then our effort will be increased appropriately.

*** For "C. On-Demand Services", we are providing an hourly rate for "Consultation" OR "Small-scale testing services" on as-needed basis to augment ongoing audits or testing for Year 1, 2, and 3. We also agree to provide our resources during normal business hours. All services will be remote. However, if onsite services are required then travel cost will be additional cost.

- GSG has a large pool of Cybersecurity experts, and we are planning to propose 2-4 resources team for each Agency / Department depending upon criteria including project schedule, stakeholder availability, etc. Some tasks may be accomplished in parallel depending upon information, systems, and stakeholders' availability. -
- For effective project scheduling, State management need to provide access to all proprietary information, applications, and systems including third parties necessary to the success of this project and all State stakeholders should be available as needed to ensure the timeliness and success of this project. -
- Customer will provide access to all proprietary information, applications, and systems including third parties necessary to the success of this project. -
- During this engagement, any vulnerabilities, sensitive data, or configuration data found will not be disclosed except to specified Customer staff. -
- The GSG Cyber team believes that entire scope of work can be successfully accomplished remotely utilizing remote access and virtual meeting/conference(s). If for any reason the Cybersecurity testing scope requires onsite testing effort for tasks such as wireless testing or physical security testing, then we would determine specific need for onsite work and corresponding accurate travel cost. We usually charge for actual travel cost as per IRS / Federal Travel Regulation. For understanding purpose, 1 trip of 4 days travel costs around \$1250 including flight, lodging, meals, transportation, etc.-
- During this effort, GSG will not be responsible for negotiations with hardware, software, or other vendors, or any other contractual relationship between the State and third parties. -
- Customer management will ensure that appropriate personnel are available to meet with GSG team, as necessary to ensure the success of this project. -
- GSG will not be obligated to extend engagements when delays result from the State's inability to meet stated prerequisites prior to an engagement, nor when delays result from State personnel not being available to provide required support to the success of this project-
- Servers' OS installation and configuration is not part of this Comprehensive Assessment scope.
- The proposal will be valid for 120 days.

D.1.4. Technical Installation Services / D.1.5. Technical Maintenance Services

Price Sheet for Services						
SERVICE NAME	SERVICE DESCRIPTION (provide detailed service features)	Service Number (optional)	List COST Per Unit	Unit of Issue	Discount % off MSRP/List (2 decimals)	Customer Price EACH/Per Unit
A. Resource, Asset, and Data Protection and Tracking a. Identify and manage configuration of software b. Manage software security vulnerabilities c. Protect and manage sensitive data d. Prevent and mitigate loss or breach of classified information e. Media protection sanitization, marking, storage, transport, and use f. Asset discovery g. Data backup h. Data replication i. System recovery j. Spam protection k. Input validation l. Error handling	IT Asset Management Analyst	Mid-Level	\$ 149.00	Hourly Rate	15.00%	\$127.60
		Senior	\$ 171.00	Hourly Rate	15.00%	\$146.44
		Lead	\$ 229.00	Hourly Rate	15.00%	\$196.11

Price Sheet for Services						
SERVICE NAME	SERVICE DESCRIPTION (provide detailed service features)	Service Number (optional)	List COST Per Unit	Unit of Issue	Discount % off MSRP/List (2 decimals)	Customer Price EACH/Per Unit
m. Flaw remediation n. Memory protection o. Vulnerability remediation p. Malicious code protection q. Virtual Private Networks (VPN) r. Virtual system and infrastructure design, implementation, management, and support services s. Encryption t. Cryptography, including key establishment and management u. Data leak protection (DLP) v. Configuration Management Database (CMDB) w. Maintenance tools	Network Security Engineer	Mid-Level	\$ 149.00	Hourly Rate	15.00%	\$127.60
		Senior	\$ 171.00	Hourly Rate	15.00%	\$146.44
		Lead	\$ 229.00	Hourly Rate	15.00%	\$196.11
B. Endpoint, Network, and Cloud Security a. Provide protection of data and services for user devices, network components, applications, and virtual/cloud systems. b. Port and service lockdown c. Application portioning d. Security function isolation e. Network disconnect f. Transmission confidentiality and integrity g. Time synchronization h. Access control, including port security and MAC address filtering i. Network interface management j. Network boundary protection k. Network segmentation and segregation l. Network monitoring m. Network mapping n. Remote access security o. Network capability and stress testing p. Cloud compliance with cybersecurity framework standards (ISO, NIST, etc.) q. Secure file sharing	Network Engineer	Mid-Level	\$ 171.00	Hourly Rate	15.00%	\$146.44
		Senior	\$ 217.00	Hourly Rate	15.00%	\$185.83
		Lead	\$ 263.00	Hourly Rate	15.00%	\$225.23
	Endpoint Security Engineer	Mid-Level	\$ 171.00	Hourly Rate	15.00%	\$146.44
		Senior	\$ 217.00	Hourly Rate	15.00%	\$185.83
		Lead	\$ 263.00	Hourly Rate	15.00%	\$225.23
	Endpoint Protection Security Architect	Mid-Level	\$ 171.00	Hourly Rate	15.00%	\$146.44
		Senior	\$ 217.00	Hourly Rate	15.00%	\$185.83
		Lead	\$ 263.00	Hourly Rate	15.00%	\$225.23
	Endpoint Security Consultant	Mid-Level	\$ 171.00	Hourly Rate	15.00%	\$146.44
		Senior	\$217.00	Hourly Rate	15.00%	\$185.83
		Lead	\$ 263.00	Hourly Rate	15.00%	\$225.23
C. Authentication and Authorization a. User and system identity management b. Credential management c. User permissions management d. Configuration management e. Identity proofing f. Identity theft protection g. Multi-Factor Authentication (MFA)	Cybersecurity Network Administrator	Mid-Level	\$ 149.00	Hourly Rate	15.00%	\$127.60
		Senior	\$ 171.00	Hourly Rate	15.00%	\$146.44
		Lead	\$ 229.00	Hourly Rate	15.00%	\$196.11

Price Sheet for Services						
SERVICE NAME	SERVICE DESCRIPTION (provide detailed service features)	Service Number (optional)	List COST Per Unit	Unit of Issue	Discount % off MSRP/List (2 decimals)	Customer Price EACH/Per Unit
h. Hardware inventory management i. Software inventory management j. Identity and Authentication Management (IAM) k. Privileged Identity Management and Privileged Access Management (PIM/PAM) l. Password management	System Administrator	Mid-Level	\$ 149.00	Hourly Rate	15.00%	\$127.60
		Senior	\$ 171.00	Hourly Rate	15.00%	\$146.44
		Lead	\$ 229.00	Hourly Rate	15.00%	\$196.11
D. Forensic and Incident Response a. Baseline establishment b. Network Architecture Documentation c. Change control d. Incident response planning and preparedness e. Incident response management and recovery f. Forensic investigative and examination g. Intrusion Protection/Prevention Systems (IPS) h. Firewalls, include Web application firewalls (WAF) a. Incident response and mitigation b. Incident reporting	Cybersecurity Forensic and Incident response Officer	Mid-Level	\$ 171.00	Hourly Rate	15.00%	\$146.44
		Senior	\$ 217.00	Hourly Rate	15.00%	\$185.83
		Lead	\$ 263.00	Hourly Rate	15.00%	\$225.23
	Forensic Analyst	Mid-Level	\$ 171.00	Hourly Rate	15.00%	\$146.44
		Senior	\$ 217.00	Hourly Rate	15.00%	\$185.83
		Lead	\$ 263.00	Hourly Rate	15.00%	\$225.23
	Security Analyst	Mid-Level	\$ 171.00	Hourly Rate	15.00%	\$146.44
		Senior	\$ 217.00	Hourly Rate	15.00%	\$185.83
		Lead	\$ 263.00	Hourly Rate	15.00%	\$225.23
E. Training and Awareness a. Provide cybersecurity awareness training to prevent phishing and other attacks b. Cybersecurity program evaluation c. Response planning and communications d. Cybersecurity improvement e. Contingency planning and training f. Incidence response training g. Cybersecurity training software and services	Cybersecurity Trainer	Mid-Level	\$ 149.00	Hourly Rate	15.00%	\$127.60
		Senior	\$ 171.00	Hourly Rate	15.00%	\$146.44
		Lead	\$ 229.00	Hourly Rate	15.00%	\$196.11
F. Information Technology Risk Assessment Comprehensive Assessment Cybersecurity risk assessment and management Payment Card Industry Assessment Security Audits Information Assurance	Cybersecurity Risk Assessor	Mid-Level	\$ 149.00	Hourly Rate	15.00%	\$127.60
		Senior	\$ 171.00	Hourly Rate	15.00%	\$146.44
		Lead	\$ 229.00	Hourly Rate	15.00%	\$196.11
	Cybersecurity Auditor	Mid-Level	\$ 149.00	Hourly Rate	15.00%	\$127.60
		Senior	\$ 171.00	Hourly Rate	15.00%	\$146.44
		Lead	\$ 229.00	Hourly Rate	15.00%	\$196.11
G. Penetration Testing • External vulnerability testing - the ability of an attacker to penetrate systems and network externally, without providing any additional information that would be	Internal Penetration Tester	Mid-Level	\$ 149.00	Hourly Rate	15.00%	\$127.60

Price Sheet for Services

SERVICE NAME	SERVICE DESCRIPTION (provide detailed service features)	Service Number (optional)	List COST Per Unit	Unit of Issue	Discount % off MSRP/List (2 decimals)	Customer Price EACH/Per Unit
<p>available to a bad actor</p> <ul style="list-style-type: none"> • Internal Network Pentest - the ability to perform lateral movement once inside the network to identify and document anomalies within the network such as missing patches, configuration flaws, use of default or weak passwords and password policies, identifiable vulnerabilities • Hosted Application Pen Testing – review the security level internally hosted applications, including the accessibility both internally and externally to test the application security and code vulnerability. • Social Engineering - Phishing campaign that will span across multiple pools of users. <p>The campaign will begin with a baseline and ease of identification increasing in difficulty throughout the engagement to complex identification. Phishing campaign that will span across multiple pools of users.</p> <ul style="list-style-type: none"> • All other SOWs items including Password cracking, Network Packets Capture Assessment/Review, Workstation and Server hardening tests, Monitoring tools assessment, and any other tests that mutually agreed upon discussion with school district and security stakeholders • C. Reporting and Documentation Requirements <p>a. Scoping sessions to determine breadth, depth, and rules of engagement of each type of test laying out mutual understanding of the assessment</p> <p>b. Impact and Comprehensive and timely outcomes report</p> <p>i. Audit trail of all tests including outcomes</p> <p>ii. Path and Methods for all successful attacks</p> <p>iii. Remediation/Fix Report for exposures and best practice recommendations</p> <p>c. Recommendations for risk mitigation, industry standard fixes and retesting process</p> <p>d. All reports must be visibly marked as “Confidential”</p> <p>e. All documentation beyond the initial RFP is to be considered confidential. This includes all reports whether compiled or generated by a tool.</p> <p>f. An executive summary of the testing, findings, and recommendations</p> <p>C. Reporting and Documentation Requirements</p> <p>a. Scoping sessions to determine breadth, depth, and rules of engagement of each type of test laying out mutual understanding of the assessment</p> <p>b. Impact and Comprehensive and timely outcomes report</p> <p>i. Audit trail of all tests including outcomes</p> <p>ii. Path and Methods for all successful attacks</p> <p>iii. Remediation/Fix Report for exposures and best practice recommendations</p> <p>c. Recommendations for risk mitigation, industry standard fixes and retesting process</p> <p>d. All reports must be visibly marked as “Confidential”</p> <p>e. All documentation beyond the initial RFP is to be considered confidential. This</p>		Senior	\$ 171.00	Hourly Rate	15.00%	\$146.44
		Lead	\$ 229.00	Hourly Rate	15.00%	\$196.11
	External Penetration Tester	Mid-Level	\$ 149.00	Hourly Rate	15.00%	\$127.60
		Senior	\$ 171.00	Hourly Rate	15.00%	\$146.44
		Lead	\$ 229.00	Hourly Rate	15.00%	\$196.11
	Cybersecurity Tech Lead	Mid-Level	\$ 149.00	Hourly Rate	15.00%	\$127.60
		Senior	\$ 171.00	Hourly Rate	15.00%	\$146.44
		Lead	\$ 229.00	Hourly Rate	15.00%	\$196.11
	Social Engineering Tester	Mid-Level	\$ 149.00	Hourly Rate	15.00%	\$127.60
		Senior	\$ 171.00	Hourly Rate	15.00%	\$146.44
		Lead	\$ 229.00	Hourly Rate	15.00%	\$196.11
	Technical Writer	Mid-Level	\$ 149.00	Hourly Rate	15.00%	\$127.60

Price Sheet for Services						
SERVICE NAME	SERVICE DESCRIPTION (provide detailed service features)	Service Number (optional)	List COST Per Unit	Unit of Issue	Discount % off MSRP/List (2 decimals)	Customer Price EACH/Per Unit
includes all reports whether compiled or generated by a tool. f. An executive summary of the testing, findings, and recommendations		Senior	\$ 171.00	Hourly Rate	15.00%	\$146.44
		Lead	\$ 229.00	Hourly Rate	15.00%	\$196.11
H. Policy and Procedure Development a. Governance development, including policy, processes, and procedures b. System maintenance policy and procedures	Technical writer	Mid-Level	\$ 149.00	Hourly Rate	15.00%	\$127.60
		Senior	\$ 171.00	Hourly Rate	15.00%	\$146.44
		Lead	\$ 229.00	Hourly Rate	15.00%	\$196.11
	Cybersecurity Assessor	Mid-Level	\$ 149.00	Hourly Rate	15.00%	\$127.60
		Senior	\$ 171.00	Hourly Rate	15.00%	\$146.44
		Lead	\$ 229.00	Hourly Rate	15.00%	\$196.11
	Cybersecurity Auditor	Mid-Level	\$ 149.00	Hourly Rate	15.00%	\$127.60
		Senior	\$ 171.00	Hourly Rate	15.00%	\$146.44
		Lead	\$ 229.00	Hourly Rate	15.00%	\$196.11
I. On-Demand Services 1. Consultation (Remote, for onsite - travel charges will be additional) 2. Small-scale testing services, as needed, to augment ongoing audits or testing 3. Security Information and Event Management services (SIEM)	Cybersecurity Consultant	Mid-Level	\$ 149.00	Hourly Rate	15.00%	\$127.60
		Senior	\$ 171.00	Hourly Rate	15.00%	\$146.44
		Lead	\$ 229.00	Hourly Rate	15.00%	\$196.11
	SIEM Security Architect	Mid-Level	\$ 149.00	Hourly Rate	15.00%	\$127.60
		Senior	\$ 171.00	Hourly Rate	15.00%	\$146.44
		Lead	\$ 229.00	Hourly Rate	15.00%	\$196.11
	SIEM security analyst	Mid-Level	\$ 149.00	Hourly Rate	15.00%	\$127.60
		Senior	\$ 171.00	Hourly Rate	15.00%	\$146.44
		Lead	\$ 229.00	Hourly Rate	15.00%	\$196.11
	IT Cybersecurity engineer	Mid-Level	\$ 149.00	Hourly Rate	15.00%	\$127.60
		Senior	\$ 171.00	Hourly Rate	15.00%	\$146.44
		Lead	\$ 229.00	Hourly Rate	15.00%	\$196.11
	SIEM administrator	Mid-Level	\$ 149.00	Hourly Rate	15.00%	\$127.60
		Senior	\$ 171.00	Hourly Rate	15.00%	\$146.44
		Lead	\$ 229.00	Hourly Rate	15.00%	\$196.11
	Internal Penetration Tester	Mid-Level	\$ 149.00	Hourly Rate	15.00%	\$127.60
		Senior	\$ 171.00	Hourly Rate	15.00%	\$146.44
		Lead	\$ 229.00	Hourly Rate	15.00%	\$196.11
	External Penetration Tester	Mid-Level	\$ 149.00	Hourly Rate	15.00%	\$127.60
		Senior	\$ 171.00	Hourly Rate	15.00%	\$146.44

Price Sheet for Services						
SERVICE NAME	SERVICE DESCRIPTION (provide detailed service features)	Service Number (optional)	List COST Per Unit	Unit of Issue	Discount % off MSRP/List (2 decimals)	Customer Price EACH/Per Unit
		Lead	\$ 229.00	Hourly Rate	15.00%	\$196.11
	Cybersecurity Tech Lead	Mid-Level	\$ 149.00	Hourly Rate	15.00%	\$127.60
		Senior	\$ 171.00	Hourly Rate	15.00%	\$146.44
		Lead	\$ 229.00	Hourly Rate	15.00%	\$196.11
	Social Engineering tester	Mid-Level	\$ 149.00	Hourly Rate	15.00%	\$127.60
		Senior	\$ 171.00	Hourly Rate	15.00%	\$146.44
		Lead	\$ 229.00	Hourly Rate	15.00%	\$196.11
	Technical Writer	Mid-Level	\$ 149.00	Hourly Rate	15.00%	\$127.60
		Senior	\$ 171.00	Hourly Rate	15.00%	\$146.44
		Lead	\$ 229.00	Hourly Rate	15.00%	\$196.11
	Cybersecurity Risk Assessor	Mid-Level	\$ 149.00	Hourly Rate	15.00%	\$127.60
		Senior	\$ 171.00	Hourly Rate	15.00%	\$146.44
		Lead	\$ 229.00	Hourly Rate	15.00%	\$196.11
	Cybersecurity Auditor	Mid-Level	\$ 149.00	Hourly Rate	15.00%	\$127.60
		Senior	\$ 171.00	Hourly Rate	15.00%	\$146.44
		Lead	\$ 229.00	Hourly Rate	15.00%	\$196.11
Additional Discount Based on Aggregate Sales						
	Contract Sales Threshold	Service Category Description	Service Number (if Applicable)	Original Discount	Additional Discount	Total Discount
	\$1,000,000.00	Any	Any	15.00%	3.00%	18.00%

D.1.6. Technical Training Services (current and future needs) / D.1.7. Technical Training Materials				
KnowBe4 – Cybersecurity Training Topics and Price Table				
Features	Silver	Gold	Platinum	Diamond
Unlimited Phishing Security Tests	✓	✓	✓	✓
Automated Security Awareness Program (ASAP)	✓	✓	✓	✓
Security 'Hints & Tips'	✓	✓	✓	✓
Training Access Level I	✓	✓	✓	✓
Automated Training Campaigns	✓	✓	✓	✓
Brandable Content	✓	✓	✓	✓
Assessments	✓	✓	✓	✓
Phish Alert Button	✓	✓	✓	✓
Phishing Reply Tracking	✓	✓	✓	✓
Active Directory Integration (ADI)	✓	✓	✓	✓
SSO/SAML Integration	✓	✓	✓	✓
Industry Benchmarking	✓	✓	✓	✓
Virtual Risk Officer™	✓	✓	✓	✓
Advanced Reporting	✓	✓	✓	✓
Training Access Level II		✓	✓	✓
Monthly Email Exposure Check		✓	✓	✓
Vishing Security Test		✓	✓	✓
Smart Groups			✓	✓
Reporting APIs			✓	✓
User Event API			✓	✓
Security Roles			✓	✓
Social Engineering Indicators (SEI)			✓	✓

USB Drive Test			✓	✓
Priority Level Support			✓	✓
Training Access Level III				✓
AI-Driven Phishing				✓
AIDA™ Artificial Intelligence-driven Agent BETA				✓
Compliance Plus - Optional Add-on	✓	✓	✓	✓
PhishER™ - Optional Add-on	✓	✓	✓	✓

Discounted Pricing By Seat 1 Year	Silver	Gold	Platinum	Diamond
25-50	\$17.10	\$20.66	\$24.23	\$28.98
51-100	\$15.20	\$18.29	\$21.38	\$26.13
101-500	\$12.35	\$14.73	\$17.10	\$21.85
501-1000	\$11.40	\$13.54	\$15.68	\$20.43
1001-2000	\$10.45	\$12.35	\$14.25	\$19.00
2001-3000	\$9.50	\$11.16	\$12.83	\$17.58
3001-5000	\$8.55	\$9.98	\$11.40	\$16.15

Assumptions:

1. Above pricing by seat include a 5% discount on MSRP Price.
2. KnowBe4 offers SaaS subscription priced per seat, per year. It offers Silver, Gold, Platinum, or Diamond levels to meet an organization's needs, comprised of three levels of training access and increasingly powerful features.
3. KnowBe4 offers attractive discounts for a 3-year contract.
4. Pricing in US\$ as per Jan 2022 for North America. List pricing may be modified at any time.