

Exhibit 2: Attachment 2.1 Version 2.1

Texas Department of Information Resources

Data Center Services Request for Offer

DCS Security Operations Services

Pricing and Volumes

Attachment 2.1

DCS Security Operations Services

Respondent:

SAIC

Date:

2/25/2020

Respondent Guidelines

This Attachment contains specific functional requirements that the Respondent must meet in order to perform the requested Services. The Respondent must respond to the requirements contained in this Attachment according to the instructions provided below. The Respondent's Response must be in the prescribed format.

Respondent Instructions

Respondent shall complete this Pricing Form.

Respondent inputs are required only in blue highlighted cells.

All Charges shall be entered as whole numbers with no rounding.

The Contract Years are aligned with the State Fiscal Year (September 1st - August 31st).

The Commencement Date for these Services will be September 1, 2020.

Pricing Instructions - Inflation

Respondent shall include any anticipated inflation in its submitted pricing, including Option Years and in the amount assumed annually in the Summary Charges.

Pricing Instructions - Asset Strategy

Respondent shall assume the asset strategy reflected in the **Attachment 2.2 Financial Responsibility Matrix**.

Tab Descriptions

Pricing Bridge

This is a Repondent completed worksheet to document the material items affecting the change in price from a prior submission to the current submission.

1. Summary Charges

This is a formula-driven summary of the Charges.

2. Run Charges

Fill out blue highlighted areas of worksheet with Annual Fixed Charges for each service per period. These Charges will fully compensate Respondent for all Steady State Run Services. The SIEM Service Charge is formula driven based on completion of the Unit Rate per period in the table below the Total Charges table. Unit Rates - Fill out blue highlighted areas of worksheet with monthly unit rates for SIEM Services for each Contract Year.

2a. Optional Services

Fill out blue highlighted areas of worksheet with SIEM Ingested Data rates per volume tier.

3. Transition

Fill out blue highlighted areas of worksheet with beginning and completion dates and Charges for each Transition Milestone. Transition Milestone requirements are documented in Exhibit 1.

4. Transformation

Fill out blue highlighted areas of worksheet with beginning and completion dates and Charges for each Transformation Project. Transformation Project requirements are documented in Exhibit 1.

5. Rate Card

Fill out Table 1 blue highlighted cells with the rates (inclusive of travel) for each Resource Category. Fill out Table 1 blue highlighted cells with the proposed additional Resource Category(s) (if necessary) and rates (inclusive of travel). Fill out Table 2 blue highlighted cells to describe the proposed additional Resouce Categories listed in the first table.

6. Assets

Fill out blue highlighted areas of worksheet to indicate if Respondent will retain hardware and provided estimated fair market value buyout of each asset. NOTE: DIR has provided an initial asset list. Additional data may be added throughout the procurement process.

7. Software

Fill out blue highlighted areas of worksheet to indicate if Respondent will retain software. NOTE: DIR has provided an initial asset list. Additional data may be added throughout the procurement process.

8. Contracts

Fill out blue highlighted areas of worksheet to indicate if Respondent will retain third party contract. NOTE: DIR has provided an initial asset list. Additional data may be added throughout the procurement process.

Appendix

The tabs in this Appendix section must be completed by Respondent. These tabs are for informational purposes during the procurement process.

A1. Assumptions

This form is for informational purposes only. The Respondent is to list all assumptions associated with the Charges and Services within the scope of the RFO. The Respondent is to provide the degree of impact on the price (High, Medium, Low, Not Applicable) and the related SOW section of the assumption.

A2. Staffing

This form is for informational purposes only. Fill out blue highlighted areas of worksheet with average FTE counts for each SOW Service per period.

A3. SOW Charges

This form is for informational purposes only. Fill out blue highlighted areas of worksheet with Charges for each SOW Service per period. Fill out blue highlighted areas of worksheet with key cost drivers for each service (e.g., devices monitored, customers, software licenses, incidents, sites, etc). DIR may convert fixed charges to variable as part of final negotiations based on variability of cost to support service. Identification of key cost drivers will help facilitate this decision.

A4. Transition BOM

Fill out blue highlighted areas of worksheet for all hardware and software included in Transition Charges. Respondent may add (insert) additional rows as necessary. Transition Bill of Materials are incremental to those indicated as being retained by the Respondent on the Assets (Tab 6) and Software (Tab 7). Hardware purchases must include five years of maintenance in Charges. Annual recurring Software License Charges, after the initial year of purchase, must be included in Tab A5 "Run BOM" if retained past Transition and reflected in Tab 2 "Run Charges". Transition Hardware and Software purchases are owned by Respondent and must be transferrable to DIR.

A5. Run BOM

This form is for informational purposes only. Fill out blue highlighted areas of worksheet for all hardware and software included in Steady State Run Charges. Respondent may add (insert) additional rows as necessary. Bill of Materials are incremental to those indicated as being retained by the Respondent on the Asset (Tab 6) and Software (Tab 7) and the BOM identified in Transition Services (tab A4). Hardware purchases must include five years of maintenance in Charges. Annual recurring Software License Charges, after the initial year of purchase, must be included annually in in Tab 2 "Run Charges". Steady State Hardware and Software purchases are owned by Respondent and must be transferrable to DIR.

A6. Transformation BOM

This form is for informational purposes only. Fill out blue highlighted areas of worksheet for all hardware and software included in Transformation Charges. Respondent may add (insert) additional rows as necessary. Bill of Materials are incremental to those indicated as being retained by the Respondent on the Assets (Tab 6) and Software (Tab 7) and the BOM identified in Transition Services (tab A4) and Run (tab A5). Hardware purchases must include five years of maintenance in Charges. Transformation Hardware and Software purchases are owned by Respondent and must be transferrable to DIR.

Pricing Bridge

Pricing Bridge - Fill out blue highlighted areas of worksheet with Original Proposal Charges and Revised Response adjustments to walk forward the Original Proposal to the Revised Response with descriptions explaining the changes. The Pricing Bridge must be provided separately for Run, Transition, and Transformation Services. A new Pricing Bridge must be completed with prior Pricing Bridge entries exactly as previously submitted.

	Base Term					Option Years				
	Year 1 FY21	Year 2 FY22	Year 3 FY23	Year 4 FY24	4 Year Total	Year 5 (FY23)	Year 6 (FY24)	Year 7 (FY25)	Year 8 (FY26)	8 Year Total
Run Charges										
Original Proposal - Run Services	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -
Transition Charges										
Transition Original Proposal	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -

Charges Summary (\$)

No Data Entry Required

Services	Base Term					Option Years				Total Charges
	Year 1 FY21	Year 2 FY22	Year 3 FY23	Year 4 FY24	Total Base Term	Year 5 FY25	Year 6 FY26	Year 7 FY27	Year 8 FY28	
Transition Services	\$ 2,950,000				\$ 2,950,000					\$ 2,950,000
DCS Security Operations Services	\$ 8,431,248	\$ 8,452,664	\$ 8,374,080	\$ 8,190,496	\$ 33,448,486	\$ 7,850,584	\$ 7,967,000	\$ 7,883,416	\$ 7,904,832	\$ 65,054,317
Total Charges before Transformation	\$ 11,381,248	\$ 8,452,664	\$ 8,374,080	\$ 8,190,496	\$ 36,398,486	\$ 7,850,584	\$ 7,967,000	\$ 7,883,416	\$ 7,904,832	\$ 68,004,317
Optional Transformation Projects:										
1. Advanced Security Analytics, Insights and Alerts	\$ 1,010,000	\$ 420,000	\$ 430,000	\$ 440,000	\$ 2,300,000	\$ 450,000	\$ 460,000	\$ 470,000	\$ 480,000	\$ 4,160,000
2. DCS Identity and Access Management Platform	\$ -	\$ 2,466,564	\$ 1,826,927	\$ 1,854,927	\$ 6,148,418	\$ 1,861,927	\$ 1,841,564	\$ 1,861,927	\$ 1,836,927	\$ 13,550,763
3. Data Loss Prevention Monitoring Services	\$ -	\$ 1,573,086	\$ 1,201,073	\$ 1,211,073	\$ 3,985,232	\$ 1,246,073	\$ 1,420,786	\$ 1,266,073	\$ 1,281,073	\$ 9,199,237
Total Charges	\$ 12,391,248	\$ 12,912,314	\$ 11,832,080	\$ 11,696,496	\$ 48,832,136	\$ 11,408,584	\$ 11,689,350	\$ 11,481,416	\$ 11,502,832	\$ 94,914,317

Steady State Run Services - Annual (\$)

Fill out blue highlighted areas of worksheet with Annual Fixed Charges for each service per period. These Charges will fully compensate Respondent for all Steady State Run Services excluding SIEM SOC Services. The SIEM SOC Service Charge is formula driven based on completion of the Unit Rate per period in the table below the Total Charges table.

Total Charges		Base Term					Option Years				
Resource Unit Description	Metric	Year 1 FY21	Year 2 FY22	Year 3 FY23	Year 4 FY24	Total Base Term	Year 5 FY25	Year 6 FY26	Year 7 FY27	Year 8 FY28	Total Charges
Fixed Charge	Fixed	\$ 5,970,914	\$ 5,965,174	\$ 5,859,434	\$ 5,648,694	\$ 23,444,216	\$ 5,281,626	\$ 5,370,886	\$ 5,260,146	\$ 5,254,406	\$ 44,611,280
SIEM SOC Services	Per aggregate number of IPS, Web Proxy, logical hosts, firewalls, WAFs	\$ 2,460,334	\$ 2,487,490	\$ 2,514,646	\$ 2,541,802	\$ 10,004,270	\$ 2,568,958	\$ 2,596,114	\$ 2,623,270	\$ 2,650,426	\$ 20,443,037
Total Charges		\$ 8,431,248	\$ 8,452,664	\$ 8,374,080	\$ 8,190,496	\$ 33,448,486	\$ 7,850,584	\$ 7,967,000	\$ 7,883,416	\$ 7,904,832	\$ 65,054,317

Unit Rates - Fill out blue highlighted areas of worksheet with monthly unit rates for SIEM SOC Services for each Contract Year.

SIEM SOC Service Variable Charge Calculation		Base Term					Option Years				
		Year 1 FY21	Year 2 FY22	Year 3 FY23	Year 4 FY24	Total Base Term	Year 5 FY25	Year 6 FY26	Year 7 FY27	Year 8 FY28	Total Charges
Estimated Monthly Volume - Devices		9,052	9,052	9,052	9,052		9,052	9,052	9,052	9,052	
Unit Rate	1 - 1,500 Devices	\$ 37.50	\$ 37.90	\$ 38.25	\$ 38.70		\$ 39.05	\$ 39.40	\$ 39.80	\$ 40.20	
	1,501 - 3,000 Devices	\$ 33.50	\$ 33.85	\$ 34.20	\$ 34.55		\$ 34.90	\$ 35.25	\$ 35.60	\$ 35.95	
	3,001 - 4,500 Devices	\$ 30.70	\$ 31.00	\$ 31.30	\$ 31.65		\$ 31.95	\$ 32.30	\$ 32.60	\$ 32.90	
	4,501 - 6,000 Devices	\$ 28.40	\$ 28.70	\$ 29.00	\$ 29.25		\$ 29.55	\$ 29.85	\$ 30.15	\$ 30.45	
	6,001 - 7,500 Devices	\$ 26.35	\$ 26.60	\$ 26.90	\$ 27.15		\$ 27.45	\$ 27.70	\$ 28.00	\$ 28.25	
	7,501 - 9,000 Devices	\$ 24.75	\$ 25.00	\$ 25.25	\$ 25.50		\$ 25.75	\$ 26.00	\$ 26.25	\$ 26.50	
	9,001 - 10,500 Devices	\$ 22.65	\$ 22.90	\$ 23.15	\$ 23.40		\$ 23.65	\$ 23.90	\$ 24.15	\$ 24.40	
	10,501 - 12,000 Devices	\$ 21.35	\$ 21.60	\$ 21.85	\$ 22.10		\$ 22.35	\$ 22.60	\$ 22.85	\$ 23.10	
	12,001 - 13,500 Devices	\$ 20.40	\$ 20.60	\$ 20.80	\$ 21.00		\$ 21.20	\$ 21.40	\$ 21.60	\$ 21.85	
	13,501 - 15,000 Devices	\$ 19.50	\$ 19.70	\$ 19.90	\$ 20.10		\$ 20.30	\$ 20.50	\$ 20.70	\$ 20.90	
15,001 - 17,500 Devices	\$ 18.50	\$ 18.70	\$ 18.90	\$ 19.10		\$ 19.30	\$ 19.50	\$ 19.70	\$ 19.90		

Optional Services (\$)

Fill out blue highlighted areas of worksheet with SIEM Ingested Data rates per volume tier.

Optional Service - SIEM Ingested Data	Base Term					Option Years				
	Year 1 FY21	Year 2 FY22	Year 3 FY23	Year 4 FY24	Total Base Term	Year 5 FY25	Year 6 FY26	Year 7 FY27	Year 8 FY28	Total Charges
Incremental Monthly Volume - Ingested TBs										
Incremental Volume Range 1: additional 0.25 TB per month	\$ 33,405	\$ 33,405	\$ 33,405	\$ 33,405		\$ 33,405	\$ 33,405	\$ 33,405	\$ 33,405	
Incremental Volume Range 2: additional 0.5 TB per month	\$ 66,811	\$ 66,811	\$ 66,811	\$ 66,811		\$ 66,811	\$ 66,811	\$ 66,811	\$ 66,811	
Incremental Volume Range 3: additional 0.75 TB per month	\$ 96,942	\$ 96,942	\$ 96,942	\$ 96,942		\$ 96,942	\$ 96,942	\$ 96,942	\$ 96,942	
Incremental Volume Range 4: additional 1.00 TB per month	\$ 129,256	\$ 129,256	\$ 129,256	\$ 129,256		\$ 129,256	\$ 129,256	\$ 129,256	\$ 129,256	
Incremental Volume Range 5: additional 1.25 TB per month	\$ 161,570	\$ 161,570	\$ 161,570	\$ 161,570		\$ 161,570	\$ 161,570	\$ 161,570	\$ 161,570	
Incremental Volume Range 6: additional 1.5 TB per month	\$ 193,883	\$ 193,883	\$ 193,883	\$ 193,883		\$ 193,883	\$ 193,883	\$ 193,883	\$ 193,883	

Transition Charges (\$)

Fill out blue highlighted areas of worksheet with beginning and completion dates and Charges for each Transition Milestone.

Att 1.1 Ref ID	Description	Beginning Date	Completion Date	Total Charges
1.1	Transition Project Plan	4/1/20	4/21/20	\$ 221,700
1.2	Operational Readiness Assessment	4/1/20	8/2/20	\$ 293,500
1.3.1	SMM Documentation Phase I	4/1/20	4/21/20	\$ 63,828
1.3.2	SMM Documentation Phase II	4/22/20	8/21/20	\$ 97,828
1.3.3	SMM Documentation Phase III	4/24/20	10/30/20	\$ 141,000
1.9	Publish CASB Standards in SMM	4/1/20	8/2/20	\$ 59,260
1.12	SIEM Service Implementation	4/1/20	9/1/20	\$ 1,407,687
1.13	Phase 1 Transition Milestones Complete	4/1/20	9/21/20	\$ 665,197
				\$ -
	FMV Buyout			\$ -
Total Transition Charges				\$ 2,950,000

Optional Transformation Charges (\$)

Fill out blue highlighted areas of worksheet with beginning and completion dates and Charges for each Transformation Project.
Ongoing costs beyond the completion date should be included through the end of Year 8.

SOW Section	Description	Beginning Date	Completion Date	Base Term					Option Years				
				Year 1 FY21	Year 2 FY22	Year 3 FY23	Year 4 FY24	Total Base Term	Year 5 FY25	Year 6 FY26	Year 7 FY27	Year 8 FY28	Total Charges
7.1	Advanced Security Analytics, Insights and Alerts	8/1/20	8/31/28										
	Labor			\$ 1,010,000	\$ 420,000	\$ 430,000	\$ 440,000	\$ 2,300,000	\$ 450,000	\$ 460,000	\$ 470,000	\$ 480,000	\$ 4,160,000
	Hardware			\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -
	Software			\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -
	Other			\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -
	Total			\$ 1,010,000	\$ 420,000	\$ 430,000	\$ 440,000	\$ 2,300,000	\$ 450,000	\$ 460,000	\$ 470,000	\$ 480,000	\$ 4,160,000
7.2	Management Platform	9/1/21	8/31/28										
	Labor			\$ -	\$ 900,728	\$ 912,520	\$ 930,520	\$ 2,743,768	\$ 937,171	\$ 933,930	\$ 948,305	\$ 965,069	\$ 6,528,243
	Hardware			\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -
	Software			\$ -	\$ 922,716	\$ 737,384	\$ 737,384	\$ 2,397,484	\$ 737,384	\$ 737,384	\$ 737,384	\$ 737,384	\$ 5,347,020
	Other			\$ -	\$ 643,120	\$ 177,023	\$ 187,023	\$ 1,007,166	\$ 187,372	\$ 170,250	\$ 176,238	\$ 134,474	\$ 1,675,500
	Total			\$ -	\$ 2,466,564	\$ 1,826,927	\$ 1,854,927	\$ 6,148,418	\$ 1,861,927	\$ 1,841,564	\$ 1,861,927	\$ 1,836,927	\$ 13,550,763
7.3	Monitoring Services	9/1/21	8/31/28										
	Labor			\$ -	\$ 530,530	\$ 546,175	\$ 556,176	\$ 1,632,881	\$ 591,176	\$ 606,718	\$ 611,176	\$ 626,176	\$ 4,068,127
	Hardware			\$ -	\$ 165,136	\$ 5,965	\$ 5,965	\$ 177,066	\$ 5,965	\$ 165,136	\$ 5,965	\$ 5,965	\$ 360,097
	Software			\$ -	\$ 648,930	\$ 648,933	\$ 648,932	\$ 1,946,795	\$ 648,932	\$ 648,932	\$ 648,932	\$ 648,932	\$ 4,542,523
	Other			\$ -	\$ 228,490	\$ -	\$ -	\$ 228,490	\$ -	\$ -	\$ -	\$ -	\$ 228,490
	Total			\$ -	\$ 1,573,086	\$ 1,201,073	\$ 1,211,073	\$ 3,985,232	\$ 1,246,073	\$ 1,420,786	\$ 1,266,073	\$ 1,281,073	\$ 9,199,237
Total Optional Transformation Charges			\$ 1,010,000	\$ 4,459,650	\$ 3,458,000	\$ 3,506,000	\$ 12,433,650	\$ 3,558,000	\$ 3,722,350	\$ 3,598,000	\$ 3,598,000	\$ 26,910,000	

Rate Card Resources (\$)

Fill out Table 1 blue highlighted cells with the rates (inclusive of travel) for each Resource Category.

Fill out Table 1 blue highlighted cells with the proposed additional Resource Category(s) (if necessary) and rates (inclusive of travel).

Fill out Table 2 blue highlighted cells to describe the proposed additional Resource Categories listed in the first table.

Table 1

Resource Category	Units	Base Term				Optional Years			
		Year 1 FY21	Year 2 FY22	Year 3 FY23	Year 4 FY24	Year 5 FY25	Year 6 FY26	Year 7 FY27	Year 8 FY28
Security Architect	Hourly	\$ 225	\$ 230	\$ 235	\$ 240	\$ 245	\$ 250	\$ 255	\$ 260
Security Engineer	Hourly	\$ 160	\$ 163	\$ 166	\$ 169	\$ 172	\$ 175	\$ 179	\$ 183
Security Analyst 1	Hourly	\$ 145	\$ 148	\$ 151	\$ 154	\$ 157	\$ 160	\$ 163	\$ 166
Security Analyst 2	Hourly	\$ 180	\$ 184	\$ 188	\$ 192	\$ 196	\$ 200	\$ 204	\$ 208
Cloud Comp Engineer	Hourly	\$ 145	\$ 148	\$ 151	\$ 154	\$ 157	\$ 160	\$ 163	\$ 166
Software Developer	Hourly	\$ 145	\$ 148	\$ 151	\$ 154	\$ 157	\$ 160	\$ 163	\$ 166
Program Director	Hourly	\$ 275	\$ 281	\$ 287	\$ 293	\$ 299	\$ 305	\$ 311	\$ 317
Senior Project Manager	Hourly	\$ 190	\$ 194	\$ 198	\$ 202	\$ 206	\$ 210	\$ 214	\$ 218
CyberArk Cybersecurity Engineer	Hourly	\$ 240	\$ 245	\$ 250	\$ 255	\$ 260	\$ 265	\$ 270	\$ 275
CyberArk Cybersecurity Architect	Hourly	\$ 300	\$ 306	\$ 312	\$ 318	\$ 324	\$ 330	\$ 337	\$ 344
CyberArk Senior Software Developer	Hourly	\$ 270	\$ 275	\$ 281	\$ 287	\$ 293	\$ 299	\$ 305	\$ 311
CyberArk Software Developer	Hourly	\$ 240	\$ 245	\$ 250	\$ 255	\$ 260	\$ 265	\$ 270	\$ 275
CyberArk Consultant	Hourly	\$ 282	\$ 288	\$ 294	\$ 300	\$ 306	\$ 312	\$ 318	\$ 324
Project Manager	Hourly	\$ 145	\$ 148	\$ 151	\$ 154	\$ 157	\$ 160	\$ 163	\$ 166

Table 2

Resource Category	Role Description	Qualifications, Experience, and Education
Security Architect	Responsible for planning, designing and implementing of security systems and controls in the infrastructure layer within enterprise IT. Ensures adequate controls on interfaces across platforms. Perform risk/vulnerability assessments of systems. Identify and update missing or outdated policies and procedures. Possesses knowledge of encryption and PKI technologies.	7-12 years designing and building secure systems, networks, and infrastructures. High organizational skills. Excellent written and verbal communication skills. Strong ability to produce technical documentation.
Security Engineer	Responsible for the research, technical analysis, recommendation, configuration, and administration of systems and procedures to ensure the protection of information processed, stored or transmitted. Provides security design, consultation, and technology governance oversight for various projects and initiatives. Undertakes complex projects requiring additional specialized technical knowledge. Acts as information liaison and subject matter expert (SME) to various business units and information technology departments. Experience with common attack patterns and exploitation techniques. Ability to write fully functional exploits for common vulnerabilities such as simple stack overflow, cross-site scripting, or SQL injection. Experience in using standard Security Assessment and Penetration Testing tools such as BurpSuite, Metasploit, and IDA Pro. Experienced in Data Science techniques such as clustering, anomaly detection, and machine learning leveraging data analysis tools such as Splunk, MapReduce etc.. Acts as a resource for direction, training and guidance for less experienced staff. Demonstrate ability to perform complex security analysis of existing systems for compliance with security requirements.	Minimum 2 - 5 years of experience. High organizational skills. Excellent written and verbal communication skills. Strong ability to produce technical documentation.

Security Analyst 1	<p>Security Analysts apply information security threat intelligence to identify and exploit vulnerabilities within different projects' environments. Responsible for implementing security measures to protect computer systems, networks and data. Information security analysts are expected to stay up-to-date on the latest intelligence, including hackers' methodologies, in order to anticipate security breaches. Responsible for preventing data loss and service interruptions by researching new technologies that will effectively protect a network. Responsible for ensuring all networks have adequate security to prevent unauthorized access. They must ensure that all security systems are current with any software or hardware changes. They must plan and document all security information in the company including physical and internet security.</p> <p>The security analysts conduct application security assessments (web, mobile, API, etc.) using off-the-shelf or internally developed exploitation tools to execute manual testing for advanced attacks. They produce and deliver vulnerability and exploit information to clients in the form of a professional security assessment report. In addition, they conduct client conference calls including project kick-off calls, notification of high/critical findings during the testing process, and close out calls to review test findings, evidence, process steps to reproduce, and remediation recommendations. They perform proactive research to identify and understand new threats, vulnerabilities, and exploits. Perform procedures and processes necessary to ensure the safety of information systems assets and to protect systems from intentional or inadvertent access or destruction. Assists in project team in Disaster Recovery (DR) planning, Business Continuity Plan (BCP) & Continuity Of Operations (COOP) assessment, development, implementation, operation.</p>	2 - 4 years of experience in information security. Have assisted system users relative to information systems security matters. Performed various access and identity management functions. 1 to 2 years of application security testing knowledge/experience.
Security Analyst 2	<p>Security Analysts apply information security threat intelligence to identify and exploit vulnerabilities within different projects' environments. Responsible for implementing security measures to protect computer systems, networks and data. Information security analysts are expected to stay up-to-date on the latest intelligence, including hackers' methodologies, in order to anticipate security breaches. Responsible for preventing data loss and service interruptions by researching new technologies that will effectively protect a network. Responsible for ensuring all networks have adequate security to prevent unauthorized access. They must ensure that all security systems are current with any software or hardware changes. They must plan and document all security information in the company including physical and internet security.</p> <p>The security analysts conduct application security assessments (web, mobile, API, etc.) using off-the-shelf or internally developed exploitation tools to execute manual testing for advanced attacks. They produce and deliver vulnerability and exploit information to clients in the form of a professional security assessment report. In addition, they conduct client conference calls including project kick-off calls, notification of high/critical findings during the testing process, and close out calls to review test findings, evidence, process steps to reproduce, and remediation recommendations. They perform proactive research to identify and understand new threats, vulnerabilities, and exploits. Perform procedures and processes necessary to ensure the safety of information systems assets and to protect systems from intentional or inadvertent access or destruction. Assists in project team in Disaster Recovery (DR) planning, Business Continuity Plan (BCP) & Continuity Of Operations (COOP) assessment, development, implementation, operation.</p>	5 or more years of experience in information security. Skilled information technology professional with advanced experience developing and implementing IT policy, standards and procedures. Responsible for creating, testing and implementing business continuity and disaster recovery plans; performing risk assessments and testing of data processing systems; installing firewalls, data encryption and other security measures; recommending security enhancements and purchases; training staff on network and information security procedures; develop reports about the efficiency of security policies and recommend any changes; organize and conduct training for all employees regarding company security and information safeguarding.
Cloud Comp Engineer	<p>Designs, plans, and integrates cloud computing and virtualization systems. Provides specific, detailed information for hardware and software selection, cloud service provider selection, implementation techniques, application & data migration techniques and tools for the most efficient solution to meet business needs, including present and future capacity requirements. Develops and conducts testing of cloud and virtualization systems.</p>	2 - 4 years of experience in cloud computing engineering. Frequent use and application of technical standards, principles, theories, concepts and techniques. Receives assignments in the form of objectives and establishes goals to meet outlined objectives. Work is reviewed by supervisor/lead to measure meeting objectives. Directs established guidelines, procedures and policies.
Software Developer	<p>Designs, develops, documents, tests and debugs application software. Conducts analysis and collaborates with subject matter experts. End product may be special use, customized, or commercial software. Determines computer user needs; analyzes system capabilities to resolve problems on program intent, output requirements, input data acquisition, programming techniques and controls; prepares operating instructions; designs and develops autonomous services, desktop applications, web applications, scripts, and utility programs. Ensures software standards are met.</p>	2 - 4 years of experience in software development. Frequent use and application of technical standards, principles, theories, concepts and techniques. Receives assignments in the form of objectives and establishes goals to meet outlined objectives. Work is reviewed by supervisor/lead to measure meeting objectives. Directs established guidelines, procedures and policies. PROBLEM COMPLEXITY: Provides solutions to a variety of technical problems of moderate scope and complexity where analysis of situations or data requires a review of the variety of factors.

Program Director	<p>Designs, plans, and coordinates work teams. Follows standard project management industry practices such as the PMI's framework. Understands business and technical objectives of a project and works closely with project sponsor. Develops detailed work plans, schedules, project estimates, resource plans, and status reports. Conducts project meetings and is responsible for project tracking and analysis. Ensure adherences to quality standards and reviews project deliverables. Manages the integration of vendor tasks and tracks and reviews vendor deliverables. Provides technical and analytical guidance to project team. Recommends and takes action to direct the analysis and solutions of problems. Communicates to client/vendors. Creates project charter and work plan and tracks budget and schedule progress via appropriate metrics. Establishes project organization and methodologies and defines roles and responsibilities. Documents risks and develops mitigation plans. Manages scope. Creates and implements a communication plan. Builds an effective team, assigns tasks to team members, and evaluates outcomes. Negotiates resources. Communicates to stakeholders and project sponsor. Identifies, tracks, and ensures resolution of issues and removal of barriers. Provides technical support to project team members. Handles complex application features and technical designs. Designs and implements the components required for complex application features. Generally manages a group of applications systems analysts. Relies on experience and judgment to plan and accomplish goals. Professional certification is highly desirable.</p>	<p>3- 7 years of experience in the field or in a related area. Familiar with standard concepts, practices, and procedures within a particular field. Relies on limited experience and judgment to plan and accomplish goals. A certain degree of creativity and latitude is required. Works under limited supervision with considerable latitude for the use of initiative and independent judgment. Minimum of three (3) years of progressive broad-based information systems, system integration and project delivery experience. Experience working with external vendors and/or Quality Assurance efforts a plus.</p>
Senior Project Manager	<p>Designs, plans, and coordinates work teams. Follows standard project management industry practices such as the PMI's framework. Understands business and technical objectives of a project and works closely with project sponsor. Develops detailed work plans, schedules, project estimates, resource plans, and status reports. Conducts project meetings and is responsible for project tracking and analysis. Ensure adherences to quality standards and reviews project deliverables. Manages the integration of vendor tasks and tracks and reviews vendor deliverables. Provides technical and analytical guidance to project team. Recommends and takes action to direct the analysis and solutions of problems. Communicates to client/vendors. Creates project charter and work plan and tracks budget and schedule progress via appropriate metrics. Establishes project organization and methodologies and defines roles and responsibilities. Documents risks and develops mitigation plans. Manages scope. Creates and implements a communication plan. Builds an effective team, assigns tasks to team members, and evaluates outcomes. Negotiates resources. Communicates to stakeholders and project sponsor. Identifies, tracks, and ensures resolution of issues and removal of barriers. Provides technical support to project team members. Handles complex application features and technical designs. Designs and implements the components required for complex application features. Generally manages a group of applications systems analysts. Relies on experience and judgment to plan and accomplish goals. Professional certification is highly desirable.</p>	<p>8 or more years of experience, relies on experience and judgment to plan and accomplish goals, independently performs a variety of complicated tasks, a wide degree of creativity and latitude is expected. Certification in Project Management by a recognized project management organization or Scrum Master a plus.</p>
CyberArk Cybersecurity Engineer	<p>Provides direct support for engineering, implementing, integrating and operating cyber security solutions. Responsibility may span network and system security engineering; design of technical solutions for network boundary protection, endpoint security, access control, auditing, log management, event management and correlation, and network monitoring; network and system vulnerability assessment; application and software security assessment; database security assessment and monitoring; software security assurance; security configuration assessment, and compliance management; incident handling, response and reporting; technical security support to Certification and accreditation (C&A) processes and testing and security impact assessments as part of change management.</p>	<p>Bachelors and five (5) years or more of related experience; Masters and three (3) years or more related experience</p>
CyberArk Cybersecurity Architect	<p>Architect, plan, configure, deploy, maintain, and upgrades COTS and custom toolsets to address vulnerabilities and/or implement security controls. Applies a combination of expert engineering knowledge of enterprise IT and security solutions to design, develop and/or implement solutions to ensure they are consistent with enterprise architecture security policies and support full spectrum military cyberspace operations. Designs, tests, and implements secure systems, security monitoring, tuning and management of IT security systems and applications, incident response, digital forensics, loss prevention, and eDiscovery actions. Includes security control design and solution planning at the system, mission, and enterprise level, security-in-depth/defense-in-depth, and other related IAM/ISSO/ISSE support functions. Involved in a wide range of security issues including architectures, firewalls, electronic data traffic, and network access. Researches and evaluates cyber capabilities and new security tools and products against operational requirements and introduces them to the enterprise in alignment with IT security strategy, and to support the offensive and defensive capability design and troubleshoot and problem solve technical and non-technical issues. . At the Leadership level this is senior technical staff dedicated to transforming customer environments into a more secure operating environment in a holistic manner.</p>	<p>Bachelors and eight (8) years or more of related experience supporting information technology projects with at least four (4) years of experience related to information or computer security; Masters and seven (7) years or more of related experience</p>
CyberArk Senior Software Developer	<p>Plans, directs and monitors the work of team members. Sets priorities to meet the needs of users. Formulates/defines system scope and objectives. Devises or modifies procedures to solve complex problems considering computer equipment capacity and limitations. Prepares detailed specifications from which programs will be written. Designs, codes, tests, debugs, and documents those programs. May be involved in related areas such as database design/management, evaluation of commercial off-the-shelf (COTS) products, and analysis of network hardware/software issues. May direct the work of other systems analysts and programmers. This skill is qualified to operate in advanced technical environments that include C++, Client/Server, Oracle, Power Builder, Visual Basic, JAVA, and other source code requirements.</p>	<p>Bachelor's degree in Computer Science or a related field. Eight (8) years of technical experience in applications software development, three of which are in systems analysis and one year which is acting as technical lead to a team of programmers/analysts. Has a good understanding of the business or function for which the application is designed.</p>

CyberArk Software Developer	<p>Designs, develops, documents, tests and debugs application software. Conducts analysis and collaborates with subject matter experts in the planning, design, development, and utilization of electronic data processing systems for information storage, processing, presentation, manipulation, display, or reporting. End product may be special use, customized, or commercial software.</p>	<p>Bachelor's degree in Computer Science or a related field. Five (5) years of technical experience in applications software development. Has a good understanding of the business or function for which the application is designed. Skilled and qualified to operate in advanced technical environments that include C++, Client/Server, Oracle, Power Builder, Visual Basic, JAVA, and other source code requirements.</p>
CyberArk Consultant	<p>Assists CIOs, CISOs and Program Managers to assess, develop, implement and maintain enterprise information/cybersecurity programs. Assist clients to interpret policies and standards related to information and cybersecurity. Develop strategies for implementing all aspects of Cybersecurity programs as well as Privacy. Devise solutions to speed adoption of standards, policy and procedures as well as measure performance and compliance. Develop policy, procedures, and best practices. Prepare presentations, papers and other materials to support the CIO, CISO and program managers to communicate policy, requirements, practices and solutions to business and system owners. Program security program office support ranging from analysis, planning, and budget. Manage project requirements, resources and deliverables. Prepare and provide management and project reports.</p>	<p>Master's degree in Computer Science, Engineering, or a related field. Ten years of experience in an area of specialization associated with the requirement.</p>
Project Manager	<p>Designs, plans, and coordinates work teams. Follows standard project management industry practices such as the PMI's framework. Understands business and technical objectives of a project and works closely with project sponsor. Develops detailed work plans, schedules, project estimates, resource plans, and status reports. Conducts project meetings and is responsible for project tracking and analysis. Ensure adherence to quality standards and reviews project deliverables. Manages the integration of vendor tasks and tracks and reviews vendor deliverables. Provides technical and analytical guidance to project team. Recommends and takes action to direct the analysis and solutions of problems. Communicates to client/vendors. Creates project charter and work plan and tracks budget and schedule progress via appropriate metrics. Establishes project organization and methodologies and defines roles and responsibilities. Documents risks and develops mitigation plans. Manages scope. Creates and implements a communication plan. Builds an effective team, assigns tasks to team members, and evaluates outcomes. Negotiates resources. Communicates to stakeholders and project sponsor. Identifies, tracks, and ensures resolution of issues and removal of barriers. Provides technical support to project team members. Handles complex application features and technical designs. Designs and implements the components required for complex application features. Generally manages a group of applications systems analysts. Relies on experience and judgment to plan and accomplish goals. Professional certification is highly desirable.</p>	<p>3- 7 years of experience in the field or in a related area. Familiar with standard concepts, practices, and procedures within a particular field. Relies on limited experience and judgment to plan and accomplish goals. A certain degree of creativity and latitude is required. Works under limited supervision with considerable latitude for the use of initiative and independent judgment. Minimum of three (3) years of progressive broad-based information systems, system integration and project delivery experience. Experience working with external vendors and/or Quality Assurance efforts a plus.</p>

Existing Hardware Used in Security Services

Fill out blue highlighted areas of worksheet to indicate if Respondent will retain hardware and provided estimated fair market value buyout of each asset.

NOTE: DIR has provided an initial asset list. Additional data may be added throughout the procurement process.

Respondent Retained? Y/N	\$ FMV	Asset Classification	Functional Category	Functional Sub- category	Category	Affected Customers	Consolidated	ID	Company	Status	Service Tier	Location	Is Virtual	Managing Group	Model Number	Primary Capability	Subcategory	Used For
	\$ -																	
	\$ -																	
	\$ -																	
	\$ -																	
	\$ -																	
	\$ -																	
	\$ -																	
	\$ -																	
	\$ -																	
	\$ -																	

Existing Software Used in Security Services

Fill out blue highlighted areas of worksheet to indicate if Respondent will retain software.

NOTE: DIR has provided an initial asset list. Additional data may be added throughout the procurement process.

Respondent Retained? Y/N	Estimated Annual Cost	Vendor	Historically Underutilized Business (HUB)	Services Description	Contact Effective Date	Contact Expiration Date	Cancellable w/o penalty Y/N	Charging Mechanism

Existing Third Party Contracts Used in Security Services

Fill out blue highlighted areas of worksheet to indicate if Respondent will retain third party contract.

NOTE: DIR has provided an initial asset list. Additional data may be added throughout the procurement process.

Respondent Retained? Y/N	Estimated Annual Cost	Respondent Annual Cost included in Pricing	Vendor	Historically Underutilized Business (HUB)	Services Description	Contact Effective Date	Contact Expiration Date	Cancellable w/o penalty Y/N	Charging Mechanism	Assignable (Y/N)
Yes	\$90,000 - \$100,000	Yes	CYBER-AR	Non-HUB	Security Provider for p	4/20/2018	3/30/2019	Y	In Unit Rates	Y

Appendix

The tabs in this Appendix section must be completed by Respondent.
These tabs are for informational purposes only.

Respondent Assumptions

The Respondent is to list all assumptions associated with the Charges and Services within the scope of the RFO.

The Respondent is to provide the degree of impact on the price (High, Medium, Low, Not Applicable) and the related SOW section of the assumption.

Item #	Price Impact (H, M, L, N/A)	SOW Ref #	Description
1			
2			
3			
4			
5			This tab was used to capture current state at the time of contract award. It is not intended to be updated on an ongoing basis and is retained for historical reference.
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			
21			
22			
23			
24			
25			
26			
27			
28			
29			
30			

Staffing Model - FTEs by Month

Informational purposes only

Fill out blue highlighted areas of worksheet with average FTE counts for each service per period.

SOW Section	SOW Services	Transition						Base Term				Optional Extension Years			
		Month 1 Mar-20	Month 2 Apr-20	Month 3 May-20	Month 4 Jun-20	Month 5 Jul-20	Month 6 Aug-20	Year 1 FY21	Year 2 FY22	Year 3 FY23	Year 4 FY24	Year 5 FY25	Year 6 FY26	Year 7 FY27	Year 8 FY28
2	Transition Services	1.75	7.47	13.43	14.90	22.85	30.14	-	-	-	-	-	-	-	-
3.1.1	Security Incident and Event Monitoring (SIEM)	-	-	-	-	-	-	0.99	0.99	0.98	0.98	0.98	0.98	0.98	0.98
3.1.2	Privileged Access Management (PAM)	-	-	-	-	-	-	0.91	0.90	0.89	0.89	0.89	0.89	0.89	0.89
3.1.3	Firewall Rule Management	-	-	-	-	-	-	0.22	0.21	0.21	0.21	0.21	0.21	0.21	0.21
3.1.4	Cloud Access Security Broker (CASB): Standards and Alerts	-	-	-	-	-	-	0.19	0.19	0.19	0.19	0.19	0.19	0.19	0.19
3.1.5	Advanced Malware Protection Standards	-	-	-	-	-	-	0.22	0.22	0.22	0.22	0.22	0.22	0.22	0.22
3.1.6	Security Threat Identification and Remediation	-	-	-	-	-	-	0.83	0.81	0.78	0.78	0.78	0.78	0.78	0.78
3.1.7	Master Security Baseline Configurations Standards	-	-	-	-	-	-	0.19	0.18	0.18	0.18	0.18	0.18	0.18	0.18
3.1.8	Establish Operating Procedures, Protocols and Coordination/Communication Mechanisms	-	-	-	-	-	-	0.38	0.36	0.33	0.33	0.33	0.33	0.33	0.33
3.1.9	Operation, Monitoring and Reporting	-	-	-	-	-	-	0.40	0.38	0.35	0.35	0.35	0.35	0.35	0.35
3.2	Security Program Management	-	-	-	-	-	-	0.45	0.45	0.45	0.45	0.45	0.45	0.45	0.45
3.3	Security Standards	-	-	-	-	-	-	0.32	0.32	0.32	0.32	0.32	0.32	0.32	0.32
3.4	Security Auditing and Reporting Requirements	-	-	-	-	-	-	0.30	0.30	0.30	0.30	0.30	0.30	0.30	0.30
3.5	Ongoing DCS Security Operations Requirements	-	-	-	-	-	-	14.19	14.19	14.19	14.19	14.19	14.19	14.19	14.19
3.6	Managed Intrusion Detection, Management and Prevention Services	-	-	-	-	-	-	0.59	0.59	0.59	0.59	0.59	0.59	0.59	0.59
3.7	Intentionally Left Blank	-	-	-	-	-	-	-	-	-	-	-	-	-	-
3.8	Security Emergency Response Services	-	-	-	-	-	-	0.47	0.46	0.46	0.46	0.46	0.46	0.46	0.46
3.9	Security Vulnerability Identification and Remediation Services	-	-	-	-	-	-	0.51	0.51	0.51	0.51	0.51	0.51	0.51	0.51
3.10	Security Incident Management	-	-	-	-	-	-	2.93	2.93	2.93	2.93	2.93	2.93	2.93	2.93

This tab was used to capture current state at the time of contract award. It is not intended to be updated on an ongoing basis and is retained for historical reference.

3.11	Risk Management and Tracking	-	-	-	-	-	-	0.71	0.70	0.68	0.68	0.68	0.68	0.68	0.68
3.12	Steady State Security Operations, Maintenance and Monitoring Requirements	-	-	-	-	-	-	0.38	0.38	0.38	0.38	0.38	0.38	0.38	0.38
3.13	Cybersecurity Assessment	-	-	-	-	-	-	0.25	0.25	0.25	0.25	0.25	0.25	0.25	0.25
3.14	Disaster Recovery Support Services	-	-	-	-	-	-	0.21	0.21	0.21	0.21	0.21	0.21	0.21	0.21
3.15	Reporting	-	-	-	-	-	-	0.25	0.25	0.25	0.25	0.25	0.25	0.25	0.25
3.16	Compliance	-	-	-	-	-	-	0.46	0.43	0.39	0.39	0.39	0.39	0.39	0.39
3.17	Quality Assurance	-	-	-	-	-	-	0.38	0.35	0.32	0.32	0.32	0.32	0.32	0.32
3.18	Industry Standards, Certifications and Compliance	-	-	-	-	-	-	0.13	0.12	0.10	0.10	0.10	0.10	0.10	0.10
6	Performance Model - Service Level Agreements	-	-	-	-	-	-	0.16	0.14	0.13	0.13	0.13	0.13	0.13	0.13
8	DCS Governance Model	-	-	-	-	-	-	0.06	0.05	0.05	0.05	0.05	0.05	0.05	0.05
9	Cross Functional Services	-	-	-	-	-	-	0.50	0.49	0.48	0.48	0.48	0.48	0.48	0.48
Total		1.75	7.47	13.43	14.90	22.85	30.14	27.61	27.36	27.11	27.11	27.11	27.11	27.11	27.11
Respondent Employees (100% of Time on Account)		1.75	6.00	9.00	11.00	14.00	28.00	25.00	24.00	24.00	24.00	24.00	24.00	24.00	24.00
Respondent Employess (<100% of Time on Account)		-	1.47	2.81	2.32	7.27	0.78	0.50	1.25	1.00	1.00	1.00	1.00	1.00	1.00
Subcontracting Staff		-	-	1.62	1.58	1.58	1.36	2.12	2.11	2.11	2.11	2.11	2.11	2.11	2.11
Total		1.75	7.47	13.43	14.90	22.85	30.14	27.61	27.36	27.11	27.11	27.11	27.11	27.11	27.11
Difference		-	-	-	-	-	-	-	-	-	-	-	-	-	-

Steady State Run Services - Annual (\$)

Informational purposes only

Fill out blue highlighted areas of worksheet with Charges for each service per period.

This tab was used to capture current state at the time of contract award. It is not intended to be updated on an ongoing basis and is retained for historical reference.

Charges by SOW Service Category		Base Term					Option Years				
SOW Section	SOW Services	Year 1 FY21	Year 2 FY22	Year 3 FY23	Year 4 FY24	Total Base Term	Year 5 FY25	Year 6 FY26	Year 7 FY27	Year 8 FY28	Total Charges
3.1.1	Security Incident and Even Monitoring (SIEM)	\$ 1,992,264	\$ 2,013,253	\$ 1,991,698	\$ 1,744,334	\$ 7,741,549	\$ 1,336,940	\$ 1,381,805	\$ 1,222,823	\$ 1,167,269	\$ 12,850,386
3.1.2	Privileged Access Management (PAM)	\$ 879,931	\$ 886,488	\$ 896,305	\$ 905,530	\$ 3,568,254	\$ 918,881	\$ 932,777	\$ 947,166	\$ 961,800	\$ 7,328,878
3.1.3	Firewall Rule Management	\$ 75,751	\$ 73,160	\$ 70,395	\$ 71,726	\$ 291,032	\$ 73,060	\$ 74,477	\$ 75,970	\$ 77,481	\$ 592,020
3.1.4	Cloud Access Security Broker (CASB): Standards and Alerts	\$ 59,976	\$ 61,107	\$ 62,220	\$ 63,401	\$ 246,704	\$ 64,585	\$ 65,838	\$ 67,159	\$ 68,494	\$ 512,780
3.1.5	Advanced Malware Protection Standards	\$ 75,095	\$ 76,543	\$ 77,956	\$ 79,455	\$ 309,049	\$ 80,896	\$ 82,451	\$ 84,103	\$ 85,784	\$ 642,283
3.1.6	Security Threat Identification and Remediation	\$ 257,279	\$ 249,270	\$ 240,598	\$ 245,067	\$ 992,214	\$ 249,553	\$ 254,350	\$ 259,455	\$ 264,640	\$ 2,020,212
3.1.7	Master Security Baseline Configurations Standards	\$ 68,290	\$ 65,542	\$ 62,627	\$ 63,796	\$ 260,255	\$ 64,906	\$ 66,102	\$ 67,370	\$ 68,660	\$ 527,293
3.1.8	Establish Operating Procedures, Protocols and Coordination/Communication Mechanisms	\$ 131,801	\$ 122,226	\$ 112,193	\$ 114,317	\$ 480,537	\$ 116,464	\$ 118,730	\$ 121,109	\$ 123,527	\$ 960,367
3.1.9	Operation, Monitoring and Reporting	\$ 168,381	\$ 159,524	\$ 150,088	\$ 152,890	\$ 630,883	\$ 155,637	\$ 158,616	\$ 161,794	\$ 165,036	\$ 1,271,966
3.2	Security Program Management	\$ 214,918	\$ 258,314	\$ 234,285	\$ 213,015	\$ 920,532	\$ 191,786	\$ 170,756	\$ 149,909	\$ 129,212	\$ 1,562,195
3.3	Security Standards	\$ 77,122	\$ 78,603	\$ 80,028	\$ 81,545	\$ 317,298	\$ 83,013	\$ 84,598	\$ 86,277	\$ 88,018	\$ 659,204
3.4	Security Auditing and Reporting Requirements	\$ 78,133	\$ 79,642	\$ 81,246	\$ 82,879	\$ 321,900	\$ 84,487	\$ 86,155	\$ 87,879	\$ 89,638	\$ 670,059
3.5	Ongoing DCS Security Operations Requirements	\$ 2,681,208	\$ 2,712,548	\$ 2,743,631	\$ 2,774,980	\$ 10,912,365	\$ 2,806,361	\$ 2,838,031	\$ 2,870,038	\$ 2,902,163	\$ 22,328,957
3.6	Prevention Services	\$ 116,532	\$ 118,741	\$ 120,849	\$ 123,093	\$ 479,215	\$ 125,347	\$ 127,747	\$ 130,316	\$ 132,925	\$ 995,550
3.7	Intentionally Left Blank	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -
3.8	Security Emergency Response Services	\$ 113,481	\$ 112,413	\$ 111,151	\$ 113,228	\$ 450,273	\$ 115,313	\$ 117,531	\$ 119,891	\$ 122,286	\$ 925,294
3.9	Security Vulnerability Identification and Remediation Services	\$ 126,179	\$ 128,563	\$ 130,850	\$ 133,287	\$ 518,879	\$ 135,735	\$ 138,343	\$ 141,122	\$ 143,942	\$ 1,078,021
3.10	Security Incident Management	\$ 132,405	\$ 134,911	\$ 137,260	\$ 139,774	\$ 544,350	\$ 142,300	\$ 145,010	\$ 147,926	\$ 150,897	\$ 1,130,483
3.11	Risk Management and Tracking	\$ 200,379	\$ 196,172	\$ 191,566	\$ 195,201	\$ 783,318	\$ 198,748	\$ 202,559	\$ 206,585	\$ 210,746	\$ 1,601,956
3.12	Steady State Security Operations, Maintenance and Monitoring Requirements	\$ 69,552	\$ 70,866	\$ 72,101	\$ 73,422	\$ 285,941	\$ 74,753	\$ 76,177	\$ 77,700	\$ 79,266	\$ 593,837
3.13	Cybersecurity Assessment	\$ 57,332	\$ 58,405	\$ 59,421	\$ 60,510	\$ 235,668	\$ 61,611	\$ 62,789	\$ 64,033	\$ 65,327	\$ 489,428
3.14	Disaster Recovery Support Services	\$ 49,443	\$ 50,393	\$ 51,311	\$ 52,287	\$ 203,434	\$ 53,237	\$ 54,257	\$ 55,341	\$ 56,451	\$ 422,720
3.15	Reporting	\$ 57,838	\$ 58,925	\$ 60,030	\$ 61,177	\$ 237,970	\$ 62,348	\$ 63,568	\$ 64,834	\$ 66,137	\$ 494,857
3.16	Compliance	\$ 158,550	\$ 142,313	\$ 125,324	\$ 127,746	\$ 553,933	\$ 130,064	\$ 132,562	\$ 135,206	\$ 137,919	\$ 1,089,684
3.17	Quality Assurance	\$ 139,017	\$ 112,732	\$ 98,482	\$ 100,384	\$ 450,615	\$ 102,250	\$ 104,232	\$ 106,314	\$ 108,443	\$ 871,854
3.18	Industry Standards, Certifications and Compliance	\$ 198,264	\$ 191,136	\$ 183,578	\$ 184,221	\$ 757,199	\$ 184,870	\$ 185,551	\$ 186,262	\$ 186,987	\$ 1,500,869
6	Performance Model - Service Level Agreements	\$ 56,030	\$ 49,066	\$ 41,813	\$ 42,628	\$ 189,537	\$ 43,424	\$ 44,267	\$ 45,153	\$ 46,056	\$ 368,437
8	DCS Governance Model	\$ 24,353	\$ 23,217	\$ 22,008	\$ 22,432	\$ 92,010	\$ 22,832	\$ 23,268	\$ 23,734	\$ 24,210	\$ 186,054
9	Cross Functional Services	\$ 171,744	\$ 168,591	\$ 165,066	\$ 168,171	\$ 673,572	\$ 171,183	\$ 174,453	\$ 177,947	\$ 181,518	\$ 1,378,673
Total Charges		\$ 8,431,248	\$ 8,452,664	\$ 8,374,080	\$ 8,190,496	\$ 33,448,486	\$ 7,850,584	\$ 7,967,000	\$ 7,883,416	\$ 7,904,832	\$ 65,054,317
Must Reconcile to Tab 2 - Run Charges		\$ 8,431,248	\$ 8,452,664	\$ 8,374,080	\$ 8,190,496	\$ 33,448,486	\$ 7,850,584	\$ 7,967,000	\$ 7,883,416	\$ 7,904,832	\$ 65,054,317
Difference		\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -

Fill out blue highlighted areas of worksheet with key cost drivers for each service (e.g., devices monitored, customers, software licenses, incidents, sites, etc).

DIR may convert fixed charges to variable as part of final negotiations based on variability of cost to support service. Identification of key cost drivers will help facilitate this decision.

SOW Section	SOW Services	Key Cost Drivers
3.1.1	Security Incident and Even Monitoring (SIEM)	<ol style="list-style-type: none"> 1. Number of endpoints 2. Number of reports 3. Number of licenses 4. Number of devices 5. Type of volume of alerts sent to SIEM
3.1.2	Privileged Access Management (PAM)	<ol style="list-style-type: none"> 1. Number of endpoints 2. Number of reports 3. Number of licenses 4. Number of devices 5. Number of privileged accounts 6. Number of different integration types
3.1.3	Firewall Rule Management	<ol style="list-style-type: none"> 1. Number of endpoints 2. Number of licenses 3. Number of devices 4. Number of different device types and deployment of configuration standards
3.1.4	Cloud Access Security Broker (CASB): Standards and Alerts	<ol style="list-style-type: none"> 1. Number of endpoints 2. Number of reports 3. Number of users 4. Number of different integration types 5. Number of cloud applications
3.1.5	Advanced Malware Protection Standards	<ol style="list-style-type: none"> 1. Number of endpoints 2. Number of reports 3. Number of devices
3.1.6	Security Threat Identification and Remediation	<ol style="list-style-type: none"> 1. Number of endpoints 2. Number of devices
3.1.7	Master Security Baseline Configurations Standards	<ol style="list-style-type: none"> 1. Number of endpoints 2. Number of different device types/manufacturers and deployment configuration standards 3. Number of approved build images 4. Number of devices
3.1.8	Establish Operating Procedures, Protocols and Coordination/Communication Mechanisms	<ol style="list-style-type: none"> 1. Number of approved managed device types 2. Number of operating systems and standard configurations 3. Number of SCP's 4. Number of devices
3.1.9	Operation, Monitoring and Reporting	<ol style="list-style-type: none"> 1. Number of endpoints 2. Number of reports 3. Number of licenses 4. Number of devices

3.2	Security Program Management	1. Number of endpoints 2. Number of reports
3.3	Security Standards	1. Number of standards
3.4	Security Auditing and Reporting Requirements	1. Number of security audits per month 2. Number of reports by complexity (Simple, Moderate, High)
3.5	Ongoing DCS Security Operations Requirements	1. Number of notifications per month 2. Number of endpoints monitored 3. Number of aggregation flows to integrate
3.6	Managed Intrusion Detection, Management and Prevention Services	1. Number of endpoints monitored 2. Number of notable events investigated per month
3.7	Intentionally Left Blank	Intentionally Left Blank
3.8	Security Emergency Response Services	1. Number of emergency responses per quarter 2. Length of emergency response activity
3.9	Security Vulnerability Identification and Remediation Services	1. Number of vulnerability scans performed per month 2. Number of vulnerabilities identified per month
3.10	Security Incident Management	1. Number of notable events investigated per month 2. Number security incidents managed per month
3.11	Risk Management and Tracking	1. Number of vulnerabilities identified and tracked per month

3.12	Steady State Security Operations, Maintenance and Monitoring Requirements	1. Number of endpoints protected
3.13	Cybersecurity Assessment	1. Number of assessments performed per month by complexity (Simple, Moderate, High)
3.14	Disaster Recovery Support Services	1. Number of DR exercises per year 1 2. Number of systems and applications included in DR
3.15	Reporting	1. Number of reports per day, per month, per year by level of complexity (Simple, Moderate, High)
3.16	Compliance	1. Number of audits per month 2. Complexity of compliance audits (Simple, Moderate, High)
3.17	Quality Assurance	1. Number of QA assessments per quarter 2. Number of quality and progress reviews 3. Number of QA specific procedures
3.18	Industry Standards, Certifications and Compliance	1. Number of standards, certifications, and compliance required
6	Performance Model - Service Level Agreements	1. Number of service requests 2. Number of customers 3. Number of services offered
8	DCS Governance Model	1. Number of committees and solution groups in-which SAIC participates 2. Number of service delivery and performance issues 3. Number of security services program issues 4. Number of contract and financial issues 5. Number of invoice disputes 6. Number of customer relationship and communications issues
9	Cross Functional Services	1. Number of integrations and MSI tool complexity 2. Number of incidents

Transition Services Bill of Materials

Informational purposes only

Fill out blue highlighted areas of worksheet for all hardware and software included in Transition Charges.

Respondent may add (insert) additional rows as necessary.

Transition Bill of Materials are incremental to those indicated as being retained by the Respondent on the Assets (Tab 6) and Software (Tab 7).

Hardware purchases must include five years of maintenance in Charges.

This tab was used to capture current state at the time of contract award. It is not intended to be updated on an on basis and is retained for historical reference.

Annual recurring Software License Charges, after the initial year of purchase, must be included in Tab A5 "Run BOM" if retained past Transition and reflected in Tab 2 "Run Charges".

Transition Hardware and Software purchases are owned by Respondent and must be transferrable to DIR.

SOW Section	Item No.	Manufacturer	Model No.	Description	Capacity	Number of Units	Unit Costs	Original Purchase	5 year Maintenance Support	Annual Subscription / License	Total Charges
2	Transition Phase Bill of Materials										
	Hardware: (List all hardware)										
						-	\$ -	\$ -	\$ -	\$ -	\$ -
						-	\$ -	\$ -	\$ -	\$ -	\$ -
						-	\$ -	\$ -	\$ -	\$ -	\$ -
						-	\$ -	\$ -	\$ -	\$ -	\$ -
	Total Hardware Charges:							\$ -	\$ -	\$ -	\$ -
	Software: (List all software)										
		Splunk	CLD-FED-BNDL		0.5/TB/day	1	\$ 135,957	\$ 135,957	\$ -	\$ -	\$ 135,957
	Total Software Charges:							\$ 135,957	\$ -	\$ -	\$ 135,957
Total Transition Bill of Materials Charges (include in Tab 3)								\$ 135,957	\$ -	\$ -	\$ 135,957

Steady State Run Services Bill Of Materials

Informational purposes only

Fill out blue highlighted areas of worksheet for all hardware and software included in Steady State Run Charges. Respondent may add (insert) additional rows as necessary.

This tab was used to capture current state at the time of

Bill of Materials are incremental to those indicated as being retained by the Respondent on the Assets (Tab 6) and Software (Tab 7) and the BOM identified in Transition Services (tab A4).

Hardware purchases must include five years of maintenance in Charges.

Annual recurring Software License Charges, after the initial year of purchase, must be included annually in in Tab 2 "Run Charges".

Steady State Hardware and Software purchases are owned by Respondent and must be transferrable to DIR.

SOW Section	Item No.	Service Area	Manufacturer	Model No.	Description	Capacity	No. of Units	Unit Costs	Pre-existing Materials	Original Purchase	5 year Maintenance	Annual Subscription / License	Total Costs	Recurring Charges (3)
DCS Security Operations Services														
3, 4, 6, 8, 9	Hardware: (List all hardware)													
							-	\$ -		\$ -	\$ -	\$ -	\$ -	\$ -
							-	\$ -		\$ -	\$ -	\$ -	\$ -	\$ -
							-	\$ -		\$ -	\$ -	\$ -	\$ -	\$ -
										\$ -	\$ -	\$ -	\$ -	\$ -
	Total Hardware Charges:													
	Software: (List all software)													
	Security	CyberArk				1000 Users		\$ -	No	\$ -	\$ 714,133.00	\$ -	\$ 714,133	\$ -
	Security	Tenable				N/A		\$ -	No	\$ -	\$ -	\$ 2,746	\$ 2,746	\$ -
	Security	Splunk				0.5/TB/day		\$ -	No	\$ -	\$ -	\$ 916,836	\$ 916,836	\$ -
	Security	FireEye				Annual		\$ -	No	\$ -	\$ -	\$ 127,682	\$ 127,682	\$ -
	Security	FireEye				Annual		\$ -	No	\$ -	\$ -	\$ 127,682	\$ 127,682	\$ -
	Security	CyberArk				1000 Users	1	595,681	No	\$ -	\$ 595,681	\$ -	\$ 595,681	\$ -
	Security	CyberArk				N/A	1	46,885	No	\$ -	\$ 46,885	\$ -	\$ 46,885	\$ -
	Security	Tenable				N/A	1	2,746	No	\$ -	\$ 2,746	\$ -	\$ 2,746	\$ -
	Total Software Costs:										\$ -	\$ 1,359,445	\$ 1,174,946	\$ 2,534,391
	Total Run Services Bill of Materials										\$ -	\$ 1,359,445	\$ 1,174,946	\$ 2,534,391

