GENERAL SERVICES ADMINISTRATION

Federal Acquisition Service

Authorized Federal Supply Schedule Price List

Online access to contract ordering information, terms and conditions, pricing, and the option to create an electronic delivery order are available through GSA Advantage!®. The website for GSA Advantage!® is: https://www.GSAAdvantage.gov.

Multiple Award Schedule (MAS)
Federal Supply Group: Professional Services
Contract Number: 47QTCA24D0038
For more information on ordering go to the following website: https://www.gsa.gov/schedules.
Contract Period: 12/21/2023 – 12/20/2028
Prices Shown Herein are Net

For more information on ordering from Federal Supply Schedules click on the FSS Schedules button at: http://fss.gsa.gov/.

CONTRACTOR:
ClearPro Partners
305 Harrison Street SE, Suite 100B Leesburg,
Virginia 20175
(703) 785-0766
Kcassidy@clearpropartners.com

CONTRACTOR'S ADMINISTRATION SOURCE:
Kevin Cassidy
305 Harrison Street SE, Suite 100B Leesburg,
Virginia 20175
(703) 785-0766
Kcassidy@clearpropartners.com

ClearPro Partners is a Mentor/Protégé Joint Venture between the following partners:

ClearFocus, Technologies (*Mentor*) GSA MAS Schedule GS-35F-444CA and SINs 54151HACS, 54151S, OLM
Procentrix, LLC Technologies (*Protégé*) GSA MAS Schedule GS-35F-0294T and SINs 518210C, 54151S, OLM

BUSINESS SIZE: Small

For more information on ordering go to the following website: https://www.gsa.gov/schedules.

CUSTOMER INFORMATION

1. Table of awarded special item number(s) with appropriate cross-reference to item descriptions and awarded price(s).

SINs	Recovery	SIN Title
54151S	54151SRC	Information Technology Professional Services
54151HACS	54151HACSRC	Highly Adaptive Cybersecurity Services
OLM	OLMRC	Order Level Materials

2. Identification of the lowest priced model number and lowest unit price for that model for each special item number awarded in the contract. This price is the Government price based on a unit of one, exclusive of any quantity/dollar volume, prompt payment, or any other concession affecting price. Contracts that have unit prices based on the geographic location of the customer, should show the range of the lowest price, and cite the areas to which the prices apply.

   See Pricelist (Government net price based on a unit of one).

3. If the Contractor is proposing hourly rates, a description of all corresponding commercial job titles, experience, functional responsibility and education for those types of employees or subcontractors who will perform services shall be provided. If hourly rates are not applicable, the Contractor shall insert "Not applicable" for this item.

   See Pricelist (includes discount and IFF).

4. Lowest Priced Item: See Pricelist (Government net price based on a unit of one).

5. Hourly Rates: See Pricelist

6. Maximum order:
   54151S: $ 500,000 per order
   54151HACS: $ 500,000 per order

7. Minimum order: $100

8. Geographic coverage (delivery area): Domestic

9. Point(s) of production (city, county, and State or foreign country): 305 Harrison Street SE, Suite 100B, Leesburg, Virginia 20175

10. Discount from list prices or statement of net price: Government Net Prices (discounts already deducted.)

11. Quantity discounts: **None**

Prompt payment terms. Information for Ordering Offices: Prompt payment terms cannot be negotiated out of the contractual agreement in exchange for other concessions: **Net 10 Days - 0.50%**

12. Foreign items (list items by country of origin): **Not Applicable**

10a. Time of delivery: (Contractor insert number of days.) **To Be Determined at the Task Order level**

10b. Expedited Delivery. Items available for expedited delivery are noted in this price list: **To Be Determined at the Task Order level**

10c. Overnight and 2-day delivery: **To Be Determined at the Task Order level**

10d. Urgent Requirements: **To Be Determined at the Task Order level**

11. F.O.B. point(s): **Destination**

12a. Ordering address(es): **305 Harrison Street SE, Suite 100B, Leesburg, Virginia 20175**

12b. Ordering procedures: **See Federal Acquisition Regulation (FAR) 8.405-3" in Customer Information Item 12b per I-FSS-600.**

13. Payment address(es): **305 Harrison Street SE, Suite 100B, Leesburg, Virginia 20175**

14. Warranty provision: **Standard Commercial Warranty Terms & Conditions**

15. Export packing charges, if applicable: **Not Applicable**

16. Terms and conditions of rental, maintenance, and repair (if applicable): **Not Applicable**

17. Terms and conditions of installation (if applicable): **Not Applicable**

18a. Terms and conditions of repair parts indicating date of parts price lists and any discounts from list prices (if applicable): **Not Applicable**

18b. Terms and conditions for any other services (if applicable): **Not Applicable**

19. List of service and distribution points (if applicable): **Not Applicable**

20. List of participating dealers (if applicable): **Not Applicable**

21. Preventive maintenance (if applicable): **Not Applicable**

22a. Special attributes such as environmental attributes (e.g., recycled content, energy efficiency, and/or reduced pollutants): **Not Applicable**

22b. If applicable, indicate that Section 508 compliance information is available for the information and communications technology (ICT) products and services and show where full details can be found (e.g. contractor's website or other location.) ICT accessibility standards can be found at: https://www.Section508.gov/. **Not applicable**

23. Unique Entity Identifier (UEI) Number: **NCMDTCHBCLD4**

24. Notification regarding registration in System for Award Management (SAM) database: **Contractor registered and active in SAM**

FINAL PRICING

The rates shown below include the Industrial Funding Fee (IFF) of 0.75%.

SIN	Labor Category	GSA PRICE including IFF 12/21/2023 – 12/20/2024	GSA PRICE including IFF 12/21/2024 – 12/20/2025	GSA PRICE including IFF 12/21/2025 – 12/20/2026	GSA PRICE including IFF 12/21/2026 – 12/20/2027	GSA PRICE including IFF 12/21/2027 – 12/20/2028
54151HACS	Cybersecurity Project Manager II (ClearFocus)			**$133.04**	**$137.03**	**$141.14**
54151HACS	Cybersecurity Project Manager III (ClearFocus)			**$160.05**	**$164.86**	**$169.80**
54151HACS	Cybersecurity Analyst I (ClearFocus)			**$101.75**	**$104.81**	**$107.95**
54151HACS	Cybersecurity Analyst II (ClearFocus)			**$126.14**	**$129.92**	**$133.82**
54151HACS	Cybersecurity Analyst III (ClearFocus)			**$149.87**	**$154.37**	**$159.00**
54151HACS	Cybersecurity Administrator II (ClearFocus)			**$113.42**	**$116.83**	**$120.33**
54151HACS	Cybersecurity Administrator III (ClearFocus)			**$138.48**	**$142.63**	**$146.91**
54151HACS	Cybersecurity Engineer I (ClearFocus)			**$110.42**	**$113.73**	**$117.15**
54151HACS	Cybersecurity Engineer II (ClearFocus)			**$144.75**	**$149.09**	**$153.56**
54151HACS	Cybersecurity Engineer III (ClearFocus)			**$160.05**	**$164.86**	**$169.80**
54151HACS	Cybersecurity Specialist I (ClearFocus)			**$92.95**	**$95.74**	**$98.61**
54151HACS	Cybersecurity Specialist II (ClearFocus)			**$113.89**	**$117.31**	**$120.83**
54151HACS	Cybersecurity Specialist III (ClearFocus)			**$144.75**	**$149.09**	**$153.56**
54151HACS	Cybersecurity Specialist IV (ClearFocus)			**$183.78**	**$189.29**	**$194.97**

54151HACS	Cybersecurity Subject Matter Expert I (ClearFocus)			**$118.29**	**$121.83**	**$125.49**
54151HACS	Cybersecurity Subject Matter Expert II (ClearFocus)			**$122.77**	**$126.46**	**$130.26**
54151HACS	Cybersecurity Subject Matter Expert III (ClearFocus)			**$159.22**	**$164.00**	**$168.92**
54151HACS	Cybersecurity Subject Matter Expert IV (ClearFocus)			**$224.73**	**$231.47**	**$238.41**
54151S	Business Analyst II	$105.79	$108.97	**$112.23**	**$115.60**	**$119.06**
54151S	Business Analyst III	$128.94	$132.81	**$136.79**	**$140.89**	**$145.11**
54151S	Business Analyst IV	$148.18	$152.62	**$157.20**	**$161.91**	**$166.77**
54151S	Program Manager	$163.35	$168.24	**$173.29**	**$178.49**	**$183.84**
54151S	Solutions Developer II	$120.71	$124.32	**$128.05**	**$131.89**	**$135.85**
54151S	Solutions Developer III	$137.88	$142.03	**$146.29**	**$150.68**	**$155.20**
54151S	Solutions Developer IV	$153.29	$157.88	**$162.62**	**$167.50**	**$172.52**
54151S	Solutions Integrator/Analyst IV	$123.02	$126.71	**$130.51**	**$134.43**	**$138.46**
54151S	Sr. Solutions Architect	$177.07	$182.38	**$187.85**	**$193.48**	**$199.28**
54151S	Sr. Subject Matter Expert	$150.96	$155.49	**$160.15**	**$164.96**	**$169.90**

SERVICE CONTRACT LABOR STANDARDS (SCLS) MATRIX

The Service Contract Labor Standards (SCLS), formerly known as the Service Contract Act (SCA), is applicable to this contract as it applies to the entire Multiple Award Schedule (MAS) and all services provided.

While no specific labor categories have been identified as being subject to SCLS/SCA due to exemptions for professional employees (FAR 22.1101, 22.1102 and 29 CRF 541.300), this contract still maintains the provisions and protections for SCLS/SCA eligible labor categories.

If and / or when the contractor adds SCLS/SCA labor categories to the contract through the modification process, the contractor must inform the Contracting Officer and establish a SCLS/SCA matrix identifying the GSA labor category titles, the occupational code, SCLS/SCA labor category titles and the applicable WD number. Failure to do so may result in cancellation of the contract.

LABOR CATEGORY DESCRIPTIONS

Labor Category Title	Labor Category Description	Minimum Education	Minimum Years of Experience
Cybersecurity Project Manager II (ClearFocus)	The Cybersecurity Project Manager II is responsible for managing the planning, execution, and delivery of government contracts, ensuring adherence to project goals, timelines, and regulatory requirements. This role involves overseeing day-to-day project activities, coordinating with stakeholders, and tracking progress to ensure successful completion within scope, budget, and schedule. The Project Manager will support risk management, resolve issues, and assist with reporting on project status and deliverables. This position requires experience in government contracting and the ability to manage project tasks and team coordination in compliance with federal standards and client expectations.	Bachelors	2
Cybersecurity Project Manager III (ClearFocus)	The Cybersecurity Project Manager III is responsible for overseeing the planning, execution, and delivery of complex government contracts, ensuring alignment with client requirements, project goals, and regulatory standards. This role involves managing all aspects of the project lifecycle, from initiation through to successful completion, while maintaining control over scope, schedule, budget, and quality. The Project Manager III will lead a team of project professionals, coordinate with stakeholders, and mitigate risks to ensure project objectives are met efficiently. This position requires extensive experience in managing government programs, strong leadership skills, and in-depth knowledge of federal contracting processes and compliance requirements. The Project Manager III will be the primary point of contact for client communication, ensuring clear and effective reporting on project progress, deliverables, and any issues or changes.	Bachelors	5
Cybersecurity Analyst I (ClearFocus)	The Cybersecurity Analyst I provides foundational technical support to government programs, focusing on ensuring the security and compliance of information systems. Responsibilities include assisting with risk assessments, supporting the application of	Bachelors	1

	cybersecurity frameworks to identify and manage security risks, and helping implement security controls. The Cybersecurity Analyst I participates in continuous monitoring efforts, assists with vulnerability assessments, and supports compliance with federal cybersecurity requirements, including FISMA and NIST standards. Additionally, the Cyberescurity Analyst I may monitor security alerts, analyze security incidents, and escalate potential threats as necessary. The role requires basic knowledge of FISMA, NIST, and cybersecurity best practices, as well as the ability to communicate security issues and solutions effectively. Experience in system security, risk management, and compliance support is desirable.		
Cybersecurity Analyst II (ClearFocus)	The Cybersecurity Analyst II provides technical support and expertise to programs, focusing on ensuring the security and compliance of information systems. Responsibilities include conducting risk assessments, applying cybersecurity frameworks to assess and manage security risks, and supporting the development and implementation of security controls. The Cybersecurity Analyst II conducts continuous monitoring, supports vulnerability assessments, and ensures compliance with federal cybersecurity requirements, including FISMA and NIST standards. Additionally, the Cyberescurity Analyst II may monitor security alerts, analyze security incidents, escalate potential threats as necessary, investigate security events, respond to incidents, and coordinate with other teams to remediate vulnerabilities. The role requires proficiency in FISMA and NIST security standards, strong knowledge of cybersecurity tools and techniques, and the ability to communicate security issues and solutions to both technical and non-technical stakeholders. Experience includes risk management, system security, compliance reporting, and SOC operations.	Bachelors	2
Cybersecurity Analyst III (ClearFocus)	The Cybersecurity Analyst III provides advanced technical expertise and leadership in ensuring the security and compliance of information systems for government programs. Responsibilities include leading risk assessments, applying and enhancing cybersecurity frameworks to manage and mitigate security risks, and providing guidance on the implementation of security controls. The Cybersecurity Analyst III oversees continuous monitoring efforts, conducts in-depth vulnerability assessments, and ensures that systems comply with federal cybersecurity requirements, including FISMA and NIST standards.	Bachelors	5

	Additionally, the Cyberescurity Analyst III may escalate potential threats as necessary, investigate security events, respond to incidents, and coordinate with other teams to remediate vulnerabilities. This role requires deep proficiency in FISMA, NIST, and other cybersecurity frameworks, advanced knowledge of cybersecurity tools and techniques, and the ability to effectively communicate complex security issues and solutions to both technical and non-technical stakeholders. Extensive experience in risk management, system security, compliance reporting, and leading cybersecurity initiatives is essential.		
Cybersecurity Administrator II (ClearFocus)	The Cybersecurity Administrator II is responsible for the configuration, maintenance, and management of secure computer systems and networks supporting government contracts. This role focuses on ensuring system performance, security, and compliance with federal cybersecurity standards. Responsibilities include implementing and maintaining security controls, monitoring system health for vulnerabilities, applying patches and updates, troubleshooting security incidents, and resolving technical issues to ensure system reliability and integrity. The Cybersecurity Administrator II collaborates with project teams to implement security changes, conduct system audits, and ensure systems meet security and operational standards in compliance with program requirements and federal regulations. This position requires experience in system administration with a focus on cybersecurity, strong problem-solving skills, and the ability to ensure systems meet both security and operational standards for government programs.	Bachelors	2
Cybersecurity Administrator III (ClearFocus)	The Cybersecurity Administrator III is responsible for the advanced configuration, maintenance, and management of secure computer systems and networks supporting government contracts. This role ensures the highest levels of system performance, security, and compliance with federal cybersecurity standards. Responsibilities include leading the implementation and enforcement of security controls, performing proactive system monitoring for vulnerabilities, applying critical patches and updates, troubleshooting complex security incidents, and resolving technical issues to maintain system integrity. The Cybersecurity Administrator III works closely with project teams to design and implement security measures, conduct system audits, and ensure all systems meet security and	Bachelors	5

	operational standards in compliance with program requirements and federal regulations. This position requires extensive experience in system administration with a focus on cybersecurity, advanced problem-solving skills, and the ability to lead efforts to ensure systems meet rigorous security and operational standards for government programs.		
Cybersecurity Engineer I (ClearFocus)	The Cybersecurity Engineer I provides foundational support in the design, implementation, and maintenance of security solutions to protect government systems and networks. Responsibilities include assisting with security assessments, implementing security controls, and supporting the integration of cybersecurity measures into system development and operations. The Cybersecurity Engineer I monitors system performance for vulnerabilities, assists in troubleshooting security incidents, and helps ensure compliance with federal cybersecurity regulations, including FISMA and NIST. This role requires a basic understanding of cybersecurity principles, security protocols, and the ability to apply technical solutions to support security and compliance requirements for government programs. Experience in cybersecurity engineering or related fields is desirable.	Bachelors	1
Cybersecurity Engineer II (ClearFocus)	The Cybersecurity Engineer II is responsible for designing, implementing, and maintaining security solutions to protect systems and networks. This role involves assessing security requirements, developing security architectures, and applying cybersecurity best practices to safeguard critical data and infrastructure. The Cybersecurity Engineer II collaborates with project teams to implement security controls, conduct risk assessments, and ensure compliance with federal cybersecurity regulations, including FISMA and NIST. Responsibilities also include monitoring system performance for potential vulnerabilities, troubleshooting security incidents, and ensuring the integration of security measures into all phases of system development and operations. This position requires experience in cybersecurity engineering, strong knowledge of security protocols, and the ability to apply technical solutions to meet security and compliance standards for government programs.	Bachelors	2
Cybersecurity Engineer III (ClearFocus)	The Cybersecurity Engineer III is responsible for leading the design, implementation, and maintenance of advanced security solutions to protect government systems and networks. This role involves conducting comprehensive security assessments, developing and	Bachelors	5

	optimizing security architectures, and applying cutting-edge cybersecurity strategies to safeguard critical infrastructure. The Cybersecurity Engineer III leads efforts to implement security controls, conduct risk assessments, and ensure full compliance with federal cybersecurity regulations, including FISMA and NIST. Responsibilities also include overseeing system performance for vulnerabilities, managing complex security incidents, and guiding the integration of security measures across all phases of system development and operations. The Cybersecurity Engineer III collaborates with cross-functional teams to ensure that security objectives align with program goals and regulatory requirements. This position requires extensive experience in cybersecurity engineering, deep knowledge of security protocols and tools, and the ability to deliver innovative security solutions that meet the highest standards for government programs.		
Cybersecurity Specialist I (ClearFocus)	The Cybersecurity Specialist I provides foundational technical support to programs by assisting in the implementation, troubleshooting, and maintenance of cybersecurity systems and solutions. Responsibilities include supporting security analyses, assisting with the configuration and maintenance of security controls, and helping integrate cybersecurity measures into existing systems. The Cybersecurity Specialist I may also assist with basic penetration testing activities to identify vulnerabilities, support threat hunting efforts to detect potential threats, and help with security engineering tasks to strengthen system security. The role involves collaborating with cross-functional teams to execute cybersecurity tasks, maintaining technical documentation related to security measures, and assisting in identifying improvements to system security. The position requires strong technical problem-solving skills, effective communication abilities, and a basic understanding of cybersecurity tools, technologies, and methodologies, including penetration testing tools, threat hunting platforms, IDS/IPS, and security monitoring tools.	Bachelors	1
Cybersecurity Specialist II (ClearFocus)	The Cybersecurity Technical Specialist II provides hands-on technical expertise to programs by implementing, troubleshooting, and optimizing cybersecurity systems and solutions. Responsibilities include performing detailed security analyses, configuring and maintaining security controls, supporting the integration of cybersecurity measures into existing	Bachelors	2

	systems, and resolving security-related issues to ensure operational efficiency. The Cybersecurity Specialist II ,may also be responsible for conducting penetration testing to identify vulnerabilities, performing threat hunting to detect potential threats, and supporting security engineering efforts to design and implement robust security infrastructures. The Cybersecurity Technical Specialist II collaborates with cross-functional teams to execute cybersecurity tasks, prepares and maintains technical documentation related to security measures, and provides recommendations to improve system security and resilience. The role requires strong technical problem-solving skills, effective communication abilities, and proficiency in relevant cybersecurity tools, technologies, and methodologies, including penetration testing tools (e.g., Kali Linux, Metasploit), threat hunting platforms, IDS/IPS, vulnerability management, and security monitoring tools.		
Cybersecurity Specialist III (ClearFocus)	The Cybersecurity Specialist III provides advanced technical expertise and leadership in the implementation, troubleshooting, and optimization of cybersecurity systems and solutions for programs. Responsibilities include conducting in-depth security analyses, designing and configuring robust security controls, and overseeing the integration of advanced cybersecurity measures into existing systems. The Cybersecurity Specialist III leads efforts in penetration testing to identify vulnerabilities, performs proactive threat hunting to detect and mitigate emerging threats, and plays a key role in security engineering to design and implement secure infrastructures. Additionally, the Specialist conducts comprehensive security control assessments to evaluate and ensure the effectiveness of security measures. The role involves collaborating with cross-functional teams, preparing and maintaining detailed technical documentation, and providing strategic recommendations to improve system security and resilience. The Cybersecurity Specialist III requires strong leadership skills, advanced problem-solving capabilities, and deep proficiency in cybersecurity tools and methodologies, including penetration testing tools (e.g., Kali Linux, Metasploit), threat hunting platforms, IDS/IPS, vulnerability management, and security monitoring tools. The position also requires the ability to communicate complex security issues and solutions effectively to both technical and non-technical stakeholders.	Bachelors	5

Cybersecurity Specialist IV (ClearFocus)	The Cybersecurity Specialist IV provides expert-level leadership and strategic guidance in the design, implementation, and optimization of cybersecurity systems and solutions for programs. Responsibilities include leading complex security analyses, developing and implementing advanced security architectures, and overseeing the integration of cutting-edge cybersecurity measures across enterprise systems. The Cybersecurity Specialist IV may direct penetration testing efforts to identify and address high-risk vulnerabilities, leads proactive threat hunting initiatives to detect and mitigate sophisticated threats, and drives security engineering efforts to build and maintain resilient infrastructures. Additionally, the Specialist conducts comprehensive security control assessments, ensuring the effectiveness of security measures and compliance with federal standards. The role involves collaborating with senior leadership and cross-functional teams to define cybersecurity strategies, preparing and presenting high-level technical documentation, and providing expert recommendations to enhance overall system security and resilience. The Cybersecurity Specialist IV requires exceptional leadership, advanced problem-solving skills, and extensive experience with cybersecurity tools and methodologies, including penetration testing tools (e.g., Kali Linux, Metasploit), threat hunting platforms, IDS/IPS, vulnerability management, and security monitoring tools. The position also requires the ability to communicate complex security strategies and solutions to both technical and executive-level stakeholders.	Bachelors	7
Cybersecurity Subject Matter Expert I (ClearFocus)	The Cybersecurity Subject Matter Expert (SME) I provides foundational technical expertise and support in the cybersecurity domain, assisting with the protection of systems, networks, and data. Responsibilities include supporting the identification and resolution of cybersecurity challenges, helping to develop security solutions, and contributing to the implementation of program strategies to address emerging threats. The Cybersecurity SME I assists in ensuring compliance with organizational goals and federal cybersecurity regulations. The role involves conducting basic security analyses, providing input on risk management and mitigation, and supporting the preparation of technical documentation and briefings. The Cybersecurity SME I also helps implement cybersecurity measures and assists in ensuring compliance with federal standards such as FISMA, NIST, and other	Bachelors	1

	relevant frameworks. The position requires a basic understanding of cybersecurity principles, strong analytical skills, effective communication abilities, and the ability to work collaboratively within a team to support the overall security posture of government programs.		
Cybersecurity Subject Matter Expert II (ClearFocus)	The Cybersecurity Subject Matter Expert (SME) II provides specialized technical expertise and support in the cybersecurity domain, utilizing strong knowledge and experience in securing systems, networks, and data. Responsibilities include advising on cybersecurity challenges, assisting in the development of security solutions, and contributing to the shaping of program strategies to address emerging threats. The Cybersecurity SME II helps ensure alignment with organizational goals and federal cybersecurity regulations. The role involves conducting security analyses, providing recommendations on risk management and mitigation, delivering briefings to technical and non-technical stakeholders, and supporting the mentoring of junior team members. The Cybersecurity SME II is also responsible for assisting in the implementation of cybersecurity measures, ensuring compliance with federal standards such as FISMA, NIST, and other relevant frameworks. The position requires strong analytical skills, effective communication abilities, and a proven track record in the cybersecurity field, supporting the overall security posture of government programs.	Bachelors	2
Cybersecurity Subject Matter Expert III (ClearFocus)	The Cybersecurity Subject Matter Expert (SME) III provides specialized expertise and strategic guidance in the cybersecurity domain, leveraging deep knowledge and extensive experience in securing systems, networks, and data. Responsibilities include advising on complex cybersecurity challenges, developing innovative security solutions, shaping program strategies to address emerging threats, and ensuring alignment with organizational goals and federal cybersecurity regulations. The Cybersecurity SME III conducts high-level security analyses, provides expert recommendations on risk management and mitigation, delivers executive-level briefings on cybersecurity posture, and mentors team members to enhance program performance and security outcomes. The role requires exceptional analytical and critical thinking skills, advanced communication and presentation abilities, and a proven track record of leadership in the cybersecurity field. The Cybersecurity SME III	Bachelors	5

	is also responsible for guiding the integration of cutting-edge cybersecurity measures, ensuring compliance with standards such as FISMA, NIST, and other federal frameworks, and influencing strategic decisions to strengthen the overall security posture of government programs.		
Cybersecurity Subject Matter Expert IV (ClearFocus)	The Cybersecurity Subject Matter Expert (SME) IV provides expert-level leadership and strategic direction in the cybersecurity domain, leveraging extensive experience and deep knowledge to safeguard complex systems, networks, and data. Responsibilities include leading the development of advanced cybersecurity strategies, advising on high-level security challenges, and driving the implementation of innovative solutions to address emerging and evolving threats. The Cybersecurity SME IV ensures alignment with organizational goals and federal cybersecurity regulations, influencing security policies and program direction at the highest levels. The role involves conducting comprehensive security analyses, providing expert recommendations on risk management, delivering executive-level briefings, and mentoring senior team members to enhance program performance and security outcomes. The Cybersecurity SME IV leads the integration of cutting-edge cybersecurity measures, ensures compliance with frameworks such as FISMA, NIST, and other federal standards, and plays a key role in shaping long-term cybersecurity strategies for government programs. The position requires exceptional leadership, advanced analytical and problem-solving skills, and the ability to communicate complex security strategies to both technical and executive stakeholders.	Bachelors	7
Business Analyst II (Procentrix, MFC: All Commercial Customers)	Under little or no supervision, applies analytical skills to support Information Technology (IT) business solution development and process improvement efforts. Performs activities such as requirements analysis, analysis and creation of policies, procedures, business cases and cost justifications. May also participate in Business Impact Assessments (BIAs).	Bachelors	4

	Collects and analyzes requirements and measurement criteria as related to business process optimization and business solution implementation efforts. Is knowledgeable of industry standard requirements analysis methodologies and notations such as UML, IDEF, etc.		
Business Analyst III (Procentrix, MFC: All Commercial Customers)	Leads analysis and design activities in support of Information Technology (IT) business solution development and process improvement efforts. Typical duties include strategic planning, requirements analysis, identification of key performance indicators (KPI), analysis and creation of policies, procedures, business cases and cost justifications. Meets with stakeholders to capture requirements and success criteria. May facilitate Joint Applications Development (JAD) sessions or utilize other requirements elicitation techniques such as surveys. May also perform Business Impact Assessments (BIAs). Is knowledgeable of industry standard requirements analysis methodologies and notations such as UML, IDEF, etc. May oversee the efforts of one or more analyst personnel. Possesses experience with requirements management tools or techniques	Bachelors	6
Business Analyst IV (Procentrix, MFC: All	Leads analysis and design activities in support of Information Technology (IT) business solution development and process improvement efforts.	Bachelors	8

Commercial Customers)	Typical duties include strategic planning, requirements analysis, identification of key performance indicators (KPI), analysis and creation of policies, procedures, business cases and cost justifications. Meets with stakeholders to capture requirements and success criteria. May facilitate Joint Applications Development (JAD) sessions or utilize other requirements elicitation techniques such as surveys. May also perform Business Impact Assessments (BIAs). Is knowledgeable of industry standard requirements analysis methodologies and notations such as UML, IDEF, etc. May oversees the efforts of one or more analyst personnel. Possesses experience with requirements management tools or techniques.		
Program Manager (Procentrix, MFC: All Commercial Customers)	Performs day-to-day program management activities relevant to project initiation, planning, execution, monitoring and closing. Applies project management best practices and organizational standards to guide project teams. Controls project scope, resource allocation, budget, schedule, and service quality. Communicates with senior program managers, senior management, and clients to ensure critical program-related issues are addressed	Bachelors	6

Solutions Developer II (Procentrix, MFC: All Commercial Customers)	Under little or no supervision, supports the development of software and hardware-based business solutions. Supports the performance of activities such as: Combining one or more COTS or GOTS products or extending their standard functionality to meet the overall functional and technical and security specifications as set forth by the Solution Architects and Business Analysts. Developing custom services, components, or modules using advanced programming languages such as J2EE, .NET, Active Server Pages, Python, or C++. Assessing, planning, designing, developing, testing, configuring, and deploying technical solutions that address business challenges. Translating architectural design into working business solutions by leveraging skills in systems design, development, process automation, System Orchestration And Response (SOAR), and technical knowledge	Bachelors	4
Solutions Developer III (Procentrix, MFC: All Commercial Customers)	Develops or overseeing the development of software and hardware-based business solutions. Performs activities such as: Combining one or more COTS or GOTS products or extending their standard functionality to meet the overall functional and technical and security specifications as set forth by the Solution Architects and Business Analysts. Developing custom services, components, or modules using advanced programming	Bachelors	6

	languages such as J2EE, .NET, Active Server Pages, Python, or C++. Assessing, planning, designing, developing, testing, configuring, and deploying technical solutions that address business challenges. Translating architectural design into working business solutions by leveraging skills in systems design, development, process automation, System Orchestration And Response (SOAR), and technical knowledge.		
Solutions Developer IV (Procentrix, MFC: All Commercial Customers)	Develop or overseeing the development of software and hardware-based business solutions. Performs activities such as: Combining one or more COTS products or extending their standard functionality to meet the overall functional, technical and security specifications as set forth by the Solution Architects and Business Analysts. Developing custom services, components, or modules using advanced programming languages such as J2EE, .NET, Active Server Pages, Python, or C++. Assessing, planning, designing, developing, testing, configuring, and deploying technical solutions addressing business challenges. Translating architectural design into working business solutions by leveraging skills in systems design, development, business process automation, System Orchestration And Response (SOAR), technical knowledge and leadership.	Bachelors	8
Solutions Integrator/Analyst IV (Procentrix, MFC: All	Performs or leads activities involving system assessments, system analysis, system design, process definition, process optimization and performance measurement.	Bachelors	6

Commercial Customers)	May also support solution teams in system development, security compliance, component and software integration, testing, and installation		
Sr. Solution Architect (Procentrix, MFC: All Commercial Customers)	Leads the creation of architectural designs for complex automation solutions that may involve a mix of COTS and custom products collectively addressing topics such as security, knowledge management, workflow, process automation, service-oriented architecture (SOA), data warehousing, business intelligence or enterprise software /hardware products. May provide overall leadership of architectural decisions made on one or more projects. Designs architectures to address business requirements and security concerns and develops plans for present and future compatibility and interface support. Ensures architectures are in compliance with government-wide, industry, or client-specific security and other standards. Evaluates compatibility of system implementation efforts with organization architectures and recommends adjustments, as appropriate. Provides consulting support on complex or emerging technologies.	Bachelors	5
Sr. Subject Matter Expert (ClearFocus, MFC: All Commercial Customers)	Provides expert guidance and leadership to project teams or clients in specialized technical or functional disciplines such as Information Security, Data Architecture, Knowledge Management, Financial Management, Human Resources Management, Acquisition Management, Operations Management or Quality Management. Provides advice often based on government or industry best practices/standards, on how to effectively implement solutions or improvements to business challenges.	Bachelors	7

	Often a recognized thought leader in specialized areas of industry or government policy, procedures, processes, or legislation. Supports implementation teams with expert knowledge that maximizes the effectiveness of overall business solutions.		