GENERAL SERVICES ADMINISTRATION

FEDERAL SUPPLY SERVICE

AUTHORIZED FEDERAL SUPPLY SCHEDULE CATALOG/PRICE LIST

On-line access to contract ordering information, terms and conditions, up-to-date pricing, and the option to create an electronic delivery order is available through **GSA** *Advantage!,* a menu-driven database system. The INTERNET address for **GSA** *Advantage!* is **http://www.gsaadvantage.gov**

SCHEDULE TITLE: MAS – MULTIPLE AWARD SCHEDULE

FSC GROUP: INFORMATION TECHNOLOGY

CONTRACT NUMBER: 47QTCA20D00BS

CONTRACT PERIOD: October 1, 2024 through September 30, 2034

For more information on ordering from Federal Supply go to this website: **www.fss.gsa.gov**

CONTRACTOR: STEEL TOAD CONSULTING LLC
5520 Research Park Dr. Ste 100
Baltimore, MD 21228-4851
Phone number: 1-833-333-8623
Fax number: (833) 754-9412

Email: **Julie@SteelToad.com**

CONTRACTOR'S ADMINISTRATION SOURCE:

Julie Sheehan
STEEL TOAD CONSULTING LLC
5520 Research Park Dr. Ste 100
Baltimore, MD 21228-4851
Phone number: 1-833-333-8623
Fax number: (833) 754-9412
Email: **Julie@SteelToad.com**

WEBSITE: www. steeltoad.com

BUSINESS SIZE: Small Business

BUSINESS TYPE: Small Business

CUSTOMER INFORMATION:

1a. TABLE OF AWARDED SPECIAL ITEM NUMBERS (SINs)

SIN	DESCRIPTION
54151S	Information Technology Professional Services
611420	Computer Training
54151HACS	Highly Adaptive Cybersecurity Services (HACS)
OLM	Order-Level Materials

1b. LOWEST PRICED MODEL NUMBER AND PRICE FOR EACH SIN:
(Government net price based on a unit of one)
See attached APPENDIX A – GSA PROPOSED 54151S - Information Engineer On-site PRICE - $130.71; 54151 HACS – Cyber Media Administrator I – PRICE - $82.02 611420 -CMMI® V2.0 BUILDING SERVICES EXCELLENCE -$537.53

1 c. HOURLY RATES (Services only):
See attached APPENDIX A – GSA PROPOSED PRICE LIST

2. **MAXIMUM ORDER*: $500,000**

NOTE TO ORDERING ACTIVITIES: *If the best value selection places your order over the Maximum Order identified in this catalog/pricelist, you have an opportunity to obtain a better schedule contract price. Before placing your order, contact the aforementioned contactor for a better price. The contractor may (1) offer a new price for this requirement (2) offer the lowest price available under this contract or (3) decline the order. A delivery order that exceeds the maximum order may be placed under the schedule contract in accordance with FAR 8.404.

3. **MINIMUM ORDER: $100.00**

4. **GEOGRAPHIC COVERAGE**: **50 States; DC**

5. **POINT(S) OF PRODUCTION**: **N/A**

6. **DISCOUNT FROM LIST PRICES:** ***GSA Net Prices are shown on the attached GSA Pricelist.***

7. **QUANTITY DISCOUNT(S): None**

8. **PROMPT PAYMENT TERMS: 0.00%; Net 30 Days – Prompt payment terms cannot be negotiated out of the contractual agreement in exchange for other concessions**

9. **FOREIGN ITEMS**: **Not Applicable**

10a. **TIME OF DELIVERY**: **Subject to Task Order**

10b. **EXPEDITED DELIVERY: Contact Contractor**

10c. **OVERNIGHT AND 2-DAY DELIVERY: Contact Contractor**

10d. **URGENT REQUIRMENTS:** Agencies can contact the Contractor's representative to affect a faster delivery. Customers are encouraged to contact the contractor for the purpose of requesting accelerated delivery.

11. **FOB POINT: Destination**

12a. **ORDERING ADDRESS: Same as Contractor**

12b. ORDERING PROCEDURES: For supplies and services, the ordering procedures, information on Blanket Purchase Agreements (BPA's) are found in Federal Acquisition Regulation (FAR) 8.405-3

13. PAYMENT ADDRESS: SteelToad Consulting LLC
PO Box 434
2323 Spencerville Road
Spencerville, MD 20868

14. WARRANTY PROVISION: ONE (1) Year, Standard Commercial Warranty. Customer should contact contractor for a copy of the warranty.

15. EXPORT PACKING CHARGES: 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 AVAILABLE):
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. Section 508 Compliance for Electronic and Information Technology (EIT):
Not Applicable

23. UNIQUE ENTITY IDENTIFIER (UEI) NUMBER: MLK6AHF6VHW4

24. NOTIFICATION REGARDING REGISTRATION IN SYSTEM FOR AWARD MANAGEMENT (SAM) DATABASE: Contractor has an Active Registration in the SAM database. Cage Code: 8DTM7

APPENDIX A LABOR CATEGORY DESCRIPTIONS

APPENDIX B TRAINING COURSE DESCRIPTIONS

APPENDIX C GSA PRICE LIST

APPENDIX A

LABOR CATEGORY DESCRIPTIONS

Network Engineer

Education: Bachelor's Degree
Years of Experience: 4

Responsibilities :

Performs duties associated with the design, testing and implementation of Local Area Networks, Wide Area Networks or Cloud Networks. Provides technical support related to LAN/WAN/Hybrid activities and end user needs. Must be experienced in the design and integration of multiple network operating systems, protocols and topologies. Develops standardized procedures for LAN/WAN/Hybrid operation and associated documentation. Evaluates new technology and makes recommendations for implementation. Analyzes requirements for system upgrades and implementations including hardware/software resources, logistics and planning issues, testing and training.

Application Developer

Education: Bachelor's Degree
Years of Experience: 3

Responsibilities :

Participates in all phases of the software development life cycle including the design, development, integration, testing and implementation phases. Performs quality assurance and technical review activities. Assists in the resolution of end-user software problems. Works with management and end-user groups to identify requirements for future product enhancements. Develops technical documentation, end-user documentation and training materials.

Project Manager

Education: Bachelor's Degree
Years of Experience: 4
Responsibilities:

Assists with the maintenance, tasks, planning and execution of project schedules as well as the preparation and delivery of status reports to the customer. Point of contact for the customer. Interacts with project staff and the customer to help coordinate activities. May serve as technical lead for the project.

Senior Subject Matter Expert

Education: Master's Degree
Years of Experience: 8
Responsibilities:

Provides expert consultative support to a functional technical area of the project. Develops solutions to complex problems. Works closely with the information technologists to identify the best technological solution to technical issues. May supervise the activities of other subject matter experts or technical personnel.

Senior Database Administrator

Education: Bachelor's Degree
Years of Experience: 5
Responsibilities :

Must have significant technical experience designing logical data models, implementing physical schema, and implementing and maintaining databases. Experience should include participation in all phases of the database development life cycle, including the data model design, physical schema implementation, application development, integration, testing, production operation, performance tuning, quality assurance, technical review, and assisting in the resolution of end-user problems for IT. Must have demonstrated expertise and experience in designing and implementing security features for structured or unstructured databases and for protecting data for the Confidentiality, Integrity and Availability (CIA) in database management systems.

IT Security Engineer

Education: Bachelor's Degree
Years of Experience: 3
Responsibilities :

Experience should include performing research on system vulnerabilities, assisting developers in the design of secure applications, conducting system penetration studies, acquiring and implementing computer security incident response tools, monitoring networks to detect intrusions, briefing management and security personnel on the incidents, and using automated tools to perform network monitoring, intrusion detection, and reaction to incidents for IT. Experience should also include security hardware/software integration as well as a strong background in network security design or development. Security experience in more than one of the security domains should include: Security and Risk Management, Asset Security, Security Architecture and Engineering, Communications and Network Security, Identity and Access Management, Security Assessment and Testing, Security Operations and Software Development Security.

Business Analyst

Education: Associates Degree

Years of Experience: 3

Responsibilities :

Provide expertise in business process and system analysis, design, improvement, and implementation efforts and in translating business process needs into technical requirements. Provide expertise in change management and training support. Provide organizational and strategic planning for a wide variety of technical and functional environments. Provide expertise in, but not limited to, Configuration Management, Strategic Planning, Knowledge Management, Business Analysis and Technical Analysis. Develop, record, and keep updated a process architecture that describes the structure of the organization's processes and process assets.

Senior Business Analyst

Education: Bachelor's Degree

Years of Experience: 5

Responsibilities :

Assist in applying common best practices for the industry to the customer using a knowledge base to create conceptual business models and to identify relevant issues and considerations in selecting application software packages. Assess the operational and functional baseline of an organization and its organizational component and help to define the direction and strategy for an engagement while ensuring the organizational needs are being addressed. Typical areas addressed include Human Resources, Finance, Supply, and operations. Identify information technology inadequacies and/or deficiencies that affect the functional area's ability to support/meet organizational goals. Generate functional area strategies for enhanced IT operations in a cross-functional area mode throughout the organization. Participate in account strategy sessions, strategic assessments and design reviews to validate enterprise approach and associated work products, such as ERP implementations coordinating the resolution of highly complex problems and tasks. Develop, record, and keep updated a process architecture that describes the structure of the organization's processes and process assets.

Information Engineer

Education: Bachelor's Degree

Years of Experience: 3

Responsibilities :

Apply business process improvement practices to re-engineer methodologies/principles and business process modernization projects. Apply, as appropriate, activity and data modeling, transaction flow analysis, internal control and risk analysis and modern business methods and performance measurement techniques. Assist in establishing standards for information systems procedures. Develop and apply organization-wide information models for use in designing and building integrated, shared software and database management systems and data warehouses. Construct sound, logical business improvement opportunities consistent with corporate Information Management guiding principles, cost savings, and open system architecture objectives. Identify the most critical objectives to business success. establish performance improvement objectives based on the organization's business objective, identify infrastructure needs to support improvement efforts, identify measures of success for meeting objectives, develop an improvement plan and keep it updated and continually communicate with stakeholders. Training and/or certification concentration would include ITIL, Professional Engineering and/or CompTIA or similar training.

Senior Information Engineer

Education: Bachelor's Degree
Years of Experience: 5

Responsibilities :

Apply an enterprise-wide set of disciplines for the planning, analysis, design and construction of information systems on an enterprise-wide basis or across a major sector of the enterprise. Develop analytical and computational techniques and methodology for problem solutions. Identify the most critical objectives to business success. establish performance improvement objectives based on the organization's business objective, identify infrastructure needs to support improvement efforts, identify measures of success for meeting objectives, develop an improvement plan and keep it updated and continually communicate with stakeholders. Perform enterprise wide strategic systems planning, business information planning, business and analysis. Perform process and data modeling in support of the planning and analysis efforts using both manual and automated tools; such as Integrated Computer-Aided Software Engineering tools. Apply reverse engineering and re-engineering disciplines to develop migration strategic and planning documents. Provide technical guidance in software engineering techniques and automated support tools. Provide daily supervision and direction to staff.

Cyber Incident Response Analyst I

Education: Bachelor's Degree
Years of Experience: 3

Responsibilities:

Contributes to generating response to crisis or urgent situations to mitigate immediate or potential threats. Handle incidents or potential events that indicate a negative impact on service delivery. Address incidents in a timely and effective manner according to the terms of applicable customer agreements and requirements. Resolving incidents may result in a change to the service delivery approach. Perform incident resolution and prevention by following a process to address incidents reported by customers, end users, and affected stakeholders. Uses mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security. Duties may include Handle and respond to cyber security incidents through coordination with stakeholders such as internal IT entities, security leadership, legal affairs, internal affairs, law enforcement, and privacy offices. Intake incident reporting, conduct ticket updates, and notify stakeholders of cyber security incidents and forensic investigations in relation to computer security incidents and escalate when necessary as well as coordinate response to computer security incidents. Recommend a course of action on manages, and records all actions taken and serve as initial POC for Events of Interest reported both internally and externally. Establishes alarm/incident escalation process and tracks, follows-up, and resolves incidents. Initiates and maintains contact with affected parties during incident resolution. Determine the source of computer incidents and take appropriate corrective actions.

- Initiate problem reports, as required, and ensure that incidents are resolved in a timely manner.
- Familiar with the network, system and applications.
- Answer inquiries regarding specific systems.
- Provide first tier support to business user and customer.
- Provide technical support for computerized telecommunications processing.
- Maintain documentation of vendor software, including issuance of new releases and problem fixes, as well as documentation of utilities and systems developed in house.
- Communicate with IS operations to signal abnormal patterns in calls or application behavior.

Cyber Incident Response Analyst II

Education: Bachelor's Degree

Years of Experience: 5

Responsibilities:

Contributes to generating response to crisis or urgent situations to mitigate immediate or potential threats. Handle incidents or potential events that indicate a negative impact on service delivery. Address incidents in a timely and effective manner according to the terms of applicable customer agreements and requirements. Resolving incidents may result in a change to the service delivery approach. Perform incident resolution and prevention by following a process to address incidents reported by customers, end users, and affected stakeholders. Uses mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security. Duties may include Handle and respond to cyber security incidents through coordination with stakeholders such as internal IT entities, security leadership, legal affairs, internal affairs, law enforcement, and privacy offices. Intake incident reporting, conduct ticket updates, and notify stakeholders of cyber security incidents and forensic investigations in relation to computer security incidents and escalate when necessary as well as coordinate response to computer security incidents. Recommend a course of action on manages, and records all actions taken and serve as initial POC for Events of Interest reported both internally and externally. Establishes alarm/incident escalation process and tracks, followsup, and resolves incidents. Initiates and maintains contact with affected parties during incident resolution. Typically is managed by an Incident manager.

Determine the source of computer incidents and take appropriate corrective actions.

- Initiate problem reports, as required, and ensure that incidents are resolved in a timely manner.
- Obtain detailed knowledge of the network, system and applications.
- Answer inquiries regarding specific systems.
- Provide second- and third-tier support to business user and customer.
- Provide technical support for computerized telecommunications processing.
- Maintain documentation of vendor software, including issuance of new releases and problem fixes, as well as documentation of utilities and systems developed in house.
- Communicate with IS operations to signal abnormal patterns in calls or application behavior.

Cyber Incident Response Analyst III

Education: Bachelor's Degree

Years of Experience: 8

Responsibilities:

Contributes to generating response to crisis or urgent situations to mitigate immediate or potential threats. Handle incidents or potential events that indicate a negative impact on service delivery. Address incidents in a timely and effective manner according to the terms of applicable customer agreements and requirements. Resolving incidents may result in a change to the service delivery approach. Perform incident resolution and prevention by following a process to address incidents reported by customers, end users, and affected stakeholders. Uses mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security. Duties may include Handle and respond to cyber security incidents through coordination with stakeholders such as internal IT entities, security leadership, legal affairs, internal affairs, law enforcement, and privacy offices. Intake incident reporting, conduct ticket updates, and notify stakeholders of cyber security incidents and forensic investigations in relation to computer security incidents and escalate when necessary as well as coordinate response to computer security incidents. Recommend a course of action on manages, and records all actions taken and serve as initial POC for Events of Interest reported both internally and externally. Establishes alarm/incident escalation process and tracks, followsup, and resolves incidents. Initiates and maintains contact with affected parties during incident resolution. Typically manages Cyber Incident Analysts.

Determine the source of computer incidents and take appropriate corrective actions.

- Initiate problem reports, as required, and ensure that incidents are resolved in a timely manner.
- Obtain detailed knowledge of the network, system and applications.
- Answer inquiries regarding specific systems.
- Provide second- and third-tier support to business user and customer.
- Provide technical support for computerized telecommunications processing.
- Maintain documentation of vendor software, including issuance of new releases and problem fixes, as well as documentation of utilities and systems developed in house.
- Communicate with IS operations to signal abnormal patterns in calls or application behavior.

Cyber Risk and Vulnerability Threat Analyst I

Education: Bachelor's Degree
Years of Experience: 2

Responsibilities:

Meet with key systems development and user project team members to determine the main components, objectives and user requirements of the system to identify the areas that require controls.

- Discuss the selection of appropriate controls with systems development and user project team members to determine and rank the major risk to and exposures of the system.
- Discuss references to authoritative sources with systems development and user project team members to identify controls to mitigate the risk to and exposures of the system.
- Evaluate available controls and participate in discussions with systems development and user project team members to advise the project team regarding the design of the system and implementation of controls.
- Periodically meet with systems development and user project team members and review the documentation and deliverables to monitor the systems development process to ensure that controls are implemented, user and business requirements are met, and the systems development/acquisition methodology is being followed.

Cyber Risk and Vulnerability Threat Analyst II

Education: Bachelor's Degree
Years of Experience: 5

Responsibilities:

Meet with key systems development and user project team members to determine the main components, objectives and user requirements of the system to identify the areas that require controls.

- Discuss the selection of appropriate controls with systems development and user project team members to determine and rank the major risk to and exposures of the system.
- Discuss references to authoritative sources with systems development and user project team members to identify controls to mitigate the risk to and exposures of the system.
- Evaluate available controls and participate in discussions with systems development and user project team members to advise the project team regarding the design of the system and implementation of control s.
- Periodically meet with systems development and user project team members and review the documentation and deliverables to monitor the systems development process to ensure that controls are implemented, user and business requirements are met, and the systems development/acquisition methodology is being followed. Typically, are managed by Cyber Risk and Vulnerability Threat Analysy III or Security Manager.

Cyber Risk and Vulnerability Threat Analyst III

Education: Bachelor's Degree

Years of Experience: 7

Responsibilities:

Meet with key systems development and user project team members to determine the main components, objectives and user requirements of the system to identify the areas that require controls.

- Discuss the selection of appropriate controls with systems development and user project team members to determine and rank the major risk to and exposures of the system.
- Discuss references to authoritative sources with systems development and user project team members to identify controls to mitigate the risk to and exposures of the system.
- Evaluate available controls and participate in discussions with systems development and user project team members to advise the project team regarding the design of the system and implementati on of controls.
- Periodically meet with systems development and user project team members and review the documentation and deliverables to monitor the systems development process to ensure that controls are implemented, user and business requirements are met, and the systems development/acquisition methodology is being followed. Typically manage Cyber Risk abd Vulnerability Threat Analysts.

Cyber Security Technical Lead

Education: Bachelor's Degree

Years of Experience: 8

Responsibilities:

Information security management provides the lead role to ensure that the organization 's information and the information processing resources under its control are properly protected. This includes leading, supporting and facilitating the implementation of an organization wide information security program that includes the development of a BIA, a BCP and a DRP related to IT department functions in support of the organization's critical business processes. A major component in establishing such programs is the application of risk management principles to assess the risk to IT assets, mitigate the risk to an appropriate level as determined by management and monitor the remaining residual risk.

Cyber Security Manager I

Education: Bachelor's Degree

Years of Experience: 5

Responsibilities:

Support cyber projects and governance structures, policies and procedures, and specific control mechanisms to assure strategic and tactical alignment with the organization's respective goals, objectives and risk management strategy. Provide proper governance to all aspects of a project that may be compromised. Cyber Task Managers apply their broad management skills and specialized functional and technical expertise to guide cyber engineering and process eams in delivering client solutions or to manage the day-to-day operations of cyber projects. The Cyber Manager monitors quality across multiple projects. This individual establishes and maintains financial, project measures and technical reports to show progress of projects to management and customers, organizes and assigns responsibilities to subordinates, and oversees the assigned tasks. Provide effective and efficient cyber project management based on hard factors such as deliverables, quality, costs and deadlines; on soft factors such as team dynamics, conflict resolution, leadership issues, cultural differences and communication; and, finally, on environmental factors such as the political and power issues in the sponsoring organization, managing the expectations of stakeholders, and the larger ethical and social issues that may surround a project.

Cyber Security Manager II

Education: Bachelor's Degree
Years of Experience: 8
Responsibilities:

Support cyber projects and governance structures, policies and procedures, and specific control mechanisms to assure strategic and tactical alignment with the organization's respective goals, objectives and risk management strategy. Provide proper governance to all aspects of a project that may be compromised. Cyber Task Managers apply their broad management skills and specialized functional and technical expertise to guide cyber engineering and process teams in delivering client solutions or to manage the dayto-day operations of cyber projects. The Cyber Manager monitors quality across multiple projects. This individual establishes and maintains financial, project measures and technical reports to show progress of projects to management and customers, organizes and assigns responsibilities to subordinates, and oversees the assigned tasks.

Provide effective and efficient cyber project management based on hard factors such as deliverables, quality, costs and deadlines; on soft factors such as team dynamics, conflict resolution, leadership issues, cultural differences and communication; and, finally, on environmental factors such as the political and power issues in the sponsoring organization, managing the expectations of stakeholders, and the larger ethical and social issues that may surround a project.

Cyber Security Manager III

Education: Bachelor's Degree
Years of Experience: 15
Responsibilities:

Support cyber projects and governance structures, policies and procedures, and specific control mechanisms to assure strategic and tactical alignment with the organization's respective goals, objectives and risk management strategy. Provide proper governance to all aspects of a project that may be compromised. Cyber Task Managers apply their broad management skills and specialized functional and technical expertise to guide cyber engineering and process teams in delivering client solutions or to manage the dayto-day operations of cyber projects. The Cyber Manager monitors quality across multiple projects. This individual establishes and maintains financial, project measures and technical reports to show progress of projects to management and customers, organizes and assigns responsibilities to subordinates, and oversees the assigned tasks.

Provide effective and efficient cyber project management based on hard factors such as deliverables, quality, costs and deadlines; on soft factors such as team dynamics, conflict resolution, leadership issues, cultural differences and communication; and, finally, on environmental factors such as the political and power issues in the sponsoring organization, managing the expectations of stakeholders, and the larger ethical and social issues that may surround a project.

Cyber System Security Engineer I

Education: Bachelor's Degree
Years of Experience: 2
Responsibilities:

Provides technical information system security engineering support to the organization that encompasses the following:

- Project life cycles, including development, operation, maintenance and decommissioning activities
- Entire organizations, including management, organizational and engineering activities
- Concurrent interactions with other disciplines, such as system software and hardware, human factors, test engineering, system management, operation and maintenance
- Interactions with other organizations, including acquisition, system management, certification, accreditation and evaluation. Review and evaluate application system audit trails to ensure that documented controls are in place to address all security, edit and processing controls. Tracking information in a change management system includes:

- History of work order activity (date of work order, programmer assigned, changes made and date closed)
- History of logons and logoffs by programmers - History of program deletions

- Identify and test existing controls to determine the adequacy of production library security to ensure the integrity of the production resources.

Cyber System Security Engineer II

Education: Bachelor's Degree

Years of Experience: 5

Responsibilities:

Provides technical information system security engineering support to the organization that encompasses the following:

- Project life cycles, including development, operation, maintenance and decommissioning activities
- Entire organizations, including management, organizational and engineering activities
- Concurrent interactions with other disciplines, such as system software and hardware, human factors, test engineering, system management, operation and maintenance
- Interactions with other organizations, including acquisition, system management, certification, accreditation and evaluation. Review and evaluate application system audit trails to ensure that documented controls are in place to address all security, edit and processing controls. Tracking information in a change management system includes:

- History of work order activity (date of work order, programmer assigned, changes made and date closed)
- History of logons and logoffs by programmers - History of program deletions

- Identify and test existing controls to determine the adequacy of production library security to ensure the integrity of the production resources.

Cyber System Security Engineer III

Education: Bachelor's Degree

Years of Experience: 7

Responsibilities:

Provides technical information system security engineering support to the organization that encompasses the following:

- Project life cycles, including development, operation, maintenance and decommissioning activities
- Entire organizations, including management, organizational and engineering activities
- Concurrent interactions with other disciplines, such as system software and hardware, human factors, test engineering, system management, operation and maintenance.

- Interactions with other organizations, including acquisition, system management, certification, accreditation and evaluation. Review and evaluate application system audit trails to ensure that documented controls are in place to address all security, edit and processing controls. Tracking information in a change management system includes:

- History of work order activity (date of work order, programmer assigned, changes made and date closed)
- History of logons and logoffs by programmers - History of program deletions

- Identify and test existing controls to determine the adequacy of production library security to ensure the integrity of the production resources. • Review and analyze test plans to determine if defined system requirements are being verified.
- Analyze test results and other audit evidence to evaluate the system maintenance process to determine whether control objectives were achieved.
- Review appropriate documentation, discuss with key personnel and use observation to evaluate system maintenance standards and procedures to ensure their adequacy.
- Discuss and examine supporting records to test system maintenance procedures to ensure that they arc being applied as described in the standards.
- Participate in post-implement Typically manages other System Security Engineers.

Cyber Subject Matter Authority I

Education: Bachelor's Degree
Years of Experience: 10
Responsibilities:

Accepted as an authority in a given domain of Cyber security, or proficient in highly demanded emergent cyber tools or processes required under special circumstances. Duties may include subject matter authority to a specific incident, security application or enterprise environment to improve security posture or resolve cyber organizational issues.

Cyber Subject Matter Authority II

Education: Bachelor's Degree
Years of Experience: 15
Responsibilities:

Accepted as an authority in a given domain of Cyber security, or proficient in highly demanded emergent cyber tools or processes required under special circumstances. Duties may include subject matter authority to a specific incident, security application or enterprise environment to improve security posture or resolve cyber organizational issues.

Cyber Subject Matter Authority III

Education: Bachelor's Degree
Years of Experience: 20
Responsibilities:

Accepted as an authority in a given domain of Cyber security, or proficient in highly demanded emergent cyber tools or processes required under special circumstances. Duties may include subject matter authority to a specific incident, security application or enterprise environment to improve security posture or resolve cyber organizational issues.

Cyber Auditor I

Education: Associates Degree

Years of Experience: 2

Responsibilities:

Performs an understand and identify risk under topical areas such as information management, IT infrastructure, IT governance and IT operations. Seeks to understand the organizational environment, business risk and business controls. A key element of the integrated approach is a discussion among the whole audit team of emerging risk, with consideration of impact and likelihood. Detailed audit work focuses on the relevant controls in place to manage this risk. IT systems frequently provide a first line of preventive and detective controls, and the integrated audit approach depends on a sound assessment of their efficiency and effectiveness.

- Identification of risk faced by the organization for the area being audited
- Identification of relevant key controls
- Review and understanding of the design of key controls
- Testing that key controls are supported by the IT system
- Testing that management controls operate effectively
- A combined report or opinion on control risk, design and weaknesses

Cyber Auditor II

Education: Bachelor's Degree

Years of Experience: 4

Responsibilities:

Performs an understand and identify risk under topical areas such as information management, IT infrastructure, IT governance and IT operations. Seeks to understand the organizational environment, business risk and business controls. A key element of the integrated approach is a discussion among the whole audit team of emerging risk, with consideration of impact and likelihood. Detailed audit work focuses on the relevant controls in place to manage this risk. IT systems frequently provide a first line of preventive and detective controls, and the integrated audit approach depends on a sound assessment of their efficiency and effectiveness.

- Identification of risk faced by the organization for the area being audited
- Identification of relevant key controls
- Review and understanding of the design of key controls
- Testing that key controls are supported by the IT system
- Testing that management controls operate effectively
- A combined report or opinion on control risk, design and weaknesses

Cyber Auditor III

Education: Bachelor's Degree

Years of Experience: 7

Responsibilities:

Performs an understand and identify risk under topical areas such as information management, IT infrastructure, IT governance and IT operations. Seeks to understand the organizational environment, business risk and business controls. A key element of the integrated approach is a discussion among the whole audit team of emerging risk, with consideration of impact and likelihood. Detailed audit work focuses on the relevant controls in place to manage this risk. IT systems frequently provide a first line of preventive and detective controls, and the integrated audit approach depends on a sound assessment of their efficiency and effectiveness.

- Identification of risk faced by the organization for the area being audited
- Identification of relevant key controls
- Review and understanding of the design of key controls
- Testing that key controls are supported by the IT system
- Testing that management controls operate effectively
- A combined report or opinion on control risk, design and weaknesses. Typically manages Cyber Auditors.

Cyber Database Administrator I

Education: Bachelor's D egree

Years of Experience: 2

Responsibilities:

Evaluates security technologies; design security aspects of the network topology, access control, identity management and other security systems; and establish security policies and security requirements. Evaluates program specifications versus policies, requirements and architecture diagrams. Works with compliance, risk management and audit functions to incorporate their requirements and recommendations for security into the security policies and architecture.

Cyber Database Administrator II

Education: Bachelor's Degree

Years of Experience: 5

Responsibilities:

The database administrator (DBA), as custodian of an organization's data, defines, secures and maintains the data structures in the corporate database system. The DBA must understand the organization and user data and data relationship (structure) requirements. This position is responsible for the security of the shared data stored on database systems. The DBA is responsible for the actual design, definition and proper maintenance of the corporate databases. The DBA usually reports directly to the director of the IPF. The DBA's role includes:

- Specifying the physical (computer-oriented) data definition.
- Changing the physical data definition to improve performance.
- Selecting and implementing database optimization tools.
- Testing and evaluating programming and optimization tools.
- Answering programmer queries and educating programmers in the database structures.
- Implementing database definition controls, access controls, update controls and concurrency controls.
- Monitoring database usage, collecting performance statistics and tuning the database.
- Defining and initiating backup and recovery procedures

Cyber Database Administrator III

Education: Bachelor's Degree

Years of Experience: 10

Responsibilities:

The database administrator (DBA), as custodian of an organization's data, defines, secures and maintains the data structures in the corporate database system. The DBA must understand the organization and user data and data relationship (structure) requirements. This position is responsible for the security of the shared data stored on database systems. The DBA is responsible for the actual design, definition and proper maintenance of the corporate databases. The DBA usually reports directly to the director of the IPF. The DBA's role includes:

- Specifying the physical (computer-oriented) data definition.
- Changing the physical data definition to improve performance.
- Selecting and implementing database optimization tools.
- Testing and evaluating programming and optimization tools.
- Answering programmer queries and educating programmers in the database structures.
- Implementing database definition controls, access controls, update controls and concurrency controls.
- Monitoring database usage, collecting performance statistics and tuning the database.
- Defining and initiating backup and recovery procedures. Typically manages Cyber Database Administrators.

Cyber Security Architect

Education: Bachelor's Degree

Years of Experience: 15

Responsibilities:

Evaluates security technologies; design security aspects of the network topology, access control, identity management and other security systems; and establish security policies and security requirements. Evaluates program specifications versus policies, requirements and architecture diagrams. Works with compliance, risk management and audit functions to incorporate their requirements and recommendations for security into the security policies and architecture.

Cyber Network Administrator I

Education: Bachelor's Degree

Years of Experience: 2

Responsibilities:

Responsible for key components of this infrastructure (e.g., routers, switches, firewalls, network segmentation, performance management, remote access). Responsible for technical and administrative control over the LAN on premius, hybid or cloud. This includes ensuring that transmission links are functioning correctly, backups of the system are occurring, and software/hardware/cloud purchases are authorized and installed properly.

Cyber Network Administrator II

Education: Associates Degree

Years of Experience: 5

Responsibilities:

Responsible for key components of this infrastructure (e.g., routers, switches, firewalls, network segmentation, performance management, remote access). Responsible for technical and administrative control over the LAN on premius, hybid or cloud. This includes ensuring that transmission links are functioning correctly, backups of the system are occurring, and software/hardware/cloud purchases are authorized and installed properly.

Cyber Network Administrator III

Education: Bachelor's Degree

Years of Experience: 8

Responsibilities:

Responsible for key components of this infrastructure (e.g., routers, switches, firewalls, network segmentation, performance management, remote access). Responsible for technical and administrative control over the LAN on premius, hybid or cloud. This includes ensuring that transmission links are functioning correctly, backups of the system are occurring, and software/hardware/cloud purchases are authorized and installed properly. Typically manages Network Administraotrs.

Cyber Operations Administrator I

Education: Bachelor's Degree

Years of Experience: 1

Responsibilities:

Responsible for computer operations personnel, including all the staff required to run the data center or cloud enterprise platform efficiently and effectively (e.g., computer operators, librarians, schedulers and data control personnel). The data center or cloud instance includes the servers and cloud services, peripherals such as highspeed printers, networking equipment, magnetic media, and storage area networks. It constitutes a major asset investment and impacts the organization's ability to function effectively.

Cyber Operations Administrator II

Education: Bachelor's Degree

Years of Experience: 8

Responsibilities:

Responsible for computer operations personnel, including all the staff required to run the data center or cloud enterprise platform efficiently and effectively (e.g., computer operators, librarians, schedulers and data control personnel). The data center or cloud instance includes the servers and cloud services, peripherals such as highspeed printers, networking equipment, magnetic media, and storage area networks. It constitutes a major asset investment and impacts the organization's ability to function effectively.

Cyber Operations Administrator III

Education: Bachelor's Degree

Years of Experience: 3

Responsibilities:

Responsible for computer operations personnel, including all the staff required to run the data center or cloud enterprise platform efficiently and effectively (e.g., computer operators, librarians, schedulers and data control personnel). The data center or cloud instance includes the servers and cloud services, peripherals such as high-speed printers, networking equipment, magnetic media, and storage area networks. t constitutes a major asset investment and impacts the organization's ability to function effectively. Typically manages Operations Administrators.

Cyber Security Specialist I

Education: High School Diploma / GED

Years of Experience: 0

Responsibilities:

Identifies and resolves highly complex issues to prevent cyber-attacks on information systems and to keep computer information systems secure from interruption of service, intellectual property theft, network viruses, financial or IP theft, and theft of sensitive customer data, allowing business to continue as normal.

This is accomplished through the systematic implementation of a cyber framework and process. The Cyber Security Specialist designs, installs, and manages security mechanisms that protect networks and information systems against hackers, breaches, viruses, and spyware by implementing security controls. The Cyber Security Specialist responds to incidents (planned and unplanned) investigates violations and recommends enhancements to mitigate potential security vulnerabilities.

Cyber Security Specialist II

Education: Bachelor's Degree

Years of Experience: 2

Responsibilities:

Identifies and resolves highly complex issues to prevent cyber-attacks on information systems and to keep computer information systems secure from interruption of service, intellectual property theft, network viruses, financial or IP theft, and theft of sensitive customer data, allowing business to continue as normal. This is accomplished through the systematic implementation of a cyber framework and process. The Cyber Security Specialist designs, installs, and manages security mechanisms that protect networks and information systems against hackers, breaches, viruses, and spyware by implementing security controls. The Cyber Security Specialist responds to incidents (planned and unplanned) investigates violations and recommends enhancements to mitigate potential security vulnerabilities.

Cyber Security Specialist III

Education: Bachelor's Degree

Years of Experience: 4

Responsibilities:

Identifies and resolves highly complex issues to prevent cyber-attacks on information systems and to keep computer information systems secure from interruption of service, intellectual property theft, network viruses, financial or IP theft, and theft of sensitive customer data, allowing business to continue as normal. This is accomplished through the systematic implementation of a cyber framework and process. The Cyber Security Specialist designs, installs, and manages security mechanisms that protect networks and information systems against hackers, breaches, viruses, and spyware by implementing security controls. The Cyber Security Specialist responds to incidents (planned and unplanned) investigates violations and recommends enhancements to mitigate potential security vulnerabilities. Typically manages Security Specialists.

Cyber Media Administrator I

Education: Associates Degree

Years of Experience: 2

Responsibilities:

Responsible for recording, issue, receive and safeguard all program and data files that are maintained on removable media. Provide additional support through the use of software that assists in maintaining inventory, movement, version control and configuration management.

Cyber Media Administrator II

Education: Associates Degree

Years of Experience: 4

Responsibilities:

Responsible for recording, issue, receive and safeguard all program and data files that are maintained on removable media. Provide additional support through the use of software that assists in maintaining inventory, movement, version control and configuration management.

APPENDIX B

TRAINING COURSE DESCRIPTIONS

CMMI® V2.0 FOUNDATIONS AND CAPABILITY COURSE

COURSE LENGTH: 2 Days – 16 Hours
MINIMUM PARTICIPANTS: 3
MAXIMUM PARTICIPANTS: 25

COURSE DESCRIPTION:

CMMI® V2.0 FOUNDATIONS AND CAPABILITY COURSE - This two-day course will teach students how to use the CMMI Version 2.0 Models, and the business value that can be gained by improving capability. The skills acquired after completing the course include connecting the CMMI model with business value, describing the components of CMMI, using CMMI as a tool for improving performance, and understanding the high-level value of a CMMI appraisal. This course is composed of lectures and class exercises, with time allotted for participant questions and discussion. The format of the course requires that students actively participate throughout the duration of the course without missing any class time. This course is well-suited for anyone interested in improving business performance. *This course does not require any prerequisites.* The course is offered at SteelToad Consulting's offices in Baltimore, Maryland, and/or can be offered on-site at the customer location. The course material is designed by CMMI Institute, with the authority and permission granted to partner organizations to provide qualified and approved CMMI course trainers to teach this course.

CMMI® V2.0 UPGRADE COURSE

COURSE LENGTH: 1 Days – 8 Hours MINIMUM
PARTICIPANTS: 3
MAXIMUM PARTICIPANTS: 25

COURSE DESCRIPTION:

CMMI® V2.0 UPGRADE COURSE. This one-day course will guide students through key components of the CMMI V2.0 model structure and key differences between CMMI Version 1.3 and CMMI Version V2.0. This course is designed for students who have taken CMMI training for prior versions of the model to upgrade their knowledge to the current CMMI, V2.0. In addition, this course is for appraisal team members who participated on a CMMI Version 1.3 appraisal, and who need to fulfill the Version 2.0 training requirements required for providing service on a CMMI V2.0 appraisal. Students must have the following prerequisite course(s*): Introduction to CMMI Version 1.3 (for Development or Services);* OR *Introduction to CMMI Version 1.2 (for Development or Services) and CMMI Version 1.3 Upgrade Training;* OR

Introduction to CMMI Version 1.1, CMMI Version 1.2 Upgrade Training, and CMMI Version 1.3 Upgrade Training. This course is composed of lectures and class exercises, with time allotted for participant questions and discussion. The course is offered at SteelToad Consulting's offices in Baltimore, Maryland, and/or can be offered on-site at the customer location. The course material is designed by CMMI Institute, with the authority and permission granted to partner organizations to provide qualified and approved CMMI course trainers to teach this course.

CMMI® V2.0 BUILDING DEVELOPMENT EXCELLENCE

COURSE LENGTH: 1 Days – 8 Hours
MINIMUM PARTICIPANTS: 3
MAXIMUM PARTICIPANTS: 25

COURSE DESCRIPTION:

CMMI® V2.0 BUILDING DEVELOPMENT EXCELLENCE course. This one-day course will teach students how to build capability in developing or engineering products and services. Most of the one-day courses are scheduled on the calendar to immediately follow the "CMMI 2.0 FOUNDATIONS AND CAPABILITY COURSE". The course is intended for product development team members and anyone interested in improving business performance. The skills acquired after completing course include the ability to locate information in the CMMI model related to best practices in engineering and development, and the ability to use the CMMI Development 2.0 view to effectively assess, improve, and sustain process capability and performance. This course is composed of lectures and class exercises, with time allotted for participant questions and discussion. *Each student is required to have taken Foundations of Capability (or CMMI Version 2.0 Upgrade Training).* The course is offered at SteelToad Consulting's offices in Baltimore, Maryland, and/or can be offered on-site at the customer location. The course material is designed by CMMI Institute, with the authority and permission granted to partner organizations to provide qualified and approved CMMI course trainers to teach this course.

CMMI® V2.0 BUILDING SERVICES EXCELLENCE

COURSE LENGTH: 1 Days – 8 Hours
MINIMUM PARTICIPANTS: 3
MAXIMUM PARTICIPANTS: 25

COURSE DESCRIPTION:

CMMI® V2.0 BUILDING SERVICES EXCELLENCE COURSE. This one-day course will teach students how to build capability in services. Most of the one-day courses are scheduled on the calendar to immediately follow the "CMMI 2.0 FOUNDATIONS AND CAPABILITY COURSE". The course is intended for service team members and anyone interested in improving business performance. The skills acquired after completing course include the ability to locate information in the CMMI model related to best practices in services, and the ability to use the CMMI Services 2.0 view to effectively assess, improve, and sustain process capability and performance. This course is composed of lectures and class exercises, with time allotted for participant questions and discussion. The format of this course requires that students actively participate throughout the duration of the course without missing any class time. *Each student is required to have taken Foundations of Capability (or CMMI Version 2.0 Upgrade Training).* This course is offered at SteelToad Consulting's offices in Baltimore, Maryland, and/or can be offered on-site at the customer location. The course material is designed by CMMI Institute, with the authority and permission granted to partner organizations

CMMI® V2.0 BUILDING SUPPLIER EXCELLENCE

COURSE LENGTH: 1 Days – 8 Hours
MINIMUM PARTICIPANTS: 3
MAXIMUM PARTICIPANTS: 25

COURSE DESCRIPTION:

CMMI® V2.0 BUILDING SUPPLIER EXCELLENCE COURSE. This one-day course will teach students how to build capability in services. The course is intended for anyone interested in improving business performance. The skills acquired after completing course include the ability to locate information in the CMMI model related to best practices in selecting and managing suppliers, and to use the CMMI Supplier Management view to effectively assess, improve, and sustain process capability and performance. This course is composed of lectures and class exercises, with time allotted for participant questions and discussion. The format of the course requires that students actively participate throughout the duration of the course without missing any class time. *Each student is required to have taken Foundations of Capability (or CMMI Version 2.0 Upgrade Training).* The course is offered at SteelToad Consulting's offices in Baltimore, Maryland, and/or can be offered on-site at the customer location. The course material is designed by CMMI Institute, with the authority and permission granted to partner organizations to provide qualified and approved CMMI course trainers to teach this course.

ISACA® CERTIFIED INFORMATION SECURITY MANAGER (CISM) COURSE.

COURSE LENGTH: 4 Days – 32 Hours
MINIMUM PARTICIPANTS: 3
MAXIMUM PARTICIPANTS: 25

COURSE DESCRIPTION:

ISACA® CERTIFIED INFORMATION SECURITY MANAGER (CISM) COURSE. The CISM course is an intensive, four-day review program to prepare individuals who manage, design, oversee and assess an enterprises' information security, and those students planning to take the Certified Information Security Manager (CISM) exam. The course focuses on the key points covered in the CISM Review Manual 15th Edition and includes class lectures, group discussions/activities, and exam practice. This course is intended for individuals with familiarity with and experience in information security management. There are no prerequisite requirements for taking the CISM Exam Preparation Course or the CISM exam; however, in order to apply for CISM certification, the candidate must meet the necessary experience requirements determined by ISACA. The skills acquired after completing the course include general exam information, information security governance, information risk management, information security program development and management, and information security incident management. and exam practice/sample exam. Typically, each day of the course will cover a single CISM domain, using lecture, group activities and practice questions. This course is offered at SteelToad Consulting's offices in Baltimore, Maryland, and/or can be offered on-site at the customer location. The course material is designed by ISACA®, with the authority and permission granted to partner organizations to provide qualified and approved CISM course trainers to teach this course.

ISACA® CERTIFIED INFORMATION SYSTEMS AUDITOR (CISA) COURSE

COURSE LENGTH: 4 Days – 32 Hours
MINIMUM PARTICIPANTS: 3
MAXIMUM PARTICIPANTS: 25

COURSE DESCRIPTION:

ISACA® CERTIFIED INFORMATION SYSTEMS AUDITOR (CISA) COURSE. The CISA Exam Preparation course is an intensive, four-day review program designed to prepare professionals for the Certified Information Systems Auditor (CISA) exam. The course focuses on the key points covered in the *CISA Review Manual 27th Edition* and includes class lectures, and group discussions. This course is intended for individuals with familiarity with and experience in information systems auditing, control or security. The skills acquired after completing course include the information system auditing process, the governance and management of information technology, information systems acquisition, development and implementation, IS operations and business resilience, and the information asset security and control. The format of each day will cover 1-2 domains' worth of information presented via lecture, group discussion and practice questions. The course is offered at SteelToad Consulting's offices in Baltimore, Maryland, and/or can be offered on-site at the customer location. The course is offered at SteelToad Consulting's offices in Baltimore, Maryland, and/or can be offered on-site at the customer location. The course material is designed by ISACA®, with the authority and permission granted to partner organizations to provide qualified and approved CISA course trainers to teach this course.

APPENDIX C – GSA PRICE LIST – STEEL TOAD CONSULTING LLC

MAS – MULTIPLE AWARD SCHEDULE

SIN	Service Proposed	Minimum Education	Minimum Years of Experience (cannot be a range)	GSA Price	Unit of Issue
ON-SITE					
54151S	Network Engineer	Bachelor's Degree	4	$156.48	Hour
54151S	Application Developer	Bachelor's Degree	3	$146.80	Hour
54151S	Project Manager	Bachelor's Degree	4	$205.72	Hour
54151S	Senior Subject Matter Expert	Master's Degree	8	$224.31	Hour
54151S	Senior Database Administrator	Bachelor's Degree	5	$145.14	Hour
54151S	IT Security Engineer	Bachelor's Degree	3	$ $185.27	Hour
54151S	Business Analyst	Associates Degree	3	$142.15	Hour
54151S	Senior Business Analyst	Bachelor's Degree	5	$155.76	Hour
54151S	Information Engineer	Bachelor's Degree	3	$131.70	Hour

54151S	Senior Information Engineer	Bachelor's Degree	5	$147.14	Hour
OFF-SITE					
54151S	Network Engineer	Bachelor's Degree	4	$177.05	Hour
54151S	Application Developer	Bachelor's Degree	3	$156.38	Hour
54151S	Project Manager	Bachelor's Degree	4	$219.15	Hour
54151S	Senior Subject Matter Expert	Master's Degree	8	$238.95	Hour
54151S	Senior Database Administrator	Bachelor's Degree	5	$154.61	Hour
54151S	IT Security Engineer	Bachelor's Degree	3	$197.36	Hour
54151S	Business Analyst	Associates Degree	3	$151.43	Hour
54151S	Senior Business Analyst	Bachelor's Degree	5	$165.92	Hour
54151S	Information Engineer	Bachelor's Degree	3	$140.29	Hour
54151S	Senior Information Engineer	Bachelor's Degree	5	$156.75	Hour
54151HACS	Cyber Incident Response Analyst I	Bachelor's Degree	3	$94.23	Hour

54151HACS	Cyber Incident Response Analyst II	Bachelor's Degree	5	$142.43	Hour

54151HACS	Cyber Incident Response Analyst III	Bachelor's Degree	8	$201.73	Hour
54151HACS	Cyber Risk and Vulnerability Threat Analyst I	Bachelor's Degree	2	$156.71	Hour
54151HACS	Cyber Risk and Vulnerability Threat Analyst II	Bachelor's Degree	5	$181.07	Hour
54151HACS	Cyber Risk and Vulnerability Threat Analyst III	Bachelor's Degree	7	$226.58	Hour
54151HACS	Cyber Security Technical Lead	Bachelor's Degree	8	$201.73	Hour
54151HACS	Cyber Security Manager I	Bachelor's Degree	5	$207.35	Hour
54151HACS	Cyber Security Manager II	Bachelor's Degree	8	$238.41	Hour
54151HACS	Cyber Security Manager III	Bachelor's Degree	15	$260.87	Hour

54151HACS	Cyber System Security Engineer I	Bachelor's Degree	2	$138.15	Hour
54151HACS	Cyber System Security Engineer II	Bachelor's Degree	5	$169.15	Hour
54151HACS	Cyber System Security Engineer III	Bachelor's Degree	7	$199.63	Hour

54151HACS	Cyber Subject Matter Authority I	Bachelor's Degree	10	$252.50	Hour
54151HACS	Cyber Subject Matter Authority II	Bachelor's Degree	15	$269.23	Hour
54151HACS	Cyber Subject Matter Authority III	Bachelor's Degree	20	$336.12	Hour
54151HACS	Cyber Auditor I	Bachelor's Degree	2	$105.81	Hour
54151HACS	Cyber Auditor II	Bachelor's Degree	4	$130.92	Hour
54151HACS	Cyber Auditor III	Bachelor's Degree	7	$176.65	Hour

54151HACS	Cyber Database Administrator I	Bachelor's Degree	2	$124.21	Hour
54151HACS	Cyber Database Administrator II	Bachelor's Degree	5	$167.71	Hour
54151HACS	Cyber Database Administrator III	Bachelor's Degree	10	$212.37	Hour
54151HACS	Cyber Security Architect	Bachelor's Degree	15	$292.39	Hour
54151HACS	Cyber Network Administrator I	Bachelor's Degree	2	$121.35	Hour

54151HACS	Cyber Network Administrator II	Bachelor's Degree	5	$168.17	Hour
54151HACS	Cyber Network Administrator III	Bachelor's Degree	8	$232.05	Hour
54151HACS	Cyber Operations Administrator I	Bachelor's Degree	1	$95.22	Hour
54151HACS	Cyber Operations Administrator II	Bachelor's Degree	8	$137.23	Hour

54151HACS	Cyber Operations Administrator III	Bachelor's Degree	3	$156.82	Hour
54151HACS	Cyber Security Specialist I	High School Diploma	0	$94.97	Hour
54151HACS	Cyber Security Specialist II	Bachelor’s Degree	2	$118.76	Hour
54151HACS	Cyber Security Specialist III	Bachelor’s Degree	4	$141.53	Hour
54151HACS	Cyber Media Administrator I	Associates Degree	2	$82.64	Hour
54151HACS	Cyber Media Administrator II	Associates Degree	4	$95.30	Hour

TRAINING COURSES

SIN	Course Title*	Course Description*	Course Length*	Minimum Participants	Maximum Participants	Contractor or Customer Facility or Both	GSA Price

611420	**CMMI® V2.0 FOUNDATIONS AND CAPABILITY COURSE**	**CMMI® V2.0 FOUNDATIONS AND CAPABILITY COURSE** - This two-day course will teach students how to use the CMMI Version 2.0 Models, and the business value that can be gained by improving capability. The skills acquired after completing the course include connecting the CMMI model with business value, describing the components of CMMI, using CMMI as a tool for improving performance, and understanding the high-level value of a CMMI appraisal. This course is composed of lectures and class exercises, with time allotted for participant questions and discussion. The format of the course requires that students actively participate throughout the duration of the course without missing any class time. This course is well-suited for anyone interested in improving business performance. *This course does not require any prerequisites.* The course is offered at Steel Toad Consulting's offices in Baltimore, Maryland, and/or can be offered on-site at the customer location. The course material is designed by CMMI Institute, with the authority and permission granted to partner organizations to provide qualified and approved CMMI course trainers to teach this course.	16 hours - (2 days)	3 Students (per CMMI Institute requirement)	25 Students (CMMI Institute has allowed virtual training only during virus restrictions. Class size for virtual learning is 15 students)	Both	$1,163.02

611420	**CMMI® V2.0 UPGRADE COURSE**	**CMMI® V2.0 UPGRADE COURSE -** This one-day course will guide students through key components of the CMMI V2.0 model structure and key differences between CMMI Version 1.3 and CMMI Version V2.0. This course is designed for students who have taken CMMI training for prior versions of the model to upgrade their knowledge to the current CMMI, V2.0. In addition, this course is for appraisal team members who participated on a CMMI Version 1.3 appraisal, and who need to fulfill the Version 2.0 training requirements required for providing service on a CMMI V2.0 appraisal. Students must have the following prerequisite course(s*): Introduction to CMMI Version 1.3 (for Development or Services);* OR *Introduction to CMMI Version 1.2 (for Development or Services) and CMMI Version 1.3 Upgrade Training;* OR *Introduction to CMMI Version 1.1, CMMI Version 1.2 Upgrade Training, and CMMI Version 1.3 Upgrade Training.* This course is composed of lectures and class exercises, with time allotted for participant questions and discussion. The course is offered at Steel Toad Consulting's offices in Baltimore, Maryland, and/or can be offered on-site at the customer location. The course material is designed by CMMI Institute, with the authority and permission granted to partner organizations to provide qualified and approved CMMI course trainers to teach this course.	8 hours (one day)	3 Students (per CMMI Institute requirement)	25 Students (CMMI Institute has allowed virtual training only during virus restrictions. Class size for virtual learning is 15 students)	Both	$772.09

611420	**CMMI® V2.0 BUILDING DEVELOPMENT EXCELLENCE**	**CMMI® V2.0 BUILDING DEVELOPMENT EXCELLENCE** course. This one-day course will teach students how to build capability in developing or engineering products and services. Most of the one-day courses are scheduled on the calendar to immediately follow the "CMMI 2.0 FOUNDATIONS AND CAPABILITY COURSE". The course is intended for product development team members and anyone interested in improving business performance. The skills acquired after completing course include the ability to locate information in the CMMI model related to best practices in engineering and development, and the ability to use the CMMI Development 2.0 view to effectively assess, improve, and sustain process capability and performance. This course is composed of lectures and class exercises, with time allotted for participant questions and discussion. *Each student is required to have taken Foundations of Capability (or CMMI Version 2.0 Upgrade Training).* The course is offered at Steel Toad Consulting's offices in Baltimore, Maryland, and/or can be offered on-site at the customer location. The course material is designed by CMMI Institute, with the authority and permission granted to partner organizations to provide qualified and approved CMMI course trainers to teach this course.	8 hours (one day)	3 Students (per CMMI Institute requirement)	25 Students (CMMI Institute has allowed virtual training only during virus restrictions. Class size for virtual learning is 15 students)	Both	$537.53

611420	**CMMI® V2.0 BUILDING SERVICES EXCELLENCE**	**CMMI® V2.0 BUILDING SERVICES EXCELLENCE COURSE.** This one-day course will teach students how to build capability in services. Most of the one-day courses are scheduled on the calendar to immediately follow the "CMMI 2.0 FOUNDATIONS AND CAPABILITY COURSE". The course is intended for service team members and anyone interested in improving business performance. The skills acquired after completing course include the ability to locate information in the CMMI model related to best practices in services, and the ability to use the CMMI Services 2.0 view to effectively assess, improve, and sustain process capability and performance. This course is composed of lectures and class exercises, with time allotted for participant questions and discussion. The format of this course requires that students actively participate throughout the duration of the course without missing any class time. *Each student is required to have taken Foundations of Capability (or CMMI Version 2.0 Upgrade Training).* This course is offered at Steel Toad Consulting's offices in Baltimore, Maryland, and/or can be offered on-site at the customer location. The course material is designed by CMMI Institute, with the authority and permission granted to partner organizations	8 hours (one day)	3 Students (per CMMI Institute requirement)	25 Students (CMMI Institute has allowed virtual training only during virus restrictions. Class size for virtual learning is 15 students)	Both	$537.53

611420	**CMMI® V2.0 BUILDING SUPPLIER EXCELLENCE**	**CMMI® V2.0 BUILDING SUPPLIER EXCELLENCE COURSE.** This one-day course will teach students how to build capability in services. The course is intended for anyone interested in improving business performance. The skills acquired after completing course include the ability to locate information in the CMMI model related to best practices in selecting and managing suppliers, and to use the CMMI Supplier Management view to effectively assess, improve, and sustain process capability and performance. This course is composed of lectures and class exercises, with time allotted for participant questions and discussion. The format of the course requires that students actively participate throughout the duration of the course without missing any class time. *Each student is required to have taken Foundations of Capability (or CMMI Version 2.0 Upgrade Training).* The course is offered at Steel Toad Consulting's offices in Baltimore, Maryland, and/or can be offered on-site at the customer location. The course material is designed by CMMI Institute, with the authority and permission granted to partner organizations to provide qualified and approved CMMI course trainers to teach this course.	8 hours (one day)	3 Students (per CMMI Institute requirement)	25 Students (CMMI Institute has allowed virtual training only during virus restrictions. Class size for virtual learning is 15 students)	Both	$1,905.79

611420	**ISACA® CERTIFIED INFORMATION SECURITY MANAGER (CISM) COURSE**	**ISACA® CERTIFIED INFORMATION SECURITY MANAGER (CISM) COURSE.** The CISM course is an intensive, four-day review program to prepare individuals who manage, design, oversee and assess an enterprises' information security, and those students planning to take the Certified Information Security Manager (CISM) exam. The course focuses on the key points covered in the CISM Review Manual 15th Edition and includes class lectures, group discussions/activities, and exam practice. This course is intended for individuals with familiarity with and experience in information security management. There are no prerequisite requirements for taking the CISM Exam Preparation Course or the CISM exam; however, in order to apply for CISM certification, the candidate must meet the necessary experience requirements determined by ISACA. The skills acquired after completing the course include general exam information, information security governance, information risk management, information security program development and management, and information security incident management. and exam practice/sample exam. Typically, each day of the course will cover a single CISM domain, using lecture, group activities and practice questions. This course is offered at Steel Toad Consulting's offices in Baltimore, Maryland, and/or can be offered on-site at the customer location. The course material is designed by ISACA®, with the authority and permission granted to partner organizations to provide qualified and approved CISM course trainers to teach this course.	32 hours (4 days)	3 Students (per CMMI Institute requirement)	25 Students	Both	$3,274.06

611420	**ISACA® CERTIFIED INFORMATION SYSTEMS AUDITOR (CISA) COURSE**	**ISACA® CERTIFIED INFORMATION SYSTEMS AUDITOR (CISA) COURSE.** The CISA Exam Preparation course is an intensive, four-day review program designed to prepare professionals for the Certified Information Systems Auditor (CISA) exam. The course focuses on the key points covered in the *CISA Review Manual 27th Edition* and includes class lectures, and group discussions. This course is intended for individuals with familiarity with and experience in information systems auditing, control or security. The skills acquired after completing course include the information system auditing process, the governance and management of information technology, information systems acquisition, development and implementation, IS operations and business resilience, and the information asset security and control. The format of each day will cover 1-2 domains' worth of information presented via lecture, group discussion and practice questions. The course is offered at Steel Toad Consulting's offices in Baltimore, Maryland, and/or can be offered on-site at the customer location. The course is offered at Steel Toad Consulting's offices in Baltimore, Maryland, and/or can be offered on-site at the customer location. The course material is designed by ISACA®, with the authority and permission granted to partner organizations to provide qualified and approved CISA course trainers to teach this course.	32 hours (4 days)	3 Students (per CMMI Institute requirement)	25 Students	Both	$3,274.06