Online access to contract ordering information, terms and conditions, up to date pricing, and the option to create an electronic delivery order are available through GSA Advantage!®, a menu driven database system. The INTERNET address GSA Advantage!® is: GSAAAdvantage.gov.

Schedule Title: Multiple Award Schedule (MAS)

FSC Group: Information Technology, Professional Services

Contract Number: 47QTCA18D000J

For more information on ordering from Federal Supply Schedules click on FSS Schedules at GSA.gov.

Contract Period:  October 13, 2017 – October 12, 2022

Company: Gabriel Enterprises Consulting Group, LLC
1727 King St. STE 105
Alexandria VA, 22314

Website: www.geconsultinggroup.com

Contract Administrator: Jason Whetsell
1727 King St. STE 105
Alexandria VA, 22314
jwhetsell@geconsultinggroup.com

Business Size: Small, woman owned, 8(a) certified small business

Price list current through modification PO-0023 effective 6/30/2022
### CUSTOMER INFORMATION

1a Table of awarded special item number(s)

<table>
<thead>
<tr>
<th>SIN</th>
<th>SIN Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>54151S</td>
<td>Information Technology and Professional Services</td>
</tr>
<tr>
<td>611420</td>
<td>Information Technology Training</td>
</tr>
<tr>
<td>54151</td>
<td>Software Maintenance</td>
</tr>
<tr>
<td>511210</td>
<td>Software Licensing</td>
</tr>
<tr>
<td>OLM</td>
<td>Order Level Materials</td>
</tr>
</tbody>
</table>

1b Lowest Priced Model Number and Price for Each SIN

(Government net price based on a unit of one)

N/A

1c Hourly Rates

<table>
<thead>
<tr>
<th>Title</th>
<th>Experience and Education</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>Training Manager</td>
<td>Bachelor’s degree or higher in Training, Business or HR Management. Project experiences of scope, length, and complexity greater than 4 years in the management of training programs, tactical training planning and delivery.</td>
<td>$141.08</td>
</tr>
<tr>
<td>eLearning Developer</td>
<td>Bachelor’s Degree or higher. Project experiences of scope, length, and complexity greater than 2 years in developing eLearning products.</td>
<td>$89.78</td>
</tr>
<tr>
<td>Instructional Systems Designer (ISD)</td>
<td>Bachelor’s Degree or higher. Project experiences of scope, length, and complexity greater than 2 years analyzing, designing, developing, and evaluating in-resident &amp; online training.</td>
<td>$111.97</td>
</tr>
<tr>
<td>Program Manager I</td>
<td>Bachelor’s degree or higher; project experiences of scope, length, and complexity greater than 2 years (likely far more) and commensurate with client's project requirements.</td>
<td>$127.97</td>
</tr>
<tr>
<td>Program Manager II</td>
<td>Master’s degree or higher; project experiences of scope, length, and complexity greater than 4 years (likely far more) and commensurate with client's project requirements.</td>
<td>$193.45</td>
</tr>
<tr>
<td>Principal Executive</td>
<td>Master’s degree or higher; project experiences of scope, length, and complexity greater than 6 years (likely more) and commensurate with client's project requirements.</td>
<td>$195.96</td>
</tr>
<tr>
<td>Business Analyst</td>
<td>Bachelor’s degree or higher; project experiences of scope, length, and complexity commensurate with client's project requirements.</td>
<td>$89.78</td>
</tr>
<tr>
<td>Title</td>
<td>Experience and Education</td>
<td>Price</td>
</tr>
<tr>
<td>-----------------------</td>
<td>------------------------------------------------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Senior Business Analyst</td>
<td>Bachelor’s degree or higher; project experiences of scope, length, and complexity greater than 2 years (likely far more) and commensurate with client’s project requirements.</td>
<td>$135.54</td>
</tr>
<tr>
<td>Senior Business Analyst II</td>
<td>Bachelor’s degree or higher; project experiences of scope, length, and complexity greater than 1 year (likely far more) and commensurate with client’s project requirements.</td>
<td>$138.20</td>
</tr>
<tr>
<td>IT Consultant</td>
<td>Bachelor’s Degree in Computer Science, Engineering, Software Development, Business, or related field of study and/or greater than four 4 years equivalent experience.</td>
<td>$87.95</td>
</tr>
</tbody>
</table>

2. **MAXIMUM ORDER:** 1,000,000

3. **MINIMUM ORDER:** $100

4. **GEOGRAPHIC COVERAGE:** 48 contiguous states and the District of Columbia.

5. **POINT(S) OF PRODUCTION:** The primary point of production is the Gabriel Enterprises Consulting Group corporate headquarters, located in Alexandria, VA

6. **DISCOUNT FROM LIST PRICES:** *GSA Net Prices are shown on the attached GSA Pricelist. Negotiated discount has been applied and the IFF has been added.*

7. **QUANTITY DISCOUNT(S):** 3% on orders over $500,000

8. **PROMPT PAYMENT TERMS:** Prompt Payment terms are net 1% Net 10. Information for Ordering Offices: Prompt payment terms cannot be negotiated out of the contractual agreement in exchange for other concessions.

9. **FOREIGN ITEMS:** N/A

10a. **TIME OF DELIVERY:** 30 DARO

10b. **EXPEDITED DELIVERY:** Items available for expedited delivery are noted in this price list or negotiated at the task order level.

10c. **OVERNIGHT AND 2-DAY DELIVERY:** Overnight and 2-day delivery are available. Contact the Contractor for rates.

10d. **URGENT REQUIREMENTS:** 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), and a sample BPA can be found at the GSA/FSS Schedule homepage (fss.gsa.gov/schedules).
13. **PAYMENT ADDRESS:** Same as contractor

14. **WARRANTY PROVISION:** N/A for services

15. **EXPORT PACKING CHARGES:** Not applicable

16. **TERMS AND CONDITIONS OF RENTAL, MAINTENANCE, AND REPAIR (IF APPLICABLE):** N/A

17. **TERMS AND CONDITIONS OF INSTALLATION (IF APPLICABLE):** N/A

18a. **TERMS AND CONDITIONS OF REPAIR PARTS INDICATING DATE OF PARTS PRICE LISTS AND ANY DISCOUNTS FROM LIST PRICES (IF AVAILABLE):** N/A

18b. **TERMS AND CONDITIONS FOR ANY OTHER SERVICES (IF APPLICABLE):** N/A

19. **LIST OF SERVICE AND DISTRIBUTION POINTS (IF APPLICABLE):** N/A

20. **LIST OF PARTICIPATING DEALERS (IF APPLICABLE):** N/A

21. **PREVENTIVE MAINTENANCE (IF APPLICABLE):** N/A

22a. **SPECIAL ATTRIBUTES SUCH AS ENVIRONMENTAL ATTRIBUTES (e.g. recycled content, energy efficiency, and/or reduced pollutants):** N/A

22b. **Section 508 Compliance for Electronic and Information Technology (EIT):** Section 508 compliance information on the supplies and services in this contract are available at the following website address (URL): Not applicable

   The EIT standard can be found at: [www.Section508.gov/](http://www.Section508.gov/).

23. **UNIQUE ENTITY IDENTIFIER (UEI) NUMBER:** YX6QZ9DYUV53

24. **NOTIFICATION REGARDING REGISTRATION IN SYSTEM FOR AWARD MANAGEMENT (SAM) DATABASE:** Contractor has an Active Registration in the SAM database.
Labor Category Descriptions

**Training Manager**
**Description:** Plans, directs, and coordinates training program activities to enhance the knowledge, skills, and abilities of the client agency personnel we support. Works with the Project Manager to provide insight into the progress and direction of training programs, staff, and budgets. The Training Manager is also responsible for organizing training programs, including creating or selecting course content and materials that align with agency project mission and objectives.

Planned training activities are driven by the Training Program and the Tactical Training plan which outline quarterly training activities. Such activities include classroom training, group certification initiatives, distance learning, coaching seminars, and professional development profile assessments based on contract requirements and deliverables. Any variation or mix of training must ensure that course content, software, systems, and equipment are appropriate and meaningful to the intended target audience and achieve the intended learning outcomes.

**eLearning Developer**
**Description:** The eLearning Developer supports the design, implementation, and ongoing facilitation of a variety of online, instructor led, and blended systems training programs to internal and external clients. This individual will be responsible for creating content that delivers effective training for varying learning styles and audiences. This individual will work closely with the Instructional Systems Designers, curriculum developer, training manager and project manager in developing multimedia to further increase the organization's teaching and learning solutions. Experience in adult learning theory, instructional design, and online learning product development; preference for experience with both rapid and robust authoring tools and integration and delivery of e-learning courseware in learning management systems. Experience with current web-based training development software (e.g. as Lectora, Articulate, Audacity, Adobe Captivate and Creative Suite tools, Camtasia, and related open-source software). Experienced in curriculum development for various delivery modalities: face to face, virtual, self-paced. Knowledge of eLearning authoring packages such as Captivate and Articulate Storyline. Experience working with HTML, CSS, and JavaScript.

**Instructional Systems Designer (ISD)**
**Description:** The Instructional Systems Designer (ISD) will be responsible for creating content that delivers effective training for varying learning styles and audiences. This individual will design and develop engaging, effective study materials, online courses, learning activities, lesson objectives, systems design guidance, categorize objectives by learning type (using Bloom’s taxonomy). The ISD professional will construct learning analysis hierarchies, identify
learning prerequisite/requirements, review/revise existing instructional materials, develop test items, determine instructional strategies, select instructional methods, select instructional media. Additional duties include the ability to analyze resource requirements/constraints, design/develop lessons, design/develop job aids, design/develop activity guides, design/develop PowerPoint presentations, evaluate instructional effectiveness, and develop plan of instructions.

**Program Manager I**

**Description:** Serves as Program manager over a department or office project. Ensures the goals, scope, and customer/agency deliverables are understood and executed by everyone on the team as well as possible.

**Program Manager II**

**Description:** In addition to Program Manager I functions, organizes, directs, and coordinates planning and production of all contract support activities. Demonstrates communications skills at all levels of management. Serves as the contractor’s authorized interface with the Contracting Officer’s Technical Representative (COTR), government management personnel, and client agency representatives. Responsible for formulating and enforcing work standards, assigning contractor schedules, reviewing work discrepancies, supervising contractor personnel, and communicating policies, purposes, and goals of the organization to subordinate personnel. Responsible for overall contract performance. Under stringent time frames, assembles and recruits as necessary to perform assigned tasks. Demonstrates capability in the overall management of multitask contracts of the size, type, and complexity as described in the Task Order.

**Principle Executive**

**Description:** A member of or direct report to the executive leadership team. Manages subordinate staff in the day-to-day performance of their jobs. Ensures that project/department milestones/goals are met and adhering to approved budgets. Has full authority for personnel actions. Extensive knowledge of department processes. Creates business strategies to facilitate project and department improvements. Identifies and helps to develop strategic relationships with partners or potential customers. Works with other departments to ensure alignment of company goals. Designs and determines terms of business agreements.

**Business Analyst**

**Description:** Analyzes, enhances, and optimizes IT systems, business processes, and training tools, used within the organization. Performs interviews, research, and benchmarking for training needs assessments and organizational gap analyses. Provides technical, managerial, and administrative assistance for problem definition, analysis, requirements development and implementation, for complex to extremely complex systems in the subject matter area.

Makes recommendations and advises on organization-wide systems and business process improvements, optimization or maintenance efforts, in the following representative areas: information systems architecture; networks/communications; telecommunications; operations and management; quality management systems; computer languages,
operating systems, database systems, security, decision support systems; risk management and electronic analysis, software including commercial software and software development, life-cycle management; modeling and simulation; graphics; data management; etc.

**Senior Business Analyst**

**Description:** In addition to Business Analyst functions, provides expertise in the areas of system architecture, SaaS system design and agile software processes. Assists project manager to maintain project schedules, risk management, and documentation. Acts as liaison between the development teams, business, and client. Facilitates workshops with stakeholders to gather requirements. Performs gap-analysis and makes recommendations to meet requirements and business processes.

Analyzes and recommends software patches and fixes capable of meeting systems and business requirements. Maintains a deep understanding of architecture, software patch fixes and techniques for managing agile software updates across a broad spectrum of systems, applications and requirements. Conducts training with stakeholders. Participates in transitions from development to production or steady state.

**Senior Business Analyst II**

**Description:** In addition to Business Analyst functions, provides expertise in the areas of system architecture, SaaS system design and agile software processes. Assists project manager to maintain project schedules, risk management, and documentation. Acts as liaison between the development teams, business, and client. Facilitates workshops with stakeholders to gather requirements. Performs gap-analysis and makes recommendations to meet requirements and business processes.

Analyzes and recommends software patches and fixes capable of meeting systems and business requirements. Maintains a deep understanding of architecture, software patch fixes and techniques for managing agile software updates across a broad spectrum of systems, applications and requirements. Conducts training with stakeholders. Participates in transitions from development to production or steady state.

**IT Consultant**

**Description:** Travels to the customer site to analyze, enhance, and optimize the IT training systems, business processes, training interfaces, used within the organization. Performs interviews, research, and benchmarking for training needs assessments and organizational gap analysis. Provides technical, managerial, and administrative assistance for problem definition, analysis, requirements development and implementation, for complex to extremely complex systems in the subject matter area.

Makes recommendations and advises on organization-wide systems and business process improvements, optimization or maintenance efforts, in the following representative areas: information systems architecture; networks/communications; telecommunications; operations and management; quality management systems; computer languages, operating systems, database systems, security, decision support systems; risk management and electronic analysis, software including commercial software and software development, life-cycle management; modeling and
simulation; graphics; data management; etc.

[This space intentionally blank]
<table>
<thead>
<tr>
<th>Title</th>
<th>Length</th>
<th>Min Participants</th>
<th>Max Participants</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classified National Security (OnDemand Training Annual subscription)</td>
<td>1 hr.</td>
<td>1</td>
<td>500</td>
<td>$19,846.85</td>
</tr>
<tr>
<td>Safeguarding and Loss Prevention of Classified Materials (OnDemand Training Annual subscription)</td>
<td>1 hr.</td>
<td>1</td>
<td>500</td>
<td>$17,872.04</td>
</tr>
<tr>
<td>Insider Threat (OnDemand Training Annual subscription)</td>
<td>1 hr.</td>
<td>1</td>
<td>500</td>
<td>$17,872.04</td>
</tr>
<tr>
<td>Sensitive Compartmented Information (SCI) Awareness (OnDemand Training Annual subscription)</td>
<td>1 hr.</td>
<td>1</td>
<td>500</td>
<td>$17,872.04</td>
</tr>
<tr>
<td>Derivative Classification (Unclassified Briefing) (OnDemand Training Annual subscription)</td>
<td>1 hr.</td>
<td>1</td>
<td>500</td>
<td>$17,872.04</td>
</tr>
<tr>
<td>SANS SEC301 Introduction to Cyber Security</td>
<td>5 day</td>
<td>5</td>
<td>20</td>
<td>$6,674.06</td>
</tr>
<tr>
<td>SANS SEC401 Security Essentials Bootcamp Style</td>
<td>6 day</td>
<td>10</td>
<td>25</td>
<td>$7,352.58</td>
</tr>
<tr>
<td>SANS SEC501 Advanced Security Essentials – Enterprise Defender</td>
<td>6 day</td>
<td>10</td>
<td>25</td>
<td>$7,352.58</td>
</tr>
<tr>
<td>SANS SEC503 Intrusion Detection In-Depth</td>
<td>6 day</td>
<td>10</td>
<td>25</td>
<td>$7,352.58</td>
</tr>
<tr>
<td>SANS SEC504 Hacker Tools, Techniques, Exploits, and Incident Handling</td>
<td>6 day</td>
<td>10</td>
<td>25</td>
<td>$7,352.58</td>
</tr>
<tr>
<td>SANS SEC560 Network Penetration Testing and Ethical Hacking</td>
<td>6 day</td>
<td>10</td>
<td>25</td>
<td>$7,352.58</td>
</tr>
<tr>
<td>SANS SEC566 Implementing and Auditing the Critical Security Controls - In-Depth</td>
<td>6 day</td>
<td>10</td>
<td>20</td>
<td>$7,352.58</td>
</tr>
<tr>
<td>SANS SEC573 Automating Information Security with Python</td>
<td>6 day</td>
<td>10</td>
<td>25</td>
<td>$7,352.58</td>
</tr>
<tr>
<td>SANS FOR500 Windows Forensic Analysis</td>
<td>6 day</td>
<td>10</td>
<td>25</td>
<td>$7,352.58</td>
</tr>
<tr>
<td>SANS FOR508 Advanced Digital Forensics, Incident Response, and Threat Hunting</td>
<td>6 day</td>
<td>10</td>
<td>25</td>
<td>$7,352.58</td>
</tr>
<tr>
<td>SANS ICS410 ICS / SCADA Security Essentials</td>
<td>6 day</td>
<td>10</td>
<td>20</td>
<td>$6,790.61</td>
</tr>
<tr>
<td>MGT512 Security Leadership Essentials for Managers</td>
<td>7 day</td>
<td>10</td>
<td>20</td>
<td>$6,383.88</td>
</tr>
<tr>
<td>SANS GIAC Certification Bundle</td>
<td>1 Day</td>
<td>1</td>
<td>1</td>
<td>$772.84</td>
</tr>
<tr>
<td>SANS Small Fixed Order Bundle (Completed with GIAC and Support Bundle)</td>
<td>Annual</td>
<td>17</td>
<td>17</td>
<td>$143,014.08</td>
</tr>
<tr>
<td>SANS Large Fixed Order Bundle (Completed with GIAC and Support Bundle)</td>
<td>Annual</td>
<td>113</td>
<td>113</td>
<td>$864,394.64</td>
</tr>
</tbody>
</table>
GEC specializes in the design and delivery of customized training for IT, Security Awareness, Classification Briefings, Doing Business with the Federal Government, Small Business Compliance, Acquisition Workforce and Workforce Engagement; deployed over on-demand eLearning and mLearning platforms with Learning Management System (LMS) systems, support, and hosting.

**Classified National Security Training**
Annual Information Security Awareness Training provides training focused on the safeguarding and handling of classified material, Foreign Intelligence Entity (FIE) Threats based on Presidential Directive PPD-12 and identifying Insider Threat - Executive Order 13587. During this course participants, will cover core policies, guidelines, procedures and Executive Orders that protect our nations classified national security information from compromise, and inadvertent disclosure, while increasing National Security Awareness. This course will identify:

- How to recognize Classified Markings
- How to recognize and report improper or suspicious conduct
- How to avoid loss, compromise, or unauthorized disclosure of classified information
- The ethics standards established by Executive Order (EO)13526

**Safeguarding and Loss Prevention of Classified Materials**
During this course, learners will cover examples of: common mistakes; scenarios; and, issues that have historically led to the loss, compromise, and unauthorized disclosure of classified information. Study case scenarios will provide learners with an opportunity, to fully understand the impact of negligent disclosure of classified national security information to unauthorized persons and the sanctions associated with those actions. Upon the completion of this course learners will be able to identify three to four best practices aimed at dismantling harmful actions against an agency, recognize two ways an information security breach could impact classified agency missions, and describe at least two leading techniques use to gain unauthorized access to classified information.

**Insider Threat Awareness Training**
During this course, participants will learn the important role they play in supporting their agency’s effort to deter, detect, and mitigate actions by cleared employees who may represent a threat to national security through potential espionage, violent acts against the Government or the Nation, or unauthorized disclosure of classified information under (EO) 13587. This course will equip participants with the ability to quickly spot potential threats that may arise in your work and personal environments including:

- The importance of detecting and reporting, potential insider threats by cleared employees
- Methodologies of adversaries to recruit trusted insiders and collect classified information
Indicators of insider threat conduct and procedures to report such conduct
Reporting Requirements for Insider Threats

**Sensitive Compartmented Information (SCI) Awareness Training**
This course describes your SCI responsibilities that require you to protect SCI classified material at all times, following all procedures and regulations, to report violations and suspicious activities, and the ability to refrain from discussing SCI information outside of the SCIF, participants will also learn how to properly process and store SCI in addition to:

- When and where to discuss SCI material
- Who might be authorized to control the SCIF
- What qualifies someone for SCI access
- How to properly access secure systems, such as JWICS within a SCIF
- How JWICS User Agreements, Do’s and Don’ts, and Password Policies impact you

**Derivative Classification (Unclassified Briefing)**
This training will provide policy, guidance, and procedures on how to properly mark classified documents using the three required elements. Derivative classifiers have a variety of responsibilities they must meet in order to properly perform derivative classification. Participants will be presented with a number of scenarios and policy guidelines that highlight holders’ expectations for the specific protection requirements for classified information. Holders will learn that “Markings and Designations” serve several purposes, such as:

- Alerting holders
- Identifying what needs to be protected
- Indicating the level of classification
- Providing additional classification guidance

**SANS SEC301 Introduction to Cyber Security**
This is a comprehensive course covering everything from core terminology to the how computers and networks function, security policies, risk management, a new way of looking at passwords, cryptographic principles, network attacks & malware, wireless security, firewalls and many other security technologies, web & browser security, backups, virtual machines & cloud computing. The course prepares you for the Global Information Security Fundamentals (GISF) certification test. The course syllabus is as follows:

- Security’s Foundation
- Computer Function and Networking
- An Introduction to Cryptography
- Cyber Security Technologies

Course Length: 5 days
Prerequisites: None
Minimum Participants: 10
Maximum Participants: 25
Location and Format: Online, OnDemand 4-Month Access Period
SANS SEC401 Security Essentials Bootcamp Style
SEC401: Security Essentials Bootcamp Style is focused on providing you the essential information security skills and techniques you need to protect and secure your organization’s critical information assets and business systems. In SEC401 you will learn the language and underlying theory of computer and information security. You will gain the essential and effective security knowledge you will need if you are given the responsibility to secure systems and/or organizations. The course syllabus is as follows:

- Network Security Essentials
- Defense-in-Depth and Attacks
- Threat Management
- Cryptography, Incident Response, and Risk Management
- Windows Security
- Linux Security

Course Length: 6 days
Prerequisites: None
Minimum Participants: 10
Maximum Participants: 25
Location and Format: Online, OnDemand 4-Month Access Period

SANS SEC501 Advanced Security Essentials – Enterprise Defender
SEC501: Advanced Security Essentials - Enterprise Defender builds on a solid foundation of core policies and practices to enable security teams to defend their enterprise. Participants will learn, 1.) how to build a comprehensive security program focused on preventing, detecting, and responding to attacks, 2.) core components of building a defensible network infrastructure and how to properly secure routers, switches, and network infrastructure, 3.) methods to detect advanced attacks on systems that are currently compromised, 4.) formal methods for performing a penetration test to find weaknesses in an organization's security apparatus, 5.) how to respond to an incident using the six-step process of incident response: Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned, 6.) approaches to analyzing malware, ranging from fully automated analysis to static properties analysis, behavioral analysis, and code analysis. The course syllabus is as follows:

- Defensive Network Architecture
- Penetration Testing
- Security Operations Foundations
- Digital Forensics and Incident Response
- Malware Analysis
- Enterprise Defender Capstone

Course Length: 6 days
SANS SEC503 Intrusion Detection In-Depth

SEC503: Intrusion Detection In-Depth is to acquaint you with the core knowledge, tools, and techniques to defend your networks with insight and awareness. You will learn about the underlying theory of TCP/IP and the most used application protocols, such as DNS and HTTP, so that you can intelligently examine network traffic for signs of an intrusion. The course syllabus is as follows:

- Fundamentals of Traffic Analysis: Part I
- Fundamentals of Traffic Analysis: Part II
- Application Protocols and Traffic Analysis
- Network Traffic Forensics
- NetWars: IDS Version

Course Length: 6 days
Prerequisites: None
Minimum Participants: 10
Maximum Participants: 25
Location and Format: Online, OnDemand 4-Month Access Period

SANS SEC504 Hacker Tools, Techniques, Exploits, and Incident Handling

SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling This course will enable individuals to identify security vulnerabilities, discover intrusions, and engage in comprehensive incident handling plans. General security practitioners, system administrators, and security architects will benefit by understanding how to design, build, and operate their systems to prevent, detect, and respond to attacks. Individuals will learn how to best prepare for an eventual breach, identify active attacks and compromises, and how to develop an incident handling process and prepare their teams for potential threats. The course syllabus is as follows:

- Incident Handling Step-by-Step and Computer Crime Investigation
- Computer and Network Hacker Exploits – Part 1
- Computer and Network Hacker Exploits – Part 2
- Computer and Network Hacker Exploits – Part 3
- Computer and Network Hacker Exploits – Part 4
- Hacker Tools Workshop

Course Length: 6 days
Prerequisites: None
Minimum Participants: 10
Maximum Participants: 50
Location and Format: Online, OnDemand 4-Month Access Period
SANS SEC560 Network Penetration Testing and Ethical Hacking
SEC560 Network Penetration Testing and Ethical Hacking is designed to get individuals ready to conduct a full-scale, high-value enterprise penetration test and at the end of the course you'll do just that. SEC560 will also cover post-exploitation, password attacks, and web apps, pivoting through the target environment to model the attacks of real-world bad actors to emphasize the importance of defense in depth. The course syllabus is as follows:

- Comprehensive Pen Testing Planning, Scoping, and Recon
- In-Depth Scanning
- Exploitation
- Password Attacks and Merciless Pivoting
- Domain Domination and Web App Pen Testing

Course Length: 6 days
Prerequisites: None
Minimum Participants: 10
Maximum Participants: 25
Location and Format: Online, OnDemand 4-Month Access Period

SANS SEC566 Implementing and Auditing the Critical Security Controls - In-Depth
SEC566 Implementing and Auditing the Critical Security Controls – In-Depth will teach individuals how to master the specific techniques and tools needed to implement and audit the Critical Controls. For security professionals SEC566 covers how to implement the controls in an existing network through cost-effective automation. For auditors, CIOs, and risk officers, this course is designed to help individuals understand how you will measure whether the Controls are effectively implemented. The course syllabus is as follows:

- Introduction and Overview of the 20 Critical Controls
- Critical Controls 3, 4, 5 and 6
- Critical Controls 7, 8, 9, 10 and 11
- Critical Controls 12, 13, 14, and 15
- Critical Controls 16, 17, 18, 19, and 20

Course Length: 6 days
Prerequisites: None
Minimum Participants: 10
Maximum Participants: 25
Location and Format: Online, OnDemand 4-Month Access Period
SANS SEC573 Automating Information Security with Python

SEC573: Automating Information Security with Python individuals will learn how to 1.) leverage Python to perform routine tasks quickly and efficiently, 2.) automate log analysis and packet analysis with file operations, regular expressions, and analysis modules to find evil, 3.) develop forensics tools to carve binary data and extract new artifacts, 4.) read data from databases and the Windows Registry, 5.) develop UDP and TCP client and server applications and so much more. The course syllabus is as follows:

- Essentials Workshop with pyWars
- Essentials Workshop with MORE pyWars
- Defensive Python
- Forensics Python
- Offensive Python
- Capture the Flag

Course Length: 6 days
Prerequisites: None
Minimum Participants: 10
Maximum Participants: 25
Location and Format: Online, OnDemand 4-Month Access Period

SANS FOR500 Windows Forensic Analysis

FOR500: Windows Forensic Analysis focuses on building in-depth digital forensics knowledge of Microsoft Windows operating systems. Individuals will learn how to recover, analyze, and authenticate forensic data on Windows systems, track particular user activity on your network, and organize findings for use in incident response, internal investigations, and civil/criminal litigation. Individuals will also be able to leverage their new skills to validate security tools, enhance vulnerability assessments, identify insider threats, track hackers, and improve security policies. The course syllabus is as follows:

- Windows Digital Forensics and Advanced Data Triage
- Core Windows Forensics Part I: Windows Registry Forensics and Analysis
- Core Windows Forensics Part II: USB Devices and Shell Items
- Core Windows Forensics Part III: Email, Key Additional Artifacts, and Event Logs
- Core Windows Forensics Part IV: Web Browser Forensics for Firefox, Internet Explorer and Chrome
- Windows Forensics Challenge

Course Length: 6 days
Prerequisites: None
Minimum Participants: 10
Maximum Participants: 25
Location and Format: Online, OnDemand 4-Month Access Period

SANS FOR508 Advanced Digital Forensics, Incident Response, and
Threat Hunting

FOR508: Advanced Incident Response and Threat Hunting Course will help individuals to detect how and when a breach has occurred, identify compromised and affected systems, perform damage assessments and determine what was stolen or changed, contain and remediate incidents, develop key sources of threat intelligence, hunt down additional breaches using knowledge of the adversary. The course syllabus is as follows:

- Advanced Incident Response & Threat Hunting
- Intrusion Analysis
- Memory Forensics in Incident Response & Threat Hunting
- Timeline Analysis
- Incident Response & Hunting Across the Enterprise | Advanced Adversary & Anti-Forensics Detection
- The APT Threat Group Incident Response Challenge

Course Length: 6 days  
Prerequisites: None  
Minimum Participants: 10  
Maximum Participants: 25  
Location and Format: Online, OnDemand 4-Month Access Period

SANS ICS410 ICS / SCADA Security Essentials

ICS410: ICS/SCADA Security Essentials provides a foundational set of standardized skills and knowledge for industrial cybersecurity professionals. The course is designed to ensure that the workforce involved in supporting and defending industrial control systems is trained to keep the operational environment safe, secure, and resilient against current and emerging cyber threats. The course syllabus is as follows:

- ICS Overview
- Field Devices & Controllers
- Supervisory Systems
- Workstations and Servers
- ICS Security Governance

Course Length: 6 days  
Prerequisites: None  
Minimum Participants: 10  
Maximum Participants: 20  
Location and Format: Online, OnDemand 4-Month Access Period

MGT512 Security Leadership Essentials for Managers

MGT512 Security Leadership Essentials for Managers covers a wide range of security topics across the entire security stack. Data, network, host, application, and user controls
are covered in conjunction with key management topics that address the overall security lifecycle. This also includes governance and technical controls focused on protecting, detecting, and responding to security issues. The course syllabus is as follows:

- Building Your Program
- Protecting Data and Networks
- Protecting and Pathing Systems
- Learning Modern Security Initiatives
- Detecting and Responding to Attacks

Course Length: 7 days
Prerequisites: None
Minimum Participants: 10
Maximum Participants: 20
Location and Format: Online, OnDemand 4-Month Access Period

**SANS GIAC Certification Bundle**

GIAC Certifications provide the highest and most rigorous assurance of cyber security knowledge and skill available to industry, government, and military clients across the world. GIAC exam content and question design are developed through a rigorous process led by GIAC’s on-staff psychometrician and reviewed by experts in each technical area. When GIAC’s are bundle with the courses they can be obtained at a discounted price.

Course Length: 1 day
Prerequisites: None
Minimum Participants: 1
Maximum Participants: 1
Location and Format: Online, OnDemand 4-Month Access Period

**SANS Small Fixed Order Bundle (Completed with GIAC and Support Bundle)**

Allows for customer flexibility in OnDemand course selection (10-50) among the following:

- SANS OnDemand (Online Training)
- SANS Mentor
- SANS SelfStudy
- SANS Summits
- SANS Simulcast
- SANS vLive (Virtual Live Training)
- SANS Live Training Events
- SANS Mentor
- SANS Private Training
- Community SANS
- GIAC Exams, (Practice Exams, Extension, Retakes, and Certification Renewal)

The fixed order provides access to an admin dashboard and the full suite of OnDemand courses listed. Payment is not required until the government receives access to the dashboard and
SANS Large Fixed Order Bundle (Completed with GIAC and Support Bundle)

Allows for customer flexibility in OnDemand course selection (51-200) among the following:

- SANS OnDemand (Online Training)
- SANS Mentor
- SANS SelfStudy
- SANS Summits
- SANS Simulcast
- SANS vLive (Virtual Live Training)
- SANS Live Training Events
- SANS Mentor
- SANS Private Training
- Community SANS
- GIAC Exams, (Practice Exams, Extension, Retakes, and Certification Renewal)

The fixed order provides access to an admin dashboard and the full suite of OnDemand courses listed. Payment is not required until the government receives access to the dashboard and training.

Course Length: 5-7 days
Prerequisites: None
Minimum Participants: 113
Maximum Participants: 113
Location and Format: Online, OnDemand 12-Month Access Period
## Software License Price List

<table>
<thead>
<tr>
<th>Title</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Event and Learning Environment Annual License</td>
<td>$73,702.77</td>
</tr>
</tbody>
</table>