QED SECURE SOLUTIONS LLC

GENERAL SERVICES ADMINISTRATION
FEDERAL SUPPLY SERVICE
AUTHORIZED FEDERAL SUPPLY SCHEDULE PRICE LIST

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 for GSA Advantage!® is: GSAAAdvantage.gov.

Multiple Award Schedule (MAS)
Information Technology – IT Hardware & IT Training

Contract Number: 47QTCA18D00G2

Contract Period: July 10, 2018, through July 9, 2023

Price List Current as of: PS-0010
MOD PS-0010 Effective 03/15/2022

Contractor:
QED Secure Solutions, LLC
105 Olympia Lane
Coppell, TX 75019-5069

Mailing Address:
106 N Denton Pat Road, Suite 120-132
Coppell, TX 75019

Phone: 214-489-7767
Fax: 214-594-9209
sales@QEDsecure.com
http://www.QEDsecure.com

Contractor’s Administration Source:
Jonathan Butts
j.butts@qedsecure.com

Small Business
For more information on ordering from Federal Supply Schedules go to the GSA Schedules page at www.gsa.gov.
CUSTOMER INFORMATION:

1a. TABLE OF AWARDED SPECIAL ITEM NUMBERS (SINs)
- 33411: Purchasing of New Electronic Equipment
- 611420: Information Technology Training
- OLM: Order Level Materials

1b. LOWEST PRICED MODEL NUMBER AND PRICE FOR EACH SIN: SEE FULL PRICING ON PAGE 3.

<table>
<thead>
<tr>
<th>SIN</th>
<th>Model</th>
<th>GSA Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>33411</td>
<td>MIST1-011-W1</td>
<td>$15,070.53</td>
</tr>
<tr>
<td>611420</td>
<td>Cyber Executive Course</td>
<td>$1007.56</td>
</tr>
</tbody>
</table>

1c. HOURLY RATES: N/A

2. MAXIMUM ORDER: $500,000.00 for SIN 33411 & $250,000.00 for SIN 611420 and OLM

3. MINIMUM ORDER: $100

4. GEOGRAPHIC COVERAGE: United States only for SIN 33411, Worldwide for 611420.

5. POINT(S) OF PRODUCTION: USA

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): additional 5% with orders of 10 units and above, SIN 33411. None for SIN 611420.

8. PROMPT PAYMENT TERMS: Net 30 Days. 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: Shipped 30 Business Days after receipt of order.

10b. EXPEDITED DELIVERY: Negotiated at time task order award.

10c. OVERNIGHT AND 2-DAY DELIVERY: Negotiated at time task order award.

10d. URGENT REQUIREMENTS: Customers are encouraged to contact the contractor for the purpose of requesting accelerated delivery.

11. FOB POINT: Destination (CONUS only) on all products. Any products shipped to HI, AK and PR FOB is Origin Pre-pay & Add. The MFC FOB terms are Origin Pre-pay and Add.

12a. ORDERING ADDRESS: Same as contractors address
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:** 106 N. Denton Tap Road, Suite 120-132, Coppell, TX 75019.

14. **WARRANTY PROVISION:** Standard Commercial Warranty. Customer should contact contractor for a copy of the warranty.

15. **EXPORT PACKING CHARGES:** N/A

16. **TERMS AND CONDITIONS OF RENTAL, MAINTENANCE AND REPAIR:** N/A

17. **TERMS AND CONDITIONS OF INSTALLATION:** N/A

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

18b. **TERMS AND CONDITIONS FOR ANY OTHER SERVICES:** N/A

19. **LIST OF SERVICE AND DISTRIBUTION POINTS:** N/A

20. **LIST OF PARTICIPATING DEALERS:** N/A

21. **PREVENTIVE MAINTENANCE:** N/A

22a. **SPECIAL ATTRIBUTES SUCH AS ENVIRONMENTAL ATTRIBUTES (E.G. RECYCLES CONTENT, ENERGY EFFICIENCY AND / OR REDUCED POLLUTANTS):** N/A

22b. **IF APPLICABLE, INDICATE THAT SECTION 508 COMPLIANCE INFORMATION IS AVAILABLE ON ELECTRONIC AND INFORMATION TECHNOLOGY (EIT) SUPPLIES AND SERVICES AND SHOW WHERE FULL DETAILS CAN BE FOUND 9EG CONTRACTORS WEBSITE OR OTHER LOCATION.) THE EIT STANDARDS CAN BE FOUND AT [WWW.SECTION508.GOV](http://WWW.SECTION508.GOV): N/A

23. **UNIQUE ENTITY IDENTIFIER (UEI) NUMBER:** C96YKHLDQM38

24. **NOTIFICATION REGARDING REGISTRATION IN SYSTEM FOR AWARD MANAGEMENT (SAM) DATABASE.** Registered in SAM.

**GSA Approved Products SIN 33411**

| MIST1-011-W1 | Mobile ICS Security Trainer (MIST) | $15,070.53 |

The Mobile ICS Security Trainer is a complete control system in a box, designed for easy presentation of control system and security concepts. It demonstrates the vulnerability of SCADA and PLC components to security failures, highlighting their impact on critical industrial processes. It also shows how to protect systems from attacks using modern SCADA security technologies. The MIST provides a self-contained ICS that features actual components and representative physical processes for a natural gas station. The MIST is accompanied with an instruction and training manual that guides students from the basic functionality of ICS to exploiting and defending against cyber-based attacks. Salient characteristics: 1. Completely self-contained industrial control system that simulates actual natural gas station including scrubber tank and compressor; 2. Hands-on access to all components of a typical industrial control system (ICS); 3. Replicates critical processes.
GSA Approved Training SIN 611420

<table>
<thead>
<tr>
<th>Training Course Title</th>
<th>GSA Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICS CyberSecurity Essentials</td>
<td>$3,022.67</td>
</tr>
<tr>
<td>Avionics Systems Cybersecurity Essentials</td>
<td>$3,022.67</td>
</tr>
<tr>
<td>Embedded Device Cybersecurity Essentials</td>
<td>$3,022.67</td>
</tr>
<tr>
<td>Embedded Device Forensics Security Essentials Course</td>
<td>$3,022.67</td>
</tr>
<tr>
<td>RF Exploitation Course</td>
<td>$3,022.67</td>
</tr>
<tr>
<td>Mission Defense Team Assessment Principles and Certification</td>
<td>$4,030.23</td>
</tr>
<tr>
<td>Cyber Executive Course</td>
<td>$1,007.56</td>
</tr>
</tbody>
</table>

Course Descriptions

1. **ICS Cybersecurity Essentials (3 Day Class)**

   **Minimum/Max Participants:** 12/25

   Today’s security environment is lacking the specialists that understand both the cyber and physical consequences associated with industrial control systems (ICS). We developed the QED ICS Cybersecurity Essentials course offering to help bridge that gap. Students will be guided through lessons that follow a series of carefully designed phases from introduction of ICS cybersecurity concepts to advanced exploitation and defense techniques. The Mobile ICS Security Trainer (MIST) provides each student with a representative ICS to explore attack consequences and defense strategies that helps emphasize fundamental concepts and enforce knowledge through hands-on exercises.

   This training provides students with knowledge and skills specific to processes, procedures, and tools that will enable them to evaluate cybersecurity vulnerabilities associated with key critical infrastructure. The course covers methods and tools for assessing ICS cybersecurity posture at the device and system levels through functional analysis, reverse engineering, protocol evaluation and exploitation development. Specific and strong emphasis is placed on creating and enhancing operations technology knowledge, skills, and abilities through course instruction and hands-on labs. The course leverages the MIST to provide students with a hands-on training environment using real-world scenarios.

2. **Avionics Systems Cybersecurity Essentials (3 Day Class)**

   **Minimum/Max Participants:** 12/25

   Over the history of aviation, aircraft have increasingly relied on computer systems to facilitate operations, reduce flight crew workload, and increase safety and efficiency. In addition to increasing the functionality of computing systems in aircraft, systems have also become more integrated over time. While these efforts have a positive effect on air travel, the increasing complexity and connectedness of these systems may make them increasingly vulnerable to cyber-attacks. We developed the QED Avionics Systems Cybersecurity Essentials course to provide an overview of how avionics systems can be exploited and how an adversary might be able to impact mission effectiveness or flight safety on one or more aircraft.

   The foundation of this course material is built upon real-world assessments of military and commercial aviation systems (including unmanned equipment). This course provides a practical and concise introduction into the world of avionics system security. Students attending this course will gain a fundamental understanding of the security problems associated with avionics systems. The course will provide the technical ability to assess and exploit the embedded devices that are commonly found within aviation systems (e.g., extract firmware/software from embedded devices, reverse engineer the firmware/software, and identify security weaknesses). This course will also provide the technical ability to assess and exploit aviation specific systems (e.g., LRUs, MIL-STD-1553, ARINC, and aviation radio protocols).
3. **Embedded Device Cybersecurity Essentials (3 Day Class)**
Minimum/Max Participants: 12/25

Identifying security vulnerabilities and mitigation strategies for traditional information technology systems relies on pre-packaged security tools and common implementation schemes. Embedded devices, however, are different in the fact that applications are typically focused on specific functionalities, rely on real-time operating systems, and vary widely. Although security tools assist in embedded device cybersecurity analysis, it is a firm understanding of the fundamentals relating to hardware, firmware and application software that is critical. As such, we designed the *QED Embedded Device Cybersecurity Essentials* course around the principles associated with cybersecurity analysis for embedded systems—from the ground up. Those individuals new to this area will gain a fundamental understanding of how to evaluate embedded systems and build the foundations for exploring this growing area. Seasoned security professionals and researchers will be able to apply knowledge learned in this class to further enhance their skills and expand their capabilities.

The *QED Embedded Device Cybersecurity Essentials* course provides foundational skills for reverse engineering, vulnerability identification, and exploit/malware analysis for embedded devices. The course leverages the Embedded Device Training Core (EDTC) to provide students with a hands-on training environment using real-world scenarios.

4. **Embedded Device Forensics Security Essentials Course (3 Day Class)**
Minimum/Max Participants: 12/25

The *QED Embedded Device Forensics Security Essentials Course* provides foundational skills for incident response, digital forensics and malware analysis for embedded devices that are at the core of critical systems. The course is designed to ensure that security experts are trained in the skill-sets necessary to respond to and perform analysis on critical infrastructure systems that are the target of a cyber compromise. The course is a three-day course that teaches the core skill-sets associated with digital forensics and incident response for ICS. The course leverages the Mobile ICS Security Trainer (MIST) and Embedded Device Training Core (EDTC) to provide students with a hands-on training environment that prepares students for real-world scenarios responding to and analyzing actual embedded device cyber-based exploits.

5. **RF Exploitation Course (3 Day Class)**
Minimum/Max Participants: 12/25

Modern technology relies heavily on the radio frequency (RF) spectrum for communications. The over-the-air transmission of data, however, provides the potential for remote system compromise. The *QED RF Exploitation Course* provides fundamental concepts on how systems can be exploited via RF. Students will learn RF device vulnerability discovery and exploitation techniques, ranging from device discovery, passive monitoring, protocol analysis, over-the-air fuzzing and reverse engineering specific to RF technologies. Hands-on labs guide students through the core principles associated with RF exploitation. Applicable laws and safety considerations are discussed.

6. **Mission Defense Team Assessment Principles and Certification (4 Day Class)**
Minimum/Max Participants: 12/25

Department of Defense (DoD) weapon systems have become increasingly sophisticated and technologically advanced. The intricacies associated with advanced technology, however, introduce complexity that makes it difficult to discern vulnerabilities that may exist due to underlying functionality, interconnections, associated subsystems and weaknesses in hardware/software. This course is designed to introduce students associated with Mission Defense Teams to the threats that exist for DoD weapon systems and provides the foundation for developing assessment and mitigation strategies. The course utilizes real-world examples and hands-on labs that walk students through how an attacker can identify attack surfaces and exploit weapon systems and
supporting infrastructure. Students will learn the fundamentals of cybersecurity as applied to DoD weapon systems along with supply chain risks, system weaknesses, operational implications, defense considerations and how an adversary can target weapon systems.

7. **Cybersecurity Weapon Systems Executive Course (1 Day Class)**

   Minimum/Max Participants: 12/25

Although traditional information technology (IT) systems can be found throughout the Department of Defense, mission success relies on the proper functionality and integrity of weapon systems and associated technology. Designed as a one day executive seminar, the *QED Cybersecurity Weapon Systems Executive Course* focuses on the impacts to the mission that can result from adversarial targeting of weapon systems via cyber exploits. Real-world examples are used to demonstrate the process used to initiate cyber-based attacks that specifically target weapon systems. The course provides in-depth discussion on the planning, intelligence gathering, vulnerability discovery and exploitation cycle that takes place to create effects. It also highlights the fundamental differences between traditional IT and weapon systems cybersecurity. Attendees will gain an appreciation of adversary TTPs and learn strategies behind assessing risk for prioritizing weapon systems cyber vulnerabilities in the context of impact to mission.