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: Federal Supply Schedule 70 – General Purpose Commercial Information Technology Equipment, Software, and Services

CONTRACT NUMBER: 47QTCA19D008T

CONTRACT PERIOD: March 27, 2019 through March 26, 2024

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

CONTRACTOR:
Cyber Resilience Group International, LLC
1390 Kenyon Street NW, Suite 320
Washington, DC 20010
202-445-3567
https://cyberresiliencegroup.com/

CONTRACTOR’S ADMINISTRATION SOURCE:
Manuel Lopez, CEO
Phone: 202-445-3567
Email: manny@cyberresiliencegroup.com
Our Clients:

CRG Solutions:

- Cybersecurity and Compliance
- Security Architecture Engineering
- Continuity of Operations Planning (COOP)
- Continuous Monitoring Strategy
- Third Party Assessments & Audits
- NIST RMF Support & Cybersecurity Engineering
- DevOps Security
- Security Control Assessments
- Software Testing and Assurance
- ISSO and ISSE Services
- Security Awareness & Workforce Training
- Computer Network Defense (CND)
- Computer Network Analysis (CNA)
- Insider Threat & Phishing Training
- Incident Response Planning
- Managed Services
- Cloud Security (FEDRAMP)

Who We Are

In a world of consultants trapped in the old model of business, CRG is different. We focus on your success by implementing data-centric strategies. Cost-effective cybersecurity must be addressed early within acquisition and be thoughtfully integrated within systems engineering, test and evaluation, and other acquisition processes in the systems development lifecycle. We are a transparent and agile consulting business made up of highly skilled minds. Our goal is to invest in our customers and deliver impactful strategic, and sustainable information-driven solutions that help customers steer clear of unforeseen risks or cyber-attacks.

CRG Certifications

CRG professionals are certified in industry and vendor benchmarks such as ISACA CISM, CRISC, CISA, IS2 CISSP, PMP, ITIL, Tripwire, Splunk, Palo Alto, Service Now, multiple regulatory compliance: FITARA, FISMA, DoDI 8510/5000, DoD 8570/8140 requirements, NIST SP 800 Series, DCID, SOX, HIPPA, ISO 27001, DCAA Compliant, Cisco, & Intel TS/SCI Cleared Senior Consultants and SMEs.
CUSTOMER INFORMATION:

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

<table>
<thead>
<tr>
<th>SIN</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>611420</td>
<td>Information Technology Training</td>
</tr>
<tr>
<td>54151S</td>
<td>Information Technology Professional Services</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Highly Adaptive Cybersecurity Services (HACS)</td>
</tr>
</tbody>
</table>

1b. **Identification of the lowest priced model number and lowest unit price:** N/A

1c. **HOURLY RATES (Services only):**

<table>
<thead>
<tr>
<th>Labor Category</th>
<th>Contract Year 1</th>
<th>Contract Year 2</th>
<th>Contract Year 3</th>
<th>Contract Year 4</th>
<th>Contract Year 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIN 54151S INFORMATION TECHNOLOGY (IT) PROFESSIONAL SERVICES</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IT Partner/Principal/Director (PPD)</td>
<td>$246.85</td>
<td>$252.28</td>
<td>$257.83</td>
<td>$263.50</td>
<td>$269.30</td>
</tr>
<tr>
<td>IT Senior Manager</td>
<td>$212.29</td>
<td>$216.96</td>
<td>$221.74</td>
<td>$226.61</td>
<td>$231.60</td>
</tr>
<tr>
<td>IT Manager</td>
<td>$187.61</td>
<td>$191.73</td>
<td>$195.95</td>
<td>$200.26</td>
<td>$204.67</td>
</tr>
<tr>
<td>IT Senior Consultant</td>
<td>$167.86</td>
<td>$171.55</td>
<td>$175.33</td>
<td>$179.18</td>
<td>$183.13</td>
</tr>
<tr>
<td>IT Consultant</td>
<td>$138.24</td>
<td>$141.28</td>
<td>$144.39</td>
<td>$147.56</td>
<td>$150.81</td>
</tr>
<tr>
<td>IT Analyst</td>
<td>$118.49</td>
<td>$121.10</td>
<td>$123.76</td>
<td>$126.48</td>
<td>$129.26</td>
</tr>
<tr>
<td>Project Controller III</td>
<td>$113.55</td>
<td>$116.05</td>
<td>$118.60</td>
<td>$121.21</td>
<td>$123.88</td>
</tr>
<tr>
<td>IT Project Delivery Manager 2</td>
<td>$162.92</td>
<td>$166.51</td>
<td>$170.17</td>
<td>$173.91</td>
<td>$177.74</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SIN 54151HACS HIGHLY ADAPTIVE CYBERSECURITY SERVICES (HACS)</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Cybersecurity Partner/Principal/Director</td>
<td>$246.85</td>
<td>$252.28</td>
<td>$257.83</td>
<td>$263.50</td>
<td>$269.30</td>
</tr>
<tr>
<td>Cybersecurity Sr. Manager</td>
<td>$222.17</td>
<td>$227.05</td>
<td>$232.05</td>
<td>$237.15</td>
<td>$242.37</td>
</tr>
<tr>
<td>Cybersecurity IT Manager</td>
<td>$189.58</td>
<td>$193.75</td>
<td>$198.02</td>
<td>$202.37</td>
<td>$206.82</td>
</tr>
<tr>
<td>Cybersecurity Engineer 3</td>
<td>$148.11</td>
<td>$151.37</td>
<td>$154.70</td>
<td>$158.10</td>
<td>$161.58</td>
</tr>
<tr>
<td>Cybersecurity Engineer</td>
<td>$148.11</td>
<td>$151.37</td>
<td>$154.70</td>
<td>$158.10</td>
<td>$161.58</td>
</tr>
<tr>
<td>Cybersecurity Analyst</td>
<td>$143.17</td>
<td>$146.32</td>
<td>$149.54</td>
<td>$152.83</td>
<td>$156.20</td>
</tr>
<tr>
<td>Cybersecurity Project Manager</td>
<td>$162.92</td>
<td>$166.51</td>
<td>$170.17</td>
<td>$173.91</td>
<td>$177.74</td>
</tr>
</tbody>
</table>
## Cybersecurity Project

<table>
<thead>
<tr>
<th>Role</th>
<th>Contract Year 1</th>
<th>Contract Year 2</th>
<th>Contract Year 3</th>
<th>Contract Year 4</th>
<th>Contract Year 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cybersecurity Project Delivery Mgr</td>
<td>$148.11</td>
<td>$151.37</td>
<td>$154.70</td>
<td>$158.10</td>
<td>$161.58</td>
</tr>
<tr>
<td>Cybersecurity Project Delivery Specialist</td>
<td>$108.61</td>
<td>$111.00</td>
<td>$113.45</td>
<td>$115.94</td>
<td>$118.49</td>
</tr>
<tr>
<td>Cybersecurity Project Sr. Analyst</td>
<td>$118.49</td>
<td>$121.10</td>
<td>$123.76</td>
<td>$126.48</td>
<td>$129.26</td>
</tr>
</tbody>
</table>

### SIN 611420 Information Technology Training

<table>
<thead>
<tr>
<th>Course Title</th>
<th>Contract Year 1</th>
<th>Contract Year 2</th>
<th>Contract Year 3</th>
<th>Contract Year 4</th>
<th>Contract Year 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISACA Certified CISM Course Bootcamp</td>
<td>$2,962.22</td>
<td>$3,027.39</td>
<td>$3,093.99</td>
<td>$3,162.06</td>
<td>$3,231.62</td>
</tr>
<tr>
<td>Enterprise Risk Management &amp; NIST Risk Management Framework (RMF) Fundamentals</td>
<td>$691.18</td>
<td>$706.39</td>
<td>$721.93</td>
<td>$737.81</td>
<td>$754.04</td>
</tr>
<tr>
<td>Enterprise Risk Management &amp; NIST Risk Management Framework (RMF) Full Program</td>
<td>$1,925.44</td>
<td>$1,967.80</td>
<td>$2,011.09</td>
<td>$2,055.34</td>
<td>$2,100.55</td>
</tr>
</tbody>
</table>

2. **MAXIMUM ORDER**:  
   - SIN 611420: $250,000  
   - SIN 54151S: $500,000  
   - SIN 54151HACS: $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 contractor 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**: The minimum order is $100

4. **GEOGRAPHIC COVERAGE**: Worldwide

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

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

7. **QUANTITY DISCOUNT(S)**: 1% for orders over $500,000 (for all SINs)

8. **PROMPT PAYMENT TERMS**:  
   - SIN 611420: Net 30  
   - SINs 54151S and 54151HACS: 0.75% if paid within 10 days/Net 30 days  
   - Information for Ordering Offices: Prompt payment terms cannot be negotiated out of the contractual agreement in exchange for other concessions.

9a. Government Purchase Cards must be accepted at or below the micro-purchase threshold.

9b. Government Purchase Cards are accepted above the micro-purchase threshold.  
   Contact contractor for limit.

10. **FOREIGN ITEMS**: N/A
11a. **TIME OF DELIVERY:** 30 days ARO

11b. **EXPEDITED DELIVERY:** Negotiated at the Task Order Level

11c. **OVERNIGHT AND 2-DAY DELIVERY:** N/A

11d. **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.

12. **FOB POINT:** Destination

13a. **ORDERING ADDRESS:** Same as contractor address

13b. **ORDERING PROCEDURES:** Ordering activities shall use the ordering procedures described in Federal Acquisition Regulation 8.405-3 when placing an order or establishing a BPA for supplies or 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).

14. **PAYMENT ADDRESS:** Same as contractor address

15. **WARRANTY PROVISION:** N/A

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

17. **TERMS AND CONDITIONS OF GOVERNMENT PURCHASE CARD ACCEPTANCE:** N/A

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

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

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

20a. **TERMS AND CONDITIONS FOR ANY OTHER SERVICES (IF APPLICABLE):** N/A

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

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

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

24a. **SPECIAL ATTRIBUTES SUCH AS ENVIRONMENTAL ATTRIBUTES (e.g. recycled content, energy efficiency, and/or reduced pollutants):** N/A

24b. **Section 508 Compliance for Electronic and Information Technology (EIT):** N/A

25. **DUNS NUMBER:** 969789242

26. **NOTIFICATION REGARDING REGISTRATION IN SYSTEM FOR AWARD MANAGEMENT (SAM) DATABASE:** Contractor has an Active Registration in the SAM database.
Provided below is a description of each of the categories of professional services offered by CRG Consulting:

**Experience Substitutions:**

<table>
<thead>
<tr>
<th>H.S. Diploma</th>
<th>4yrs added relevant IT experience</th>
<th>Equals</th>
<th>Bachelor’s Degree</th>
</tr>
</thead>
<tbody>
<tr>
<td>Associate’s Degree</td>
<td>1 yr. added relevant experience</td>
<td>Equals</td>
<td>Bachelor’s Degree</td>
</tr>
<tr>
<td>Bachelor’s Degree</td>
<td>2yrs added relevant IT experience</td>
<td>Equals</td>
<td>Master’s Degree</td>
</tr>
<tr>
<td>Master’s Degree</td>
<td>4yrs added relevant IT experience</td>
<td>Equals</td>
<td>Ph.D.</td>
</tr>
</tbody>
</table>

**Cybersecurity Partner/Principal/Director: [PPD] [SIN 54151HACS]:**

**Minimum Education:** Bachelor’s Degree (BS/BA) or equivalent  
**Minimum Experience:** This position requires a minimum of fifteen years of information technology experience.  
**General Experience:** Experience typically includes: executive level management and direction on client engagements, experience in project definition and systems analysis, creation of competitive strategies, and integration of global technical solutions. A PPD is proficient in project estimation and resource planning efforts and in resolving project issues, such as technical compatibility, client expectations, and timing. A PPD identifies themes capable of being developed into new Cybersecurity strategy methodology, helps to ensure overall soundness of analytical approach, and can suggest alternatives. A PPD manages resources; champions firm initiatives and leads developments in new business enterprises through technical innovations. Other experience includes coordinating multiple projects and team and assisting clients in achieving desired program results.  
**Functional Responsibility:** Serves as the client's Cybersecurity engagement manager for specific project areas and assumes responsibility for client communications related to communicating technical concerns. Is the contractor's liaison and point of contact with the Contracting Officer’s Technical and delegated government representatives. Maintains responsibility for formulating work standards, creating strategic project objectives, and managing client issues and feedback. Assumes accountability for supervising designated resources and enforcing quality control practices for each Cybersecurity project. Maintains responsibility for project reviews and overall contract progress and performance.

**Cybersecurity Senior Manager: [SIN 54151HACS]:**

**Minimum Education:** Bachelor’s Degree (BS/BA) or equivalent  
**Minimum Experience:** This position requires a minimum of seven years of information technology experience.  
**General Experience:** Experience typically includes engagement experience in program scope and approach, focus on program delivery and technical integration, ability to drive Cybersecurity Strategy and planning changes at the executive levels, oversight of key cybersecurity enablers, and management of project resources. Maintains responsibility for managing the program team and daily operations of project development or serves in a role as a highly experienced Technical expert and helps to ensure client comfort and feasibility with designed solution. Other experience includes communication with client and project managers and management of multiple projects across various industry lines.  
**Functional Responsibility:** Manages Cybersecurity program activities and is a key point of contact with client executives. Assumes responsibility for program delivery and oversight of key technical enablers on projects and identification of needs for new tools. Conducts regular interaction and communications with the Contracting Officer’s Technical and delegated government representatives. Maintains responsibility for managing technical solutions, delegating appropriate resources, and helping to ensure quality assurance principles are met across projects and deliverables.

**Cybersecurity IT Manager: [SIN 54151HACS]:**

**Minimum Education:** Bachelor’s Degree (BS/BA) or equivalent  
**Minimum Experience:** This position requires a minimum of five years of information technology experience.  
**General Experience:** Experience typically includes management and direction on client engagements or extensive knowledge of and experience with system development and implementation, development of engagement work plans, deployment of program criterion, and related activities. Devises or modifies procedures to solve complex problems, provides guidance and experience on technical solution implementation, engages resources and/or serves as a team leader, performs analyses of client issues, interprets implications of design, and helps to ensure that software design meets business needs. Other experience includes implementing business process reengineering, developing financial
models, orchestrating change management principles, conducting performance measurements, and providing cybersecurity expertise.

**Functional Responsibility:** Serves in the role of project team leader over assigned support areas, often filling the position of project team lead and instructing, directing, and monitoring the work of other cybersecurity staff or serves in a role of an experienced Cybersecurity technical expert. Conducts analysis of work plan completeness, prepares status reports, and supports quality control practices. Performs analyses of client issues, assesses appropriate alternatives and recommends solutions. Communicates client expectations to project team, and escalates appropriate issues to senior level project staff. Maintains technical knowledge within industry and service line.

**Cybersecurity Engineer 3: [SIN 54151HACS]:**

**Minimum Education:** Bachelor’s Degree (BS/BA) or equivalent

**Minimum Experience:** This position requires a minimum of five years of IT consulting and/or directly relevant industry experience and/or educational training in related fields.

**General Experience:** Experience typically includes program management support and familiarity with client issues, assistance with design issues, leading client teams, analysis of project data, and development of appropriate deliverables. Proficient in the use of firm tools and enables better to support the overall objectives and goals of the program objectives. Demonstrates these skills by performing status reports, verifying work plan completeness, and communicating with team members.

**Functional Responsibility:** Provides senior-level analytical and program support and is focused on providing high performance work. A Cybersecurity Senior Consultant contributes to engagement work plan development and often leads less complex engagement tasks to completion within scope and budget. Serves as a senior-level analytical correspondent within engagement team. Assumes responsibility for contributing to work plan development, reaching engagement milestones, and may lead specific Cybersecurity project tasks. Applies business modeling, process modeling, and business design techniques. Conducts analysis of appropriate consulting tools to satisfy program requirements and creates project deliverables. Formulates diagnoses through financial or statistical modeling, assesses appropriate alternatives, and offers conclusions to Project Manager. This position performs analyses and makes diagnoses, as well as defines symptoms and problems, and develops conclusions.

**Cybersecurity Engineer: [SIN 54151HACS]:**

**Minimum Education:** Bachelor’s Degree (BS/BA) or equivalent

**Minimum Experience:** This position requires a minimum of five years in the IT field or other related work experience.

**General Experience:** Experience typically includes proficiency in analysis and defining business needs, applying methodologies, support of program management, exposure to client issues, and development of project deliverables. Aids on completing work plan activities, analyzes relevant data and information, and institutes and supports business solutions.

**Functional Responsibility:** Provides analytical and program support. Completes assigned Cybersecurity engagement tasks within the project scope and budget, while meeting deliverable requirements. Serves as a key analytical resource on engagement team. Assumes responsibility for conducting relevant research, distilling data, and creating reports. Actively engages consulting tools and methodologies to meet project objectives and complete program management activities. Maintains responsibility for quality assurance practices and fostering completion and accuracy of system documentation.

**Cybersecurity Analyst: [SIN 54151HACS]:**

**Minimum Education:** Bachelor’s Degree (BS/BA) or equivalent

**Minimum Experience:** This position requires a minimum of five years of experience in an IT field or related work experience.

**General Experience:** Experience typically includes performing technical and non-technical analyses on project issues and helps to ensure technical implementations follow quality assurance metrics, has programming experience in one or more languages, and is versed in system testing. Other experience includes data warehousing, information systems design, financial modeling, and business process improvement documentation.

**Functional Responsibility:** Serves as a Cybersecurity IT resource on engagement team. Analyzes data and systems architecture, creates designs, and implements information systems solutions. Assists project team in meeting program objectives timely and effectively. Assumes responsibility for process documentation and technical soundness.

**Cybersecurity Project Manager [SIN 54151HACS]:**

**Minimum Education:** Bachelor’s Degree (BS/BA) preferred or equivalent

**Minimum Experience:** This position has a minimum of ten years of consulting and/or industry experience.

**General Experience:** Experience typically includes performing technical and non-technical analyses on project issues and helps to ensure technical implementations follow quality assurance metrics, has programming experience in one or more languages, and is versed in system testing. Other experience includes data warehousing, information systems design, financial modeling, and business process improvement documentation.
**Functional Responsibility**: Primary responsibilities are client service delivery and operations execution on projects ranging in scope including, but not limited to: technology strategy, architecture and service management; Cybersecurity; systems integration; data analytics and visualization; application development and maintenance; help desk operations; infrastructure/network design and management; and cloud (e.g., software, platform, infrastructure as a service). Possess competencies in multiple Cybersecurity technologies, business processes, or combination of both. Collaborates with project teams comprised of other consulting practitioners. Works independently to execute a portion of the project scope and may perform as a project manager on Cybersecurity engagements of moderate size complexity or lead one or multiple work streams on large engagements. Leads deliverables and reviews the work of others for quality and accuracy. Teaches others on the project team about the client environment and mission, and overall project scope. Communicates project delivery schedule and milestones while maintaining productive and professional relationships with client. May perform analyses of a technical or non-technical nature. The role is for a specific Cybersecurity client engagement and employment is tied to ongoing Federal client demand.

**Cybersecurity Project Delivery Manager [SIN 54151HACS]**:
**Minimum Education**: Bachelor’s Degree (BS/BA) preferred or equivalent  
**Minimum Experience**: This position has a minimum of seven years of consulting and/or industry experience.  
**General Experience**: Experience typically includes ability to support Cybersecurity engagements of greater than average size and complexity; ability to lead multiple teams and multiple clients with confidence; excellent teamwork and interpersonal skills; professional oral and written communication skills; drives and leads problem solving and troubleshooting, as well as the development of these skills in junior staff; ability to mentor and manage junior staff and further their professional growth, and ability to acquire U.S. Security Clearance preferred, but not required.  
**Functional Responsibility**: Primary responsibilities are to proactively improve the IT operational systems, processes, and policies in support of the client’s mission through the management and guidance of multiple work streams, teams, and clients. Supports engagements related, but not limited to: technology strategy, architecture and service management; IT and cybersecurity; systems integration; data analytics and visualization; application development and maintenance; help desk operations; infrastructure/network design and management; and cloud (e.g., software, platform, infrastructure as a service). Provides input to key deliverable structure and content, as well as facilitating buy-in of proposed solutions from top management levels. Responsibilities also include directing timely delivery of quality work products for the client. Management engagement risk. The role is specific client IT engagement and employment is tied to ongoing Federal client demand. Responsible for the professional development of Project Delivery junior staff performing the role of counselor and coach, as well as providing leadership and support. This aspect of the role also requires providing input and guidance into the staffing/onboarding/roll-off and/or out-processing of Project Delivery resources.

**Cybersecurity Project Delivery Specialist: [SIN 54151HACS]**:  
**Minimum Education**: Bachelor’s Degree (BS/BA) preferred or equivalent  
**Minimum Experience**: This position has a minimum of five years of consulting and/or industry experience.  
**General Experience**: Experience typically includes ability to work independently; ability to manage small Cybersecurity engagements or work streams within larger engagements; professional oral and written communication skills; problem solving and troubleshooting skills; able to exercise mature judgment; excellent teamwork and interpersonal skills; able to handle multiple team members with confidence; aptitude for troubleshooting and problem-solving and ability to acquire U.S. Security Clearance preferred, but not required.  
**Functional Responsibility**: Primary responsibilities are to have a fundamental understanding of Cybersecurity best practices while taking ownership of tasks and/or project workstreams and guiding more junior professionals. Supports and/or leads workstreams on engagements related, but not limited to: technology strategy, architecture and service management; Cybersecurity; systems integration; data analytics and visualization; application development and maintenance; help desk operations; infrastructure/network design and management; and cloud (e.g., software, platform, infrastructure as a service). Role requires performing analysis and diagnosing client issues. Expected to actively share knowledge and acquired skills with team members through formal and informal channels. Aids in proposal development as required on an as-needed basis. Works independently to execute a portion of the project scope and may perform as a work stream / team lead that directs the work of junior staff. Contributes to deliverables, reviews the work of others for quality and accuracy. Demonstrates an understanding of the client environment and overall project scope. This role is for a specific client Cybersecurity engagement and employment is tied to ongoing Federal client demand.

**Cybersecurity Project Senior Analyst: [SIN 54151HACS]**:  
**Minimum Education**: Bachelor’s Degree (BS/BA) preferred or equivalent  
**Minimum Experience**: This position has a minimum of three years of consulting and/or industry experience.
**General Experience:** Experience typically includes ability to work independently, under general guidance; ability to lead project deliverables through to completion; experience working in teams and in a team environment that is process-oriented and deadline-driven; professional oral and written communication skills; relevant software or application skills necessary to complete job successfully; problem solving and troubleshooting skills with the ability to exercise mature judgment; and ability to acquire U.S. Security Clearance preferred, but not required.

**Functional Responsibility:** Primary responsibilities are to have a fundamental understanding of Cybersecurity best practices. Leads and supports tasks, including deliverable development, on Cybersecurity engagement related, but not limited to: technology strategy, architecture and service management; Cybersecurity; systems integration; data analytics and visualization; application development and maintenance; help desk operations; infrastructure/network design and management; and cloud (e.g., software, platform, infrastructure as a service). Creates and/or pursues project deliverables. May guide and coach Project Delivery Analysts in deliverable development. Able to perform tasks independently. This role performs analysis and diagnoses client issues while demonstrating an understanding of the client environment and overall project scope. This role is for a specific client Cybersecurity engagement and employment is tied to ongoing Federal Client demand.

**IT Partner/Principal/Director [SIN 54151S]:**

**Minimum Education:** Bachelor’s Degree (BS/BA) or equivalent

**Minimum Experience:** This position requires a minimum of ten years of information technology experience.

**General Experience:** Experience typically includes: executive level management and direction on client engagements, experience in project definition and systems analysis, creation of competitive strategies, and integration of global technical solutions. A PPD is proficient in project estimation and resource planning efforts and in resolving project issues, such as technical compatibility, client expectations, and timing. A PPD identifies themes capable of being developed into new IT strategy methodology, helps to ensure overall soundness of analytical approach, and is able to suggest alternatives. A PPD manages resources; champions firm initiatives and leads developments in new business enterprises through technical innovations. Other experience includes coordinating multiple projects and team and assisting clients in achieving desired program results.

**Functional Responsibility:** Serves as the client’s engagement manager for specific project areas and assumes responsibility for client communications related to communicating technical concerns. Is the contractor’s liaison and point of contact with the Contracting Officer’s Technical and delegated government representatives. Maintains responsibility for formulating work standards, creating strategic project objectives, and managing client issues and feedback. Assumes accountability for supervising designated resources and enforcing quality control practices for each project. Maintains responsibility for project reviews and overall contract progress and performance.

**IT Senior Manager: [SIN 54151S]:**

**Minimum Education:** Bachelor’s Degree (BS/BA) or equivalent

**Minimum Experience:** This position requires a minimum of eight years of information technology experience.

**General Experience:** Experience typically includes engagement experience in program scope and approach, focus on program delivery and technical integration, ability to drive IT Strategy and planning changes at the executive levels, oversight of key information technology enablers, and management of project resources. Maintains responsibility for managing the program team and daily operations of project development or serves in a role as a highly experienced Technical expert and helps to ensure client comfort and feasibility with designed solution. Other experience includes communication with client and project managers and management of multiple projects across various industry lines.

**Functional Responsibility:** Manages program activities and is a key point of contact with client executives. Assumes responsibility for program delivery and oversight of key technical enablers on projects and identification of needs for new tools. Conducts regular interaction and communications with the Contracting Officer’s Technical and delegated government representatives. Maintains responsibility for managing technical solutions, delegating appropriate resources, and helping to ensure quality assurance principles are met across projects and deliverables.

**IT Manager: [SIN 54151S]:**

**Minimum Education:** Bachelor’s Degree (BS/BA) or equivalent

**Minimum Experience:** This position requires a minimum of five years information technology experience.

**General Experience:** Experience typically includes management and direction on client engagements or extensive knowledge of and experience with system development and implementation, development of engagement work plans, deployment of program criterion, and related activities. A Project Manager devoices or modifies procedures to solve complex problems, provides guidance and experience on technical solution implementation, engages resources and/or serves as a team leader, performs analyses of client issues, interprets implications of design, and helps to ensure that software design meets business needs. Other experience includes implementing business process reengineering, developing financial models, orchestrating change management principles, and conducting performance measurements.
IT Senior Consultant: [SIN 54151S]:
Minimum Education: Bachelor’s Degree (BS/BA) or equivalent
Minimum Experience: This position has a minimum of five years of IT consulting and/or directly relevant industry experience and/or educational training in related fields.
General Experience: Experience typically includes program management support and familiarity with client issues, assistance with design issues, leading client teams, analysis of project data, and development of appropriate deliverables. Proficient in the use of firm tools and enablers to better support the overall objectives and goals of the program objectives. Demonstrates these skills by performing status reports, verifying work plan completeness, and communicating with team members.
Functional Responsibility: Provides senior-level analytical and program support and is focused on providing high performance work. An IT Senior Consultant contributes to engagement work plan development and often leads less complex engagement tasks to completion within scope and budget. Serves as a senior-level analytical correspondent within engagement team. Assumes responsibility for contributing to work plan development, reaching engagement milestones, and may lead specific project tasks. Applies business modeling, process modeling, and business design techniques. Conducts analysis of appropriate consulting tools to satisfy program requirements and creates project deliverables. Formulates diagnoses through financial or statistical modeling, assesses appropriate alternatives, and offers conclusions to Project Manager. This position performs analyses and makes diagnoses, as well as defines symptoms and problems, and develops conclusions.

IT Consultant: [SIN 54151S]:
Minimum Education: Bachelor’s Degree (BS/BA) or equivalent
Minimum Experience: This position requires a minimum of five years in the IT field or other related work experience.
General Experience: Experience typically includes proficiency in analysis and defining business needs, applying methodologies, support of program management, exposure to client issues, and development of project deliverables. Aids on completing work plan activities, analyzes relevant data and information, and institutes and supports business solutions.
Functional Responsibility: Provides analytical and program support. Completes assigned engagement tasks within the project scope and budget, while meeting deliverable requirements. Serves as a key analytical resource on engagement team. Assumes responsibility for conducting relevant research, distilling data, and creating reports. Actively engages consulting tools and methodologies to meet project objectives and complete program management activities. Maintains responsibility for quality assurance practices and fostering completion and accuracy of system documentation.

IT Analyst: [SIN 54151S]:
Minimum Education: Bachelor’s Degree (BS/BA) or equivalent
Minimum Experience: This position requires three years of experience in an IT field or related work experience.
General Experience: Experience typically includes performing technical and non-technical analyses on project issues and helps to ensure technical implementations follow quality assurance metrics, has programming experience in one or more languages, and is versed in system testing. Other experience includes data warehousing, information systems design, financial modeling, and business process improvement documentation.

Functional Responsibility: Serves as an information technology resource on engagement team. Analyzes data and systems architecture, creates designs, and implements information systems solutions. Assists project team in meeting program objectives timely and effectively. Assumes responsibility for process documentation and technical soundness.

Project Controller III (Senior Project Controller) [54151S]:
Minimum Education: Bachelor’s Degree (BS/BA) or equivalent
Minimum Experience: This position requires a minimum of 5 years of experience in a financial analysis role.
General Experience: Project Controllers specialize in project operations serving as a focal point for key aspects of program’s business and financial management and control. Project controllers provide engagement management knowledge for the entire project management team(s) by assisting with initiating and controlling organization and logistical aspects of projects. Their greatest value, however, is in their understanding and application of sound business and financial processes to ensure efficient program execution.
Responsibilities: Project Controller III’s (PCIII) are responsible for supporting one or more project teams through the coordination and management of key program and financial management activities. PCIII’s take the lead role in the implementation of appropriate project management controls such as forecasting, budgeting, financial analysis, reconciliation, and forecasting processes. PCIII’s also develop and implement the necessary standards and metrics for project, quality, and risk management activities and offer financial advice tailored for their particular project. PCIII’S often provide oversight and management of other program control resources and are responsible for deliverable quality
reviews. buy-in of proposed solutions from top management levels. Responsibilities also include directing timely delivery of quality work products for the client. Management engagement risk. The role is specific client IT engagement and employment is tied to ongoing Federal client demand. Responsible for the professional development of Project Delivery junior staff performing the role of counselor and coach, as well as providing leadership and support. This aspect of the role also requires providing input and guidance into the staffing/onboarding/roll-off and/or out processing of Project Delivery resources.

**IT Project Delivery Manager 2 [54151S]:**

**Minimum Education:** Bachelor’s Degree (BS/BA) or equivalent

**Minimum Experience:** This position requires a minimum of 9 years of experience

**General Experience:** Experience typically includes ability to manage IT engagements of moderate size and complexity, or work streams within a large engagement; professional oral and written communication skills, and presentation skills; strong problem solving and troubleshooting skills; ability to mentor and manage junior staff and further their professional growth, and ability to acquire U.S. Security Clearance preferred, but not required.

**Functional Responsibility:** Primary responsibilities are client service delivery and operations execution on projects ranging in scope including, but not limited to: technology strategy, architecture and service management; IT security; systems integration; data analytics and visualization; application development and maintenance; help desk operations; infrastructure/network design and management; and cloud (e.g., software, platform, infrastructure as a service). Possess competencies in multiple IT technologies, business processes, or combination of both. Collaborates with project teams comprised of other consulting practitioners. Works independently to execute a portion of the project scope, and may perform as a project manager on IT engagements of moderate size complexity, or lead one or multiple work streams on large engagements. Leads deliverables and reviews the work of others for quality and accuracy. Teaches others on the project team about the client environment and mission, and overall project scope. Communicates project delivery schedule and milestones while maintaining productive and professional relationships with client. May perform analyses of a technical or non-technical nature. The role is for a specific IT client engagement and employment is tied to ongoing Federal client demand.
Course Descriptions
SIN 611420 Information Technology Training

Certified Information Security Manager (CISM)

Course Overview
In this course, students will establish processes to ensure that information security measures align with established business needs.

Who Should Attend
The intended audience for this course is information security and IT professionals, such as network administrators and engineers, IT managers, and IT auditors, and other individuals who want to learn more about information security, who are interested in learning in-depth information about information security management, who are looking for career advancement in IT security, or who are interested in earning the CISM certification.

Course Objectives
Establish and maintain a framework to provide assurance that information security strategies are aligned with business objectives and consistent with applicable laws and regulations. Identify and manage information security risks to achieve business objectives. Create a program to implement the information security strategy. Implement an information security program. Oversee and direct information security activities to execute the information security program. Plan, develop, and manage capabilities to detect, respond to, and recover from information security incidents.

Course Outline
- Information Security Governance
  9. Develop an Information Security Strategy
  10. Align Information Security Strategy with Corporate Governance
  11. Identify Legal and Regulatory Requirements
  12. Justify Investment in Information Security
  13. Identify Drivers Affecting the Organization
  14. Obtain Senior Management Commitment to Information Security
  15. Define Roles and Responsibilities for Information Security
  16. Establish Reporting and Communication Channels

Day 1- Information Risk Management

  17. Implement an Information Risk Assessment Process
  18. Determine Information Asset Classification and Ownership
  19. Conduct Ongoing Threat and Vulnerability Evaluations
  20. Conduct Periodic BIAs
  21. Identify and Evaluate Risk Mitigation Strategies
  22. Integrate Risk Management into Business Life Cycle Processes
  23. Report Changes in Information Risk

Day 2- Information Security Program Development

  24. Develop Plans to Implement an Information Security Strategy
  25. Security Technologies and Controls
  26. Specify Information Security Program Activities
  27. Coordinate Information Security Programs with Business Assurance Functions
  28. Identify Resources Needed for Information Security Program Implementation
  29. Develop Information Security Architectures
  30. Develop Information Security Policies
  31. Develop Information Security Awareness, Training, and Education Programs
  32. Develop Supporting Documentation for Information Security Policies
Day 3- Information Security Program Implementation

33. Integrate Information Security Requirements into Organizational Processes
34. Integrate Information Security Controls into Contracts
35. Create Information Security Program Evaluation Metrics

Day 4- Information Security Program Management

36. Manage Information Security Program Resources
37. Enforce Policy and Standards Compliance
38. Enforce Contractual Information Security Controls
39. Enforce Information Security During Systems Development
40. Maintain Information Security Within an Organization
41. Provide Information Security Advice and Guidance
42. Provide Information Security Awareness and Training
43. Analyze the Effectiveness of Information Security Controls
44. Resolve Noncompliance Issues

Day 5- Incident Management and Response

45. Develop an Information Security Incident Response Plan
46. Establish an Escalation Process
47. Develop a Communication Process
48. Integrate an IRP
49. Develop IRTs
50. Test an IRP
51. Manage Responses to Information Security Incidents
52. Perform an Information Security Incident Investigation
53. Conduct Post-Incident Reviews

This course is intended for information security managers with at least 5 years’ experience in the Information security field, length of course is 5 days

Location can be at customer site or offsite depending on student participation. Earning a CISM certificate satisfies Federal Civilian & DoD 857001-M requirements for IAM Level II & III CND-SP Manager job roles.

Course Overview

The RMF for Federal Agencies training program is suitable for federal employees and contractors in non-DoD “civil” agencies and the intelligence community. The full program consists of a one-day RMF for Federal Agencies – Fundamentals class, followed by a three- day RMF for Federal Agencies – In Depth class. • RMF for Federal Agencies – Fundamentals (One Day) provides an overview of information security and risk management and proceeds to a high-level view of FISMA regulations, roles, and responsibilities, and NIST RMF process steps, including security authorization (aka. certification and accreditation). It also includes an introduction to the NIST RMF documentation package and the NIST security controls. • RMF for Federal Agencies – In Depth (Three Days) expands on these topics at a level of detail that enables practitioners to immediately apply the training to their daily work. Each student will gain an in depth knowledge of the NIST publications along with the practical guidance needed to implement them in his/her environment. Each activity in the NIST SP 800-37 Risk Management Framework is covered in detail, as is each component of the documentation package. NIST SP 800-53 Security Controls and NIST 800- 53a Assessment Procedures are covered in detail, as are CNSSI 1253 “enhancements” applicable to National Security systems and the intelligence community. “Class participation” exercises and collaboration reinforce key concepts. RMF for Federal Agencies

▪ Fundamentals is recommended as a “prerequisite” to RMF for Federal Agencies – In Depth.
Who Should Attend?

The RMF for Federal Agencies training program is suitable for employees and contractors of federal “civil” agencies and the intelligence community, as well as their supporting vendors and service providers. Managers and others who wish to gain high-level knowledge of RMF should attend RMF for Federal Agencies – Fundamentals (one day).

Those who wish to gain detailed implementation knowledge of RMF and NIST Security Controls should attend both RMF for Federal Agencies – Fundamentals and RMF for Federal Agencies – In Depth (total of four days).

**RMF for Federal Agencies – Fundamental (One Day Course)**

- Introduction and Logistics
- Information Security and Risk Management Foundation
- Understanding FISMA
- FIPS and NIST Special Pubs
- Risk Management Evolves (NIST SP 800-37, 800-39)
- Introduction to the RMF Life Cycle
- Key Roles in the RMF
- RMF Documentation
- Introduction to Security Controls
- Supporting Resources
- Course Summary
- Course Evaluation

Location can be at customer site or offsite depending on student participation.

**RMF for Federal Agencies – In Depth for Senior Management and Program Managers (Three Day Course)**

**Day 1**

- Introduction and Logistics
- Foundations of Information Security and Risk Management
- Exercise 1 - Security Brainstorming
- Roles and Responsibilities
- Exercise 2 - Roles/Responsibilities
- RMF Life Cycle Process (NIST SP 800-37)
- "Step 0" - Preparing for RMF
- Exercise 3 - System Boundary
- Step 1 – Categorize (FIPS 199, NIST SP 800-60)
- Exercise 4 - System Categorization
- Step 2 – Select (FIPS 200, NIST SP 800-53)
- Step 3 – Implement
- Step 4 - Assess

**Day 2**
• Step 5 – Authorize
• Step 6 – Monitor (NIST SP 800-137)
• Exercise 5 - RMF Life Cycle
• RMF Challenges
• RMF Documentation
• System Security Plan
• Security Assessment Report
• Plan of Action and Milestones (POA&M)
• Supporting Documentation (Artifacts)
• Exercise 6 - RMF Documentation
• NIST Security Controls
• Management Controls
• Operational Controls

Day 3

• Technical Controls
• Exercise 7 – “Dissecting” a Security Control
• Security Controls Assessment (NIST SP 800-53A)
• Exercise 8 - Security Control Assessment
• RMF Resources
• Automated Security Tools
• Exercise 9 - Security Testing Tools
• Practical Guidance
• Exercise 10 - RMF Project Plan Case Study
• Course Summary • Course Evaluation • RMF "Jeopardy

Location can be at customer site or offsite depending on student participation.