

GENERAL SERVICES ADMINISTRATION AUTHORIZED FEDERAL SUPPLY SCHEDULE PRICE LIST

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

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

**Special Item Number 132-51
Information Technology (IT) Professional Services**

**Special Item Number 132-52
Electronic Commerce Services and Subscription Services**

**Special Item Number 132-60F
IT and Identity Access Management (IAM) Professional Services**

Note 1: All non-professional labor categories must be incidental to and used solely to support hardware, software and/or professional services, and cannot be purchased separately.

Note 2: Offerors and Agencies are advised that the Group 70 – Information Technology Schedule is not to be used as a means to procure services which properly fall under the Brooks Act. These services include, but are not limited to, architectural, engineering, mapping, cartographic production, remote sensing, geographic information systems and related services. FAR 36.6 distinguishes between mapping services of an A/E nature and mapping services which are not connected nor incidental to the traditionally accepted A/E Services.

Note 3: This solicitation is not intended to solicit for the reselling of IT Professional Services, except for the provision of implementation, maintenance, integration or training services in direct support of a product. Under such circumstances the services must be performance by the publisher or manufacturer or one of their authorized agents.

CONTRACT NUMBER: GS-35F-0235Y

CONTRACT PERIOD: March 3, 2012 through March 2, 2017

PRICELIST CURRENT THROUGH: Modification PS-0010 dated June 2, 2015

For more information on ordering from this Federal Supply Schedule contract, please visit:
www.gsa.gov/schedules

CONTRACTOR:



Cloudburst Security, LLC
6506 Loisdale Road
Suite 325
Springfield, Virginia 22150
Tel: 703-224-8966
Fax: 703-842-8200
Web: www.cloudburstsecurity.com

CONTRACTOR'S POINT OF CONTACT FOR CONTRACT ADMINISTRATION:

Andrea Suzara Bennett, President
Cloudburst Security, LLC
6506 Loisdale Road
Suite 325
Springfield, Virginia 22150
Tel: 703-224-8966
Fax: 703-842-8200
Web: www.cloudburstsecurity.com

BUSINESS SIZE: Women-Owned Small Business

CONTRACTOR INFORMATION

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

| | |
|---------|---|
| 132-51 | Information Technology Professional Services |
| 132-52 | Electronic Commerce Services and Subscription Services |
| 135-60F | IT and Identity Access Management (IAM) Professional Services |

1b. LOWEST PRICED MODEL NUMBER AND PRICE FOR EACH AWARDED SIN:

See Descriptions and Pricing Matrix (below).

1c. HOURLY RATES (Services only):

See Descriptions and Pricing Matrix (below).

2. MAXIMUM ORDER THRESHOLD:

SIN 132-51 \$500,000
SIN 132-52 \$500,000
SIN 132-60F \$1,000,000

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

3. MINIMUM ORDER THRESHOLD: \$1.00 for all SINS

4. GEOGRAPHIC COVERAGE: Domestic delivery

5. POINT(S) OF PRODUCTION:

Springfield, Virginia, United States

6. DISCOUNT FROM MARKET RATE:

GSA Net Prices can be found in Pricing Matrixes (below). Negotiated discounts have been applied and the Industrial Funding Fee has been added.

7. QUANTITY DISCOUNT(S): None

8. PROMPT PAYMENT TERMS: Net 30

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

9b. Government Purchase Cards are not accepted above the micro-purchase threshold. Contact contractor for limit.

10. FOREIGN ITEMS: None

11a. TIME OF DELIVERY:

Negotiated with the Ordering Agency at the Task Order level.

- 11b. EXPEDITED DELIVERY:** Negotiated with the Ordering Agency at the Task or Delivery Order level
- 11c. OVERNIGHT AND 2-DAY DELIVERY:** Contact the Contractor for Overnight and 2-day rates.
- 11d. URGENT REQUIRMENTS:** Agencies can contact the Contractor's representative to affect a faster delivery. Customers are encouraged to contact the Contractor for the purpose of requesting accelerated delivery.
- 12. FOB POINT:** Destination
- 13a. ORDERING ADDRESS:**
- Cloudburst Security, LLC
6506 Loisdale Road
Suite 325
Springfield, Virginia 22150
Tel: 703-224-8966
Fax: 703-842-8200
- 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:**
- Cloudburst Security, LLC
6506 Loisdale Road
Suite 325
Springfield, Virginia 22150
Tel: 703-224-8966
Fax: 703-842-8200
- 15. WARRANTY PROVISION:** Standard Commercial Warranty
- 16. EXPORT PACKING CHARGES:** None
- 17. TERMS AND CONDITIONS OF GOVERNMENT PURCHASE CARD ACCEPTANCE:** None

- 18. TERMS AND CONDITIONS OF RENTAL, MAINTENANCE, AND REPAIR (IF APPLICABLE):** Not Applicable
- 19. TERMS AND CONDITIONS OF INSTALLATION (IF APPLICABLE):**
Not Applicable
- 20. TERMS AND CONDITIONS OF REPAIR PARTS INDICATING DATE OF PARTS PRICE LISTS AND ANY DISCOUNTS FROM LIST PRICES (IF AVAILABLE):**
Not Applicable
- 20a. TERMS AND CONDITIONS FOR ANY OTHER SERVICES (IF APPLICABLE):**
Not Applicable
- 21. LIST OF SERVICE AND DISTRIBUTION POINTS (IF APPLICABLE):**
Not Applicable
- 22. LIST OF PARTICIPATING DEALERS (IF APPLICABLE):**
Not Applicable
- 23. PREVENTIVE MAINTENANCE (IF APPLICABLE):**
Not Applicable
- 24a. SPECIAL ATTRIBUTES SUCH AS ENVIRONMENTAL ATTRIBUTES (e.g. recycled content, energy efficiency, and/or reduced pollutants):**
Not Applicable
- 24b. Section 508 Compliance for Electronic and Information Technology (EIT):**
Not Applicable
- 25. DUNS NUMBER:** 788223647
- 26. NOTIFICATION REGARDING REGISTRATION IN SYSTEM FOR AWARD MANAGEMENT (SAM) DATABASE:**

Contractor has an active registration in the System for Award Management (SAM) database.
-

**27. INFORMATION TECHNOLOGY (IT) PROFESSIONAL SERVICES (SIN 132-51)
PRICE LIST**

| INFORMATION TECHNOLOGY (IT) PROFESSIONAL SERVICES (SIN 132-51) PRICE LIST | | | | | |
|--|--------------------------------|--------------------------------|--------------------------------|--------------------------------|--------------------------------|
| Labor Category | Year 1 | Year 2 | Year 3 | Year 4 | Year 5 |
| Period of Performance | 3 Mar 12 - 2 Mar 13 | 3 Mar 13 - 2 Mar 14 | 3 Mar 14 - 2 Mar 15 | 3 Mar 15 - 2 Mar 16 | 3 Mar 16 - 2 Mar 17 |
| Advanced Cyber Threat Analyst III | - | - | \$206.74 | \$206.74 | \$211.40 |
| Advanced Cyber Threat Analyst II | | \$153.65 | \$156.53 | \$160.05 | \$163.65 |
| Cyber Intelligence Analyst II | | \$90.53 | \$92.23 | \$94.30 | \$96.42 |
| Cyber Risk Specialist III | - | \$120.53 | \$123.24 | \$126.01 | \$128.85 |
| Cyber Risk Specialist II | \$106.00 | \$108.39 | \$110.82 | \$113.32 | \$115.87 |
| Cyber Risk Specialist I | \$92.00 | \$94.07 | \$96.19 | \$98.35 | \$100.56 |
| Cyber Security Engineer I | | \$79.44 | \$80.93 | \$82.75 | \$84.61 |
| Cyber Security Specialist II | | \$153.00 | \$155.87 | \$159.38 | \$162.96 |
| Cyber Security Specialist I | \$106.00 | \$108.39 | \$110.82 | \$113.32 | \$115.87 |
| Cyber Threat Analyst II | \$110.00 | \$112.48 | \$115.01 | \$117.59 | \$120.24 |
| Junior Security Specialist | - | \$75.32 | \$77.01 | \$78.75 | \$80.52 |
| Information System Security Officer I | \$95.00 | \$97.14 | \$99.32 | \$101.56 | \$103.84 |
| Information Assurance Analyst I | | \$88.00 | \$89.65 | \$91.67 | \$93.73 |
| Information Assurance Analyst II | \$107.43 | \$109.85 | \$112.32 | \$114.85 | \$117.43 |
| Information Security Analyst III | - | \$129.52 | \$132.43 | \$135.41 | \$138.46 |
| Information Security Analyst II | \$105.00 | \$107.36 | \$109.78 | \$112.25 | \$114.77 |
| Information Security Analyst I | | \$76.00 | \$77.43 | \$79.17 | \$80.95 |
| Information Security Engineer II | \$127.00 | \$129.86 | \$132.78 | \$135.77 | \$138.82 |
| Information System Security Officer (ISSO) I | | | | | |
| Network Specialist II | \$104.00 | \$106.34 | \$108.73 | \$111.18 | \$113.68 |
| Network Specialist I | \$95.00 | \$97.14 | \$99.32 | \$101.56 | \$103.84 |
| Project Manager II | \$125.00 | \$127.81 | \$130.69 | \$133.63 | \$136.64 |
| Security Assessment & Authorization Analyst II | | \$99.06 | \$100.92 | \$103.19 | \$105.51 |
| Security Assessment & Authorization Analyst III | - | \$120.59 | \$123.30 | \$126.08 | \$128.91 |
| SOC Engineer I | | \$88.85 | \$90.51 | \$92.55 | \$94.63 |
| SOC Operator | | \$66.72 | \$67.97 | \$69.50 | \$71.06 |
| SOC Operator II | - | \$88.71 | \$90.71 | \$92.75 | \$94.83 |
| Solutions Architect/Engineer II | | \$127.00 | \$129.38 | \$132.29 | \$135.27 |
| Solutions Integration Engineer I | | \$76.88 | \$78.32 | \$80.08 | \$81.88 |
| Subject Matter Expert I | \$125.00 | \$127.81 | \$130.69 | \$133.63 | \$136.64 |

Commercial Job Title**Cyber Intelligence Analyst II**

Minimum Education and Experience Bachelor's degree in Information Technology or Business -OR- Associate's degree and two (2) years relevant experience with professional certification, such as CISSP or GREM or GCIH or CEH -OR- four (4) years relevant experience with professional certification, such as CISSP or GREM or GCIH or CEH.

Minimum/General Experience: Minimum of six (6) years Information Technology experience; minimum four (4) years Cyber Threat Intelligence experience.

Functional Responsibility: Provides all-source intelligence analysis with a focus on Advanced Cyber Threats. Provides cyber threat and intelligence analysis, and develops briefings and reports to distribute and aid in information sharing and protection efforts. Provides classified cyber threat and intelligence briefings to senior government officials, and prepares classified and unclassified reports for sharing with other agencies and working groups. Maintains subject matter expertise on existing and emerging cyber threats and threat actors.

Commercial Job Title**Cyber Risk Specialist III**

Minimum Education and Experience: Bachelor's degree in Information Technology or Business -OR- Associate's degree and two (2) years relevant experience with professional certification, such as CISSP or CISM -OR- four (4) years relevant experience with professional certification, such as CISSP or CISM.

Minimum/General Experience: Minimum of eight (8) years Information Technology experience; minimum four (4) years Cyber Security experience.

Functional Responsibility: Ensure clients utilize a comprehensive framework that enables their cyber security management to make accurate risk-based decisions on where to focus resources for tactical and strategic cyber security operations. Provide recommendations for prioritization of audit findings based on highest potential impact and risk to the organization. Perform periodic risk assessment activities and recommend courses of action to clients that minimize risk while meeting business requirements. Develop and evaluate security system plans and risk assessments. Perform periodic reviews of government cyber security policies and provide recommendations for enhancements based on federal compliance mandates and current and emerging cyber security threats and trends. Perform review of security controls, configurations, and architectures and provide recommendations of where to focus efforts to mitigate the most risk to the organization. Performs certification and accreditation activities or interfaces with certification and accreditation team to ensure all systems are certified and accredited and have the proper security controls required for their sensitivity and classification level.

Commercial Job Title**Cyber Risk Specialist II**

Minimum Education and Experience Bachelor's degree in Information Technology or Business -OR- Associate's degree and two (2) years relevant experience with professional certification, such as CISSP or CISM -OR- four (4) years relevant experience with professional certification, such as CISSP or CISM.

Minimum/General Experience: Minimum of six (6) years Information Technology experience; minimum four (4) years Cyber Risk Management experience.

Functional Responsibility: Ensure clients utilize a comprehensive framework that enables their cyber security management to make accurate risk-based decisions on where to focus resources for tactical and strategic cyber security operations. Provide recommendations for prioritization of audit findings based on highest potential impact and risk to the organization. Perform periodic risk assessment activities and recommend courses of action to clients that minimize risk while meeting business requirements. Develop and evaluate security system plans and risk assessments. Perform periodic reviews of government cyber security policies and provide recommendations for enhancements based on federal compliance mandates and current and emerging cyber security threats and trends. Perform review of security controls, configurations, and architectures and provide recommendations of where to focus efforts to mitigate the most risk to the organization. Performs certification and accreditation activities or interfaces with certification and accreditation team to ensure all systems are certified and accredited and have the proper security controls required for their sensitivity and classification level.

Commercial Job Title**Cyber Risk Specialist I**

Minimum Education and Experience Bachelor's degree in Information Technology or Business -OR- Associate's degree and one (1) year relevant experience with professional certification, such as CISSP -OR- two (2) years relevant experience with professional certification, such as CISSP.

Minimum/General Experience: Minimum of three (3) years Information Technology experience; minimum one (1) year Cyber Risk experience.

Functional Responsibility: Ensure clients utilize a comprehensive framework that enables their cyber security management to make accurate risk-based decisions on where to focus resources for tactical and strategic cyber security operations. Provide recommendations for prioritization of audit findings based on highest potential impact and risk to the organization. Perform periodic risk assessment activities and recommend courses of action to clients that minimize risk while meeting business requirements. Develop and evaluate security system plans and risk assessments. Perform periodic reviews of government cyber security policies and provide recommendations for enhancements based on federal compliance mandates and current and emerging cyber security threats and trends. Perform review of security

controls, configurations, and architectures and provide recommendations of where to focus efforts to mitigate the most risk to the organization. Performs certification and accreditation activities or interfaces with certification and accreditation team to ensure all systems are certified and accredited and have the proper security controls required for their sensitivity and classification level.

Commercial Job Title

Cyber Security Engineer I

Minimum Education and Experience Bachelor's degree in Information Technology or Business -OR- Associate's degree and one (1) year relevant experience with professional certification, such as Security+ or CEH -OR- two (2) years relevant experience with professional certification, such as Security+ or CEH.

Minimum/General Experience: Minimum of three (3) years Information Technology experience; minimum one (1) year Cyber Security experience.

Functional Responsibility: Performs administration and engineering tasks for Cyber Security tools including, but not limited to: firewalls, Host and Network Intrusion Detection/Prevention, SIEM tools, and Anti-Malware solutions. Performs research on new features, versions, and vendor bug fixes to ensure all tools and solutions function in a reliable and secure fashion. Works on security engineering projects under direction of senior engineers. Performs troubleshooting of client security tools and solutions, and escalates issues to senior engineers as needed. Performs tuning and configuration changes in coordination with change management and analyst stakeholders.

Commercial Job Title

Cyber Security Specialist II

Minimum Education and Experience Bachelor's degree in Information Technology or Business -OR- Associate's degree and two (2) years relevant experience with professional certification, such as GPEN, CEH, LPT, CISA, or OSCP -OR- two (2) years relevant experience with professional certification, such as GPEN, CEH, LPT, CISA, or OSCP.

Minimum/General Experience: Minimum of six (6) years Information Technology experience; minimum four (4) years Information Security experience.

Functional Responsibility: Performs security assessment activities depending on the scope of the project, including: network vulnerability assessments, network penetration testing, wireless penetration testing/assessments, application security vulnerability assessments, application penetration testing, application source code vulnerability analysis, operational assessments, interviews, and tabletop exercises. Clearly communicates findings with client-identified points of contact through established communications channels and agreed upon reporting deliverables. Leads client briefings and table-top exercises.

Commercial Job Title**Cyber Security Specialist I**

Minimum Education and Experience Bachelor's degree in Information Technology or Business -OR- Associate's degree and two (2) years relevant experience with professional certification, such as GPEN, CEH, LPT, CISA, or OSCP -OR- two (2) years relevant experience with professional certification, such as GPEN, CEH, LPT, CISA, or OSCP.

*Note: substitution experience requirements listed are in addition to the experience requirements below.

Minimum/General Experience: Minimum of four (4) years Information Technology experience; minimum two (2) years Information Security experience.

Functional Responsibility: Performs security assessment activities depending on the scope of the project, including: network vulnerability assessments, network penetration testing, wireless penetration testing/assessments, application security vulnerability assessments, application penetration testing, application source code vulnerability analysis, operational assessments, interviews, and tabletop exercises. Clearly communicates findings with client-identified points of contact through established communications channels and agreed upon reporting deliverables.

Commercial Job Title**Cyber Threat Analyst II**

Minimum Education and Experience: Bachelor's degree in Information Technology or Business -OR- Associate's degree and two (2) years relevant experience with professional certification, such as CISSP or GCIH -OR- four (4) years relevant experience with professional certification, such as CISSP or GCIH.

Minimum/General Experience: Minimum of six (6) years Information Technology experience; minimum four (4) years Information Security experience.

Functional Responsibility: Manages cyber threat information and provides executive reporting as needed. Investigates, analyzes, and reports on sophisticated cyber threats affecting client networks. Participates in agency and government-wide cyber security working groups dealing with advanced persistent threat issues. Evaluates and makes recommendations for the purchase of tools/technologies in support of Cyber Threat Analysis. Designs and develops custom tools to fill gaps in situational awareness and reduce client technology cost.

Commercial Job Title:**Junior Security Specialist**

Minimum Education and Experience Bachelor's degree in Information Technology or Business -OR- Associate's degree and one (1) year relevant experience with professional

certification, such as CAP or Security+ -OR- two (2) years relevant experience with professional certification, such as CAP or Security+

Minimum/General Experience: Minimum of two (2) years Information Technology experience; minimum one (1) year Cyber Security experience.

Functional Responsibility: Ensure clients utilize a comprehensive framework that enables their cyber security management to make accurate risk-based decisions on where to focus resources for tactical and strategic cyber security operations. Provide recommendations for prioritization of audit findings based on highest potential impact and risk to the organization. Perform periodic risk assessment activities and recommend courses of action to clients that minimize risk while meeting business requirements. Develop and evaluate security system plans and risk assessments. Perform periodic reviews of government cyber security policies and provide recommendations for enhancements based on federal compliance mandates and current and emerging cyber security threats and trends. Perform review of security controls, configurations, and architectures and provide recommendations of where to focus efforts to mitigate the most risk to the organization. Performs certification and accreditation activities or interfaces with certification and accreditation team to ensure all systems are certified and accredited and have the proper security controls required for their sensitivity and classification level.

Commercial Job Title

Information Assurance Analyst II

Minimum Education and Experience Bachelor's degree in Information Technology or Business -OR- Associate's degree and two (2) years relevant experience with professional certification, such as CISSP or CISM -OR- four (4) years relevant experience with professional certification, such as CISSP or CISM.

Minimum/General Experience: Minimum of six (6) years Information Technology experience; minimum four (4) years Information Assurance experience.

Functional Responsibility: Coordinate and lead enclave, agency, and government-wide Information Assurance initiatives. Assist government clients in building a successful enterprise Information Assurance capability. Evaluate new enterprise systems and software for security risk. Write Standard Operating Procedures/CONOPS. Perform security architecture review and design. Assist government clients in maintaining compliance for a variety of IA policy requirements, both internal and external. Assist Certification & Accreditation staff by performing Security Test & Evaluation (ST&E). Perform enterprise vulnerability assessment activities, including scanning, tracking compliance to IAVA's and other patches, and assisting system administrators with remediation. Perform evaluations of potential IA tools and solutions and test/integrate selected tools into customer environments.

Commercial Job Title

Information Assurance Analyst I

Minimum Education and Experience Bachelor's degree in Information Technology or Business -OR- Associate's degree and one (1) year relevant experience with professional certification, such as CISSP or GCIH -OR- two (2) years relevant experience with professional certification, such as CISSP (Associate), CEH, or Security+.

Minimum/General Experience: Minimum of four (4) years Information Technology experience; minimum two (2) years Information Security experience.

Functional Responsibility: Coordinate enclave, agency, and government-wide Information Assurance initiatives. Assist government clients in building a successful enterprise Information Assurance capability. Evaluate new enterprise systems and software for security risk. Assist in updates of Standard Operating Procedures/CONOPS. Assist government clients in maintaining compliance for a variety of IA policy requirements, both internal and external. Assist Certification & Accreditation staff by performing Security Test & Evaluation (ST&E). Perform enterprise vulnerability assessment activities, including scanning, tracking compliance to IAVA's and other patches, and assisting system administrators with remediation. Perform evaluations of potential IA tools and solutions and test/integrate selected tools into customer environments.

Commercial Job Title

Information Security Analyst III

Minimum Education and Experience: Bachelor's degree in Information Technology or Business -OR- Associate's degree and two (2) years relevant experience with professional certification, such as CISSP or GCIA or GCIH -OR- four (4) years relevant experience with professional certification, such as CISSP or GCIA or GCIH.

Minimum/General Experience: Minimum of eight (8) years Information Technology experience; minimum four (4) years Cyber Security experience.

Functional Responsibility: Acts as Senior Analyst, providing subject matter expertise on advanced security event analysis, advanced threat characteristics, malware, forensics, and incident response. Acts as escalation point for Junior & Mid-Level Analysts. Focuses on advanced threats and optimization of security event analysis and incident response procedures and solutions. Performs digital media analysis to determine effects of and indicators from cyber attacks. Performs security device changes on as-needed basis.

Commercial Job Title

Information Security Analyst II

Minimum Education and Experience Bachelor's degree in Information Technology or Business -OR- Associate's degree and two (2) years relevant experience with professional certification, such as CISSP or GCIH -OR- four (4) years relevant experience with professional certification, such as CISSP or GCIH.

Minimum/General Experience: Minimum of six (6) years Information Technology experience; minimum four (4) years Information Security experience.

Functional Responsibility: Monitors security systems to ensure optimal performance and reporting are maintained and makes recommendations for improvements to the customer. Performs security event analysis and correlation, including researching potential links to known cyber security threats. Performs digital media analysis to determine effects of and indicators from cyber attacks. Performs security device changes on as-needed basis.

I Commercial Job Title

Information Security Analyst I

Minimum Education and Experience Bachelor's degree in Information Technology or Business -OR- Associate's degree and one (1) year relevant experience with professional certification, such as CISSP or GCIH -OR- two (2) years relevant experience with professional certification, such as CISSP or GCIH.

Minimum/General Experience: Minimum of three (3) years Information Technology experience; minimum one (1) year Information Security experience.

Functional Responsibility Monitors security systems to ensure optimal performance and reporting are maintained and makes recommendations for improvements to the customer. Performs security event analysis and correlation, including researching potential links to known cyber security threats. Performs digital media analysis to determine effects of and indicators from cyber attacks. Performs incident response and triage activities and escalates to senior personnel per established procedures. Performs security device changes on as-needed basis.

Commercial Job Title

Information Security Engineer II

Minimum Education and Experience Bachelor's degree in Information Technology or Business -OR- Associate's degree and two (2) years relevant experience with professional certification, such as CISSP or vendor-specific -OR- four (4) years relevant experience with professional certification, such as CISSP or vendor-specific.

Minimum/General Experience: Minimum of six (6) years Information Technology experience; minimum four (4) years Information Security experience.

Functional Responsibility Documents the security architecture and standard operating procedures for administration of security devices and systems. Monitors security systems to ensure optimal performance and reporting are maintained, and makes recommendations for improvements to the customer. Performs gap analysis of security controls and assists client in prioritizing security countermeasure procurements. Provides subject matter expertise related to Cyber Network Defense tools, as well as their placement and configuration. Acts as senior security engineer/architect and leads security engineering projects. Performs advanced troubleshooting of client security tools and solutions.

Commercial Job Title **Information System Security Officer (ISSO) I**

Minimum Education and Experience Bachelor's degree in Information Technology or Business -OR- Associate's degree and one (1) year relevant experience with professional certification -OR- two (2) years relevant experience with professional certification.

Minimum/General Experience: Minimum of three (3) years Information Technology experience; minimum one (1) year ISSO experience.

Functional Responsibility Work with system engineers and administrators to develop corrective action plans from internal and external audits. Perform routine self-assessment audits to ensure compliance with agency and federal security requirements. Provide tracking, coordination, and reporting for required cyber security training activities. Review and develop system security plans and other required security documentation as required. Perform vulnerability assessment scans or interpret results of scans and track mitigation actions and progress of system engineers and administrators. Perform certification and accreditation activities as required to ensure assigned systems remain accredited and risk is managed to an acceptable level.

Commercial Job Title **Network Specialist II**

Minimum Education and Experience: Bachelor's degree in Information Technology or Business -OR- Associate's degree and two (2) years relevant experience with professional certification -OR- four (4) years relevant experience with professional certification.

Minimum/General Experience: Minimum of eight (6) years Information Technology experience; minimum four (4) years Network Specialist experience.

Functional Responsibility Performs network engineering and administration to ensure high performance and availability of client networks and systems. Monitors network equipment to proactively detect and resolve issues before they impact end users. Performs troubleshooting to quickly resolve network issues and minimize customer impact. Works with cyber security staff to ensure all network and security devices are configured to prevent unauthorized access and preserve high availability. Provides senior engineering support for enterprise system and network projects including network and system architecture design.

Commercial Job Title: SOC Operator II

Minimum Education and Experience: Bachelor's degree in Information Technology or Business -OR- Associate's degree and two (2) years relevant experience with professional certification -OR- four (4) years relevant experience with professional certification.

Minimum/General Experience: Minimum of five (5) years Information Technology experience; minimum four (3) years Information Security experience.

Functional Responsibility: Monitors IDS/IPS and SIEM alerts and triages incidents according to severity and risk; In-depth understanding of IDS, IPS, Firewall and router configurations; Performs packet capture and analysis; Identifies trends and make recommendations for changes to the security architecture to mitigate threats. Assists Senior Analysts with advanced analysis and incident response investigations. Provides assistance, training, and mentoring to Junior Analysts.

Commercial Job Title: SOC Operator

Minimum Education and Experience: Bachelor's degree in Information Technology or Business -OR- Associate's degree and one (1) year relevant experience with professional certification, such as GCIH, CCNA, CCNP, CCNAS, CISSP (Associate) or Security+ -OR- two (2) years relevant experience with professional certification.

Minimum/General Experience: Minimum of three (3) years Information Technology experience; minimum one (1) year Information Security experience.

Functional Responsibility: Monitors IDS/IPS and SIEM alerts and triages incidents according to severity and risk; In-depth understanding of IDS, IPS, Firewall and router configurations; Performs packet capture and analysis; Identifies trends and make recommendations for changes to the security architecture to mitigate threats.

Commercial Job Title: Solutions Architect Engineer II

Minimum Education and Experience: Bachelor's degree in Information Technology or Business -OR- Associate's degree and two (2) years relevant experience with professional certification, such as CISSP or vendor-specific -OR- four (4) years relevant experience with professional certification, such as CISSP or vendor-specific.

Minimum/General Experience: Minimum of six (6) years Information Technology experience; minimum four (4) years Information Security Architecture or Engineering experience.

Functional Responsibility: Documents the security architecture, performs analysis and recommends enhancements to improve security and availability, and reviews proposed architecture changes to assess impact to security posture. Performs evaluations of new technologies and implements new security tools and capabilities, consistent with federal and agency-specific requirements. Performs gap analysis of security controls and assists client in prioritizing security countermeasure procurements. Maintains subject matter expertise on broad range of Cyber Security tools and technologies, especially current and proposed solutions for existing clients. Acts as liaison between cyber security, vendor partners, enterprise architecture, and IT operations and engineering through participation in working groups, tiger teams, and enterprise projects.

Commercial Job Title: **Solutions Integration Engineer I**

Minimum Education and Experience: Bachelor's degree in Information Technology or Business -OR- Associate's degree and one (1) year relevant experience with professional certification, such as CISSP (Associate) or Security+ or vendor specific certification -OR- two (2) years relevant experience with professional certification, such as CISSP (Associate) or Security+ or vendor specific certification

Minimum/General Experience: Minimum of three (3) years Information Technology experience; minimum one (1) year Information Security experience

Functional Responsibility: Performs evaluations of new technologies and implements new security tools and capabilities, consistent with federal and agency-specific requirements. Provides integration and customization of COTS and GOTS cyber security tools and products, including custom coding, scripting, and configuration changes to support federal and agency-specific requirements. Participates in the requirements gathering and analysis process, and attends agency and US government wide working groups pertaining to requirements related to current projects such as: continuous monitoring, cyber threat indicator sharing, and insider threat.

Commercial Job Title **Subject Matter Expert I**

Minimum Education and Experience: Bachelor's degree in Information Technology or Business -OR- Associate's degree and one (1) year relevant experience with professional certification -OR- two (2) years relevant experience with professional certification.

Minimum/General Experience: Minimum of six (6) years Information Technology experience; minimum four (4) years Subject Matter experience.

Functional Responsibility: Develops or reviews requirements from a project's inception to its conclusion in the subject matter area for simple to moderately complex systems. Serves as technical expert on local-level project teams providing technical direction, interpretation, and alternatives. Assists other senior consultants with analysis and evaluation of select systems

and/or applications. Assists with the preparation of recommendations for system improvement, optimization, development, and/or maintenance efforts.

**ELECTRONIC COMMERCE SERVICES AND SUBSCRIPTION SERVICES
(SIN 132-52)**

| MANUFACTURER NAME | MFR PART NO (# of Emails) | PRODUCT DESCRIPTION | GSA Price with IFF |
|--------------------------|--------------------------------------|---|---------------------------|
| ThreatSim | 500 | anti-phishing tool for testing and training | \$ 9,500.00 |
| ThreatSim | 750 | anti-phishing tool for testing and training | \$ 12,500.00 |
| ThreatSim | 1000 | anti-phishing tool for testing and training | \$ 15,500.00 |
| ThreatSim | 1500 | anti-phishing tool for testing and training | \$ 19,000.00 |
| ThreatSim | 2000 | anti-phishing tool for testing and training | \$ 22,500.00 |
| ThreatSim | 2500 | anti-phishing tool for testing and training | \$ 25,000.00 |
| ThreatSim | 3000 | anti-phishing tool for testing and training | \$ 27,500.00 |
| ThreatSim | 3500 | anti-phishing tool for testing and training | \$ 30,000.00 |
| ThreatSim | 4000 | anti-phishing tool for testing and training | \$ 32,500.00 |
| ThreatSim | 4500 | anti-phishing tool for testing and training | \$ 34,000.00 |
| ThreatSim | 5000 | anti-phishing tool for testing and training | \$ 35,500.00 |
| ThreatSim | 5500 | anti-phishing tool for testing and training | \$ 37,000.00 |
| ThreatSim | 6000 | anti-phishing tool for testing and training | \$ 38,500.00 |
| ThreatSim | 6500 | anti-phishing tool for testing and training | \$ 40,000.00 |
| ThreatSim | 7000 | anti-phishing tool for testing and training | \$ 41,500.00 |
| ThreatSim | 7500 | anti-phishing tool for testing and training | \$ 43,000.00 |
| ThreatSim | 8000 | anti-phishing tool for testing and training | \$ 44,000.00 |

| | | | |
|-----------|--------|---|---------------|
| ThreatSim | 8500 | anti-phishing tool for testing and training | \$ 45,000.00 |
| ThreatSim | 9000 | anti-phishing tool for testing and training | \$ 46,000.00 |
| ThreatSim | 9500 | anti-phishing tool for testing and training | \$ 47,000.00 |
| ThreatSim | 10000 | anti-phishing tool for testing and training | \$ 48,000.00 |
| ThreatSim | 12000 | anti-phishing tool for testing and training | \$ 51,500.00 |
| ThreatSim | 15000 | anti-phishing tool for testing and training | \$ 56,750.00 |
| ThreatSim | 17000 | anti-phishing tool for testing and training | \$ 60,250.00 |
| ThreatSim | 20000 | anti-phishing tool for testing and training | \$ 65,500.00 |
| ThreatSim | 22500 | anti-phishing tool for testing and training | \$ 69,250.00 |
| ThreatSim | 25000 | anti-phishing tool for testing and training | \$ 73,000.00 |
| ThreatSim | 27500 | anti-phishing tool for testing and training | \$ 75,750.00 |
| ThreatSim | 30000 | anti-phishing tool for testing and training | \$ 80,500.00 |
| ThreatSim | 35000 | anti-phishing tool for testing and training | \$ 85,500.00 |
| ThreatSim | 40000 | anti-phishing tool for testing and training | \$ 90,500.00 |
| ThreatSim | 45000 | anti-phishing tool for testing and training | \$ 95,500.00 |
| ThreatSim | 50000 | anti-phishing tool for testing and training | \$ 100,500.00 |
| ThreatSim | 60000 | anti-phishing tool for testing and training | \$ 108,000.00 |
| ThreatSim | 80000 | anti-phishing tool for testing and training | \$ 121,750.00 |
| ThreatSim | 90000 | anti-phishing tool for testing and training | \$ 126,750.00 |
| ThreatSim | 100000 | anti-phishing tool for testing and training | \$ 125,000.00 |
| ThreatSim | 125000 | anti-phishing tool for testing and training | \$ 138,000.00 |

**IT AND IDENTITY ACCESS MANAGEMENT (IAM) PROFESSIONAL SERVICES
(SIN 132-60F)**

| IT AND IDENTITY ACCESS MANAGEMENT (IAM) PROFESSIONAL SERVICES (SIN 132-60F) PRICE LIST | | | | | |
|---|--------------------------------|--------------------------------|--------------------------------|--------------------------------|--------------------------------|
| Labor Category | Year 1 | Year 2 | Year 3 | Year 4 | Year 5 |
| Period of Performance | 3 Mar 12 - 2 Mar 13 | 3 Mar 13 - 2 Mar 14 | 3 Mar 14 - 2 Mar 15 | 3 Mar 15 - 2 Mar 16 | 3 Mar 16 - 2 Mar 17 |
| ICAM Policy Specialist III | - | \$135.60 | \$138.65 | \$141.77 | \$144.96 |
| ICAM Technical SME III | - | \$155.87 | \$159.38 | \$162.96 | \$166.63 |

LABOR CATEGORY DESCRIPTIONS (132-60F)

Commercial Job Title

ICAM Policy Specialist III

Minimum Education and Experience: Bachelor's degree in Information Technology or Business -OR- Associate's degree and two (2) years relevant experience with professional certification, such as CISSP or CISM -OR- four (4) years relevant experience with professional certification, such as CISSP or CISM

Minimum/General Experience: Minimum of eight (8) years Information Technology experience; minimum five (5) years FICAM experience.

Functional Responsibility: Develops or reviews requirements from a project's inception to its conclusion in the subject matter area for simple to moderately complex systems. Serves as technical expert on local-level project teams providing technical direction, interpretation, and alternatives. Assists other senior consultants with analysis and evaluation of select systems and/or applications. Assists with the preparation of recommendations for system improvement, optimization, development, and/or maintenance efforts.

Commercial Job Title:

ICAM Technical SME III

Minimum Education and Experience: Bachelor's degree in Information Technology or Business -OR- Associate's degree and four (4) years relevant experience with professional certification, such as CISSP or vendor-specific Identity/Access Management certification - OR- six (6) years relevant experience with professional certification, such as CISSP or vendor-specific Identity/Access Management certification

Minimum/General Experience: Minimum of eight (8) years Information Technology experience; minimum seven (7) years Identity Management experience.

Functional Responsibility: Provides engineering and integration of advanced Identity & Access Management solutions, throughout all project and system lifecycle phases. Supports customer requirements gathering, product evaluations, product integration, and manages identities and account provisioning once the system is functional.