



**GENERAL SERVICES ADMINISTRATION
FEDERAL SUPPLY SERVICE
AUTHORIZED FEDERAL SUPPLY SCHEDULE CATALOG/PRICE LIST**

We get IT right by customizing and adapting IA services for compliance and cost effectiveness. Our pragmatic approach builds success earlier for our customers. Services include Information Assurance & Security, Cyber Security, Health Care IT, IT Infrastructure, and compliance services to meet requirements A&A (formerly C&A), NIST, FISMA and HIPAA.

EmeSec Incorporated is a Service Disabled Veteran Owned Small Business (SDVOSB), Woman-Owned, 8(a) company founded in 2003. EmeSec holds certifications in ISO/IEC 20000-1:2005, ISO 9001:2008, and ISO/IEC 27001:2005

Social-economic status: Small business, Woman Owned business, Service Disabled Veteran Owned Small business, SBA Certified Small Disadvantaged business and SBA Certified 8(a) Firm.

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>

**GENERAL PURPOSE COMMERCIAL INFORMATION TECHNOLOGY
EQUIPMENT, SOFTWARE, AND SERVICES**

FSC GROUP: 70

FPDS Code D302	IT Systems Development Services
FPDS Code D306	IT Systems Analysis Services
FPDS Code D307	Automated Information Systems Design and Integration Services
FPDS Code D308	Programming Services
FPDS Code D310	IT Backup and Security Services
FPDS Code D311	IT Data Conversion Services
FPDS Code D316	IT Network Management Services
FPDS Code D399	Other Information Technology Services, Not Elsewhere Classified

EmeSec Incorporated
1818 Library Street, Suite 500
Reston, VA 20190

703-956-3036 – 703-956-3009 fax
www.emesec.net

GS-35F-0027S

Period Covered by Contract: October 18th, 2005 through October 17th, 2020

Pricelist current through Modification PO-0015, effective October 16, 2015

Products and ordering information in this Authorized Information Technology Schedule Pricelist are also available on the GSA Advantage! System (<http://www.gsadvantage.gov>).

List of Mass Mod Approvals

Mod #	Mod Title	Date of Acceptance
A013	Schedule 70 Refresh 24	11/16/2009
A095	Schedule 70 Refresh 26	7/24/2010
A112	Authorized Negotiators	4/17/2011
A160	Schedule 70 Refresh 27	6/29/2011
A188	Schedule 70 Refresh 28	11/22/2011
A197	Schedule 70 Refresh 29	1/16/2013
A215	Schedule 70 Refresh 30	1/18/2013
A308	Schedule 70 Refresh 31	1/21/2013
A344	Removal of Clause I-FSS-125	12/13/2013
A345	Schedule 70 Refresh 32	9/30/2013
A377	Schedule 70 Refresh 33	5/28/2014
A403	Schedule 70 Refresh 34	01/05/2015
A454	Schedule 70 Refresh 35	06/10/2015

1a. TABLE OF AWARDED SPECIAL ITEM NUMBER (SIN):

132-51 - Information Technology Professional Services – see descriptions on pages 8 to 12.

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

132-51 - Analyst—IT (JUNIOR) at \$70.42 per hour. 1c.

HOURLY RATES (Services Only): See page 15.

2. MAXIMUM ORDER: \$500,000.

3. MINIMUM ORDER: \$100.

4. GEOGRAPHIC COVERAGE:

Domestic delivery is delivery within the 48 contiguous states, Alaska, Hawaii, Puerto Rico, Washington, DC, and U.S. Territories. Domestic delivery also includes a port or consolidation point, within the aforementioned areas, for orders received from overseas activities.

Overseas delivery is delivery to points outside of the 48 contiguous states, Washington, DC, Alaska, Hawaii, Puerto Rico, and U.S. Territories.

The Geographic Scope of Contract will be domestic delivery.

5. **POINT OF PRODUCTION:** Reston, Virginia (Fairfax County).
6. **DISCOUNT FROM LIST PRICES:** Government prices are net.
7. **QUANTITY DISCOUNT(S):** N/A
8. **PROMPT PAYMENT TERMS:** Net 30 days from receipt of invoice or date of acceptance, whichever is later.
- 9a. **Government Purchase Cards are accepted at or below the micro-purchase threshold.**
- 9b. **Government Purchase Cards are accepted above the micro-purchase threshold.**
10. **FOREIGN ITEMS:** None.
- 11a. **TIME OF DELIVERY:** As mutually agreed.
- 11b. **EXPEDITED DELIVERY:** As negotiated on the task order level.
- 11c. **OVERNIGHT AND 2-DAY DELIVERY:** As negotiated on the task order level.
- 11d. **URGENT REQUIRMENTS:** As negotiated on the task order level.
12. **FOB POINT:** Destination.
- 13a. **ORDERING ADDRESS:**
- EmeSec Incorporated
1818 Library Street, Suite 500
Reston, VA 20190
- 13b. **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.
14. **PAYMENT ADDRESS:**
- EmeSec Incorporated
1818 Library Street, Suite 500
Reston, VA 20190
15. **WARRANTY PROVISION:** Not applicable.
16. **EXPORT PACKING CHARGES:** Not applicable.
17. **TERMS AND CONDITIONS OF GOVERNMENT PURCHASE CARD ACCEPTANCE:** Accepted at or below and above the micro-purchase level.
18. **TERMS AND CONDITIONS OF RENTAL, MAINTENANCE, AND REPAIR:** N/A
19. **TERMS AND CONDITIONS OF INSTALLATION:** N/A
20. **TERMS AND CONDITIONS OF REPAIR PARTS INDICATING DATE OF PARTS PRICE LISTS AND ANY DISCOUNTS FROM LIST PRICES:** N/A
- 20a. **TERMS AND CONDITIONS FOR ANY OTHER SERVICES:** N/A

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

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

23. **PREVENTIVE MAINTENANCE:** 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 EIT:** N/A.

The EIT standard can be found at: www.Section508.gov/.

25. **DUNS NUMBER:** 12-897-6821

26. **NOTIFICATION REGARDING REGISTRATION IN SYSTEM OF AWARD MANAGEMENT (SAM) DATABASE:** Yes. CAGE code is 3EPT1

**TERMS AND CONDITIONS APPLICABLE TO INFORMATION TECHNOLOGY (IT)
PROFESSIONAL SERVICES (SPECIAL ITEM NUMBER 132-51)**

1. SCOPE

a. The prices, terms and conditions stated under Special Item Number 132-51 Information Technology Professional Services apply exclusively to IT Professional Services within the scope of this Information Technology Schedule.

b. The Contractor shall provide services at the Contractor's facility and/or at the ordering activity location, as agreed to by the Contractor and the ordering activity.

2. PERFORMANCE INCENTIVES I-FSS-60 Performance Incentives (April 2000)

a. Performance incentives may be agreed upon between the Contractor and the ordering activity on individual fixed price orders or Blanket Purchase Agreements under this contract.

b. The ordering activity must establish a maximum performance incentive price for these services and/or total solutions on individual orders or Blanket Purchase Agreements.

c. Incentives should be designed to relate results achieved by the contractor to specified targets. To the maximum extent practicable, ordering activities shall consider establishing incentives where performance is critical to the ordering activity's mission and incentives are likely to motivate the contractor. Incentives shall be based on objectively measurable tasks.

3. ORDER

a. Agencies may use written orders, EDI orders, blanket purchase agreements, individual purchase orders, or task orders for ordering services under this contract. Blanket Purchase Agreements shall not extend beyond the end of the contract period; all services and delivery shall be made and the contract terms and conditions shall continue in effect until the completion of the order. Orders for tasks which extend beyond the fiscal year for which funds are available shall include FAR 52.232-19 (Deviation – May 2003) Availability of Funds for the Next Fiscal Year. The purchase order shall specify the availability of funds and the period for which funds are available.

b. All task orders are subject to the terms and conditions of the contract. In the event of conflict between a task order and the contract, the contract will take precedence.

4. PERFORMANCE OF SERVICES

a. The Contractor shall commence performance of services on the date agreed to by the Contractor and the ordering activity.

b. The Contractor agrees to render services only during normal working hours, unless otherwise agreed to by the Contractor and the ordering activity.

c. The ordering activity should include the criteria for satisfactory completion for each task in the Statement of Work or Delivery Order. Services shall be completed in a good and workmanlike manner.

d. Any Contractor travel required in the performance of IT Services must comply with the Federal Travel Regulation or Joint Travel Regulations, as applicable, in effect on the date(s) the travel is performed. Established Federal Government per diem rates will apply to all Contractor travel. Contractors cannot use GSA city pair contracts.

5. **STOP-WORK ORDER (FAR 52.242-15) (AUG 1989)**

(a) The Contracting Officer may, at any time, by written order to the Contractor, require the Contractor to stop all, or any part, of the work called for by this contract for a period of 90 days after the order is delivered to the Contractor, and for any further period to which the parties may agree. The order shall be specifically identified as a stop-work order issued under this clause. Upon receipt of the order, the Contractor shall immediately comply with its terms and take all reasonable steps to minimize the incurrence of costs allocable to the work covered by the order during the period of work stoppage. Within a period of 90 days after a stop-work is delivered to the Contractor, or within any extension of that period to which the parties shall have agreed, the Contracting Officer shall either-

(1) Cancel the stop-work order; or

(2) Terminate the work covered by the order as provided in the Default, or the Termination for Convenience of the Government, clause of this contract.

(b) If a stop-work order issued under this clause is canceled or the period of the order or any extension thereof expires, the Contractor shall resume work. The Contracting Officer shall make an equitable adjustment in the delivery schedule or contract price, or both, and the contract shall be modified, in writing, accordingly, if-

(1) The stop-work order results in an increase in the time required for, or in the Contractor's cost properly allocable to, the performance of any part of this contract; and

(2) The Contractor asserts its right to the adjustment within 30 days after the end of the period of work stoppage; provided, that, if the Contracting Officer decides the facts justify the action, the Contracting Officer may receive and act upon the claim submitted at any time before final payment under this contract.

(c) If a stop-work order is not canceled and the work covered by the order is terminated for the convenience of the Government, the Contracting Officer shall allow reasonable costs resulting from the stop-work order in arriving at the termination settlement.

(d) If a stop-work order is not canceled and the work covered by the order is terminated for default, the Contracting Officer shall allow, by equitable adjustment or otherwise, reasonable costs resulting from the stop-work order.

6. **INSPECTION OF SERVICES**

In accordance with FAR 52.212-4 CONTRACT TERMS AND CONDITIONS--COMMERCIAL ITEMS (MAR 2009) (DEVIATION I - FEB 2007) for Firm-Fixed Price orders and FAR 52.212-4 CONTRACT TERMS AND CONDITIONS COMMERCIAL ITEMS (MAR 2009) (ALTERNATE I OCT 2008) (DEVIATION I - FEB 2007) applies to Time-and-Materials and Labor-Hour Contracts orders placed under this contract.

7. **RESPONSIBILITIES OF THE CONTRACTOR**

The Contractor shall comply with all laws, ordinances, and regulations (Federal, State, City, or otherwise) covering work of this character. If the end product of a task order is software, then FAR 52.227-14 (Dec 2007) Rights in Data - General, may apply.

8. **RESPONSIBILITIES OF THE ORDERING ACTIVITY**

Subject to security regulations, the ordering activity shall permit Contractor access to all facilities necessary to perform the requisite IT Professional Services.

9. **INDEPENDENT CONTRACTOR**

All IT Professional Services performed by the Contractor under the terms of this contract shall be as an independent Contractor, and not as an agent or employee of the ordering activity.

10. **ORGANIZATIONAL CONFLICTS OF INTEREST**

a. Definitions.

“Contractor” means the person, firm, unincorporated association, joint venture, partnership, or corporation that is a party to this contract.

“Contractor and its affiliates” and “Contractor or its affiliates” refers to the Contractor, its chief executives, directors, officers, subsidiaries, affiliates, subcontractors at any tier, and consultants and any joint venture involving the Contractor, any entity into or with which the Contractor subsequently merges or affiliates, or any other successor or assignee of the Contractor.

An “Organizational conflict of interest” exists when the nature of the work to be performed under a proposed ordering activity contract, without some restriction on ordering activities by the Contractor and its affiliates, may either (i) result in an unfair competitive advantage to the Contractor or its affiliates or (ii) impair the Contractor’s or its affiliates’ objectivity in performing contract work.

b. To avoid an organizational or financial conflict of interest and to avoid prejudicing the best interests of the ordering activity, ordering activities may place restrictions on the Contractors, its affiliates, chief executives, directors, subsidiaries and subcontractors at any tier when placing orders against schedule contracts. Such restrictions shall be consistent with FAR 9.505 and shall be designed to avoid, neutralize, or mitigate organizational conflicts of interest that might otherwise exist in situations related to individual orders placed against the schedule contract. Examples of situations, which may require restrictions, are provided at FAR 9.508.

11. **INVOICES**

The Contractor, upon completion of the work ordered, shall submit invoices for IT Professional services. Progress payments may be authorized by the ordering activity on individual orders if appropriate. Progress payments shall be based upon completion of defined milestones or interim products. Invoices shall be submitted monthly for recurring services performed during the preceding month.

12. **PAYMENTS**

For firm-fixed price orders the ordering activity shall pay the Contractor, upon submission of proper invoices or vouchers, the prices stipulated in this contract for service rendered and accepted. Progress payments shall be made only when authorized by the order. For time and materials orders, the Payments under Time and Materials and Labor Hour Contracts at FAR 52.212-4 (MAR 2009) (ALTERNATE I – OCT 2008) (DEVIATION I – FEB 2007) applies to time and materials orders placed under this contract. For labor hour orders, the Payment under Time and Materials and Labor Hour Contracts at FAR 52.212-4 (MAR 2009) (ALTERNATE I – OCT 2008) (DEVIATION I – FEB 2007) applies to labor hour orders placed under this contract. 52.216-31(Feb 2007) Time-and-Materials/Labor-Hour Proposal Requirements—Commercial Item Acquisition. As prescribed in 16.601(e)(3), insert the following provision:

(a) The Government contemplates award of a Time-and-Materials or Labor-Hour type of contract resulting from this solicitation.

(b) The offeror must specify fixed hourly rates in its offer that include wages, overhead, general and administrative expenses, and profit. The offeror must specify whether the fixed hourly rate for each labor category applies to labor performed by—

- (1) The offeror;
- (2) Subcontractors; and/or
- (3) Divisions, subsidiaries, or affiliates of the offeror under a common control.

13. RESUMES

Resumes shall be provided to the GSA Contracting Officer or the user ordering activity upon request.

14. INCIDENTAL SUPPORT COSTS

Incidental support costs are available outside the scope of this contract. The costs will be negotiated separately with the ordering activity in accordance with the guidelines set forth in the FAR.

15. APPROVAL OF SUBCONTRACTS

The ordering activity may require that the Contractor receive, from the ordering activity's Contracting Officer, written consent before placing any subcontract for furnishing any of the work called for in a task order.

16. DESCRIPTION OF IT PROFESSIONAL SERVICES AND PRICING

Number	Labor Category	Minimal General Experience	Functional Duties	Minimum Education
1	Senior Information Security Engineer	Two years' experience in providing risk analysis assessments using best business practices; Able to demonstrate business value either through cost savings or return on investment	Carries out risk assessment analysis, review and procedures; Developed all information systems documentation related to products and services; matched best practices with company standard practices and goals requirements. Provides network hardware and software implementation; includes migration of critical applications; Testing of network capabilities and functionality; training of system administrator(s).	BA or BS Degree; Or 4 years' experience in aspects of network security and professional security certification.
2	Senior Network Engineer	Two years' experience with general and proprietary network equipment, policies, plans and procedures including broadband and wireless access issues; security applications	Works with Senior Information Security Engineer to report on the procedures, plans and policies as they relate to risks for the organization. Develops documentation for report. Prepares hardware for implementation; tests applications upon implementation for functionality; establishes remote access capabilities; provides training regarding remote access; and outlines recovery procedures for hardware and software.	BS or BA Degree with two years' experience with network plans and policy; OR 5 years of technical computer network experience and an understanding of applications.

Number	Labor Category	Minimal General Experience	Functional Duties	Minimum Education
3	Principal IT Specialist	A least one experience as Team Leader in the development of certification and Accreditation package in accordance guidelines; sets project goals; monitors performance and development of deliverables.	Provides daily technical and managerial supervision and direction to senior system engineers and other staff to accomplish certification and accreditation of major web systems. Assists the project manager with high level advice in determining workload distribution to ensure completion on time and on budget for this analysis. Provides guidance on data flow; security documentation for complex system. Establishes direction to senior system engineers and other staff to accomplish initial status related to certification and accreditation for developing general support system; Establishes the timeline and initial requirements assessment for certification and accreditation; Assists the project manager and customer in evaluating a means for lowering risks of certification to the system while lowering overall costs for certification to the system.	MS Degree and experience with NIST elements or BS degree with 4 years' experience in Information Assurance including a security certification and experience with NIST elements.
4	Senior Engineer/Analyst	Two years' experience; responsible for integrating technical security analysis and evaluation into a report with minimal assistance from more senior project leader. Works with client to identify undocumented risks, clarifies available security documentation.	Responsible for the creation of C&A documentation (both hardware and software descriptions) for system under analysis and evaluation; includes limit configuration testing and evaluation of test results; reports issues to Principal IT Specialist for review, analysis and final risk determination. Evaluates available systems documentation; Updates documentation and guidance on data flow assessments; Identifies highest areas of risk for regulatory compliance including FDA, HIPAA and NIST; security documentation for complex system.	BS degree; Past management of up to 4 personnel; 3 years of security planning or implementation.
5	Technical Analyst	Responsible for editing technical documentation; works with others to make documents more readable and coherent; adapts format as needed to do so.	Works with the project leader to establish version numbers, documents library and select font, colors and format for technical documents to streamline editing and make documents ease to save and use. Works with the technical team members to edit and ensure documentation is readable and coherent. Takes guidance from other team members to validate if grammar edits change technical meaning; Works with the technical team leaders to finalize technical documents; prepares final deliverable reports; manages document library and destruction of documents as required by contract.	Associate Degree or 2 years experience in creating or analyzing written technical documents.

Number	Labor Category	Minimal General Experience	Functional Duties	Minimum Education
6	Principal Information Engineer	Two years' experience in documenting Information Assurance related to compliance guidelines; Works with customer to interview, implement and improve technologies and auditing capabilities	Responsible for the developing assessment criteria and interview process for the System Security Plan for a complex general support system; Responsible for developing consensus and gaining adequate information from a complex political organization; Establishes technical hardware and software boundaries of the System Security Plan. Provides final product deliverable review and edits to staff. Provides supervision and management for the development of emergency continuity planning and disaster recovery related to IT infrastructure support to the entire organization; Establishes interview process and data gathering related to emergency planning; Works with other contracted entities and provides final review of product deliverable	BS degree with professional security certification and 2 years' experience or 6 years' experience with professional security certification.
7	Senior Application Engineer	3 years' experience in technical and administrative security controls for networks and applications; Able to adjust compliance recommendations specific to the organization; Applies knowledge of system and guidelines to make recommendations	Responsible for documenting identified controls and current practices related to Network Infrastructure of a complex organization in order to identify and prioritize risk evaluation and mitigation. Responsible for quantifying the security risks based on the findings. Works with the Principal Information Engineer and customer to optimize compliance documentation; Prioritizes activities and remediation findings to minimize system and organizational risks. Creates procedure templates and documents to support a System Security Plan.	BS degree or 4 years experience in application security related to technical controls.
8	Functional Analyst	Two years' experience in assessing network or system controls, threats and vulnerabilities and in assessing security practices and procedures;	Aids in identifying risks and documenting basic controls for the System Security Plan; responsible for documenting specific system security procedures under the guidance of others. Aids in developing the procedures related to continuity of operations, contingency work and disaster recovery; Works with others and the customer in establishing templates for recording actions, lessons learned, and other requirements related to the contingency plan. Responsible for documenting appropriate system security controls in place under the guidance of others. Compares practices to information assurance best practices.	BS degree or 4 years work experience in computer field.

Number	Labor Category	Minimal General Experience	Functional Duties	Minimum Education
9	Security Analyst	1 year past experience IT system management and implementation of specific regulatory compliance in Privacy or Security documentation; able to complete or relate regulatory compliance to risk	Establishes a cross matrix of HIPAA Privacy and HIPAA Security regulations; evaluates rules for areas of overlap. Creates a crosswalk of areas of overlap with HIPAA Security rules and the mandated regulations of DITSCAP, NIST, and FISMA; incorporate comments to make spreadsheet a tool for evaluating HIPAA compliance. Establishes an action plan for meeting compliance across a multi-organization enterprise; attend meetings and offer security comments; assists in evaluating enterprise wide policies; trains and assists security and policy personnel to understand implications and requirements of HIPAA Privacy and HIPAA Security.	BS/BA Degree or 4 years computer or clinical project experience.
10	HIPAA Security Manager	Two years past experience in developing security policies with client; Able to identify weaknesses of policies and practices and facilitate change to meet compliance regulations;	Establishes requirements for HIPAA Security compliance at the organization; Meet and set expectations with customer and technical managers. Works with customer and clinical leaders to evaluate and establish baseline actions in policy development. Works with client to identify strategies and plan for compliance accountability in quickest method possible; Provides leadership related to HIPAA Security and implementation; Evaluates existing policies and risk assessment regarding HIPAA compliance.	BS degree and professional security certification or 6 years' experience and a professional security certification with experience in policy development and security practice development.
11	Senior Information Engineer	Past experience in monitoring and evaluating security operations of network infrastructure and application toolsets. Able to apply software engineering principles. A minimum of one year experience in managing small teams to accomplish risk assessment, regulatory compliance requirements and/or testing of controls	Begins Certification and Accreditation under DITSCAP guidelines in a classified environment of software toolset; identifies stage of toolset development and existing documentation for the system. Responsible for supervision of and contributions to development of all SSAA requirements under DITSCAP guidelines; Coordinates with other vendors and customers for accurate information and assessment. Supervises the system test and evaluation components related Certification and Accreditation under DITSCAP guidelines in a classified environment; completes System test and evaluation and document findings; Works with customer to mitigate risks where appropriate.	BS degree with Information Security Certification.

Number	Labor Category	Minimal General Experience	Functional Duties	Minimum Education
12	Computer Security System Engineer	Two years' experience in developing C&A documentation for software applications under stringent conditions meeting NIST and/or DITSCAP requirements	Works with Senior engineer to develop specific components of Certification and Accreditation documentation under DITSCAP guidelines in a classified environment; Interviews and reviews documentation as it relates to C&A with a team. Develops Certification and Accreditation documentation in conjunction with others under DITSCAP guidelines in a classified environment: responsible for testing technical controls and reporting the results; identifies risk mitigation specifics regarding C&A results. Certification and Accreditation under DITSCAP guidelines in a classified environment of software toolset; includes all documentation and system test and evaluation.	BA or BS degree OR 6 years' experience in IT Security/Information Assurance.
13	Senior Security Advisor	Two years past healthcare security experience related to networks, clinical systems, and security applications; past experience with HIPAA Security or privacy issues	Provides advisory consultation on prioritization of Regulatory Compliance plan and specific milestones for optimized completion of work compliance. Provides advisory consultation on policy development specific to regulatory compliance; reviews, discusses and edits organizational IA policies. Reviews policies and procedures as well as architectural changes related to Information Security and Information Assurance; Makes recommendations on optimizing accomplishment of IA tasks.	MS Degree and professional security certification or BS degree with professional Security certification and 2 years broad security experience.
14	Project/ Program Manager—IT (INTERMEDIATE)	5 Years	Provides program and/ or project management support to mid-to-large size efforts; supervises the performance of the effort; provides guidance to staff; serves as the interface between EmeSec and the customer; has responsibility for operational decisions.	BS Degree OR 7 Years Exp. w/ AS Degree in IT Field or 9 Years Exp. w/ HS Diploma in related field
15	Project/ Program Manager—IT (JUNIOR)	1 Year	Provides program and/ or project management support to small-to-mid size efforts; supervises the performance of the effort; provides guidance to staff; serves as the interface between EmeSec and the customer; has responsibility for operational decisions.	AS Degree OR 4 Years' Experience with HS Diploma
16	Analyst—IT (INTERMEDIATE)	5 Years	Provides a broad range general analysis services related to information technology issues and efforts that require up to an intermediate level of knowledge.	BS Degree OR 7 Years Exp. w/ AS Degree in IT Field or 9 Years Exp. w/ HS Diploma

Number	Labor Category	Minimal General Experience	Functional Duties	Minimum Education
17	Analyst—IT (JUNIOR)	1 Year	Provides a broad range general analysis services related to information technology issues and efforts that require up to a basic level of knowledge.	AS Degree OR 3 Years' Experience with HS Diploma
18	Information Assurance Specialist—IT (PRINCIPAL)	12 Years	Provides guidance, oversight, management, or expert-level support to efforts intended to mitigate information-related risks, analyzing or protecting information systems, and/ or ensuring confidentiality, integrity, authentication, availability, and non-repudiation.	MS Degree w/ Certifications OR 14 Years Exp. w/ BS Degree in related field
19	Information Assurance Specialist—IT (SENIOR)	8 Years	Provides management or senior-level support to efforts intended to mitigate information-related risks, analyzing or protecting information systems, and/ or ensuring confidentiality, integrity, authentication, availability, and non-repudiation.	BS Degree w certifications OR 10 Years Exp. w/ BS Degree in related field or 12 Years Exp. w/ AS Degree; or HS with 15 years' experience
20	Information Assurance Specialist—IT (INTERMEDIATE)	5 Years	Provides intermediate-level support to efforts intended to mitigate information-related risks, analyzing or protecting information systems, and/ or ensuring confidentiality, integrity, authentication, availability, and non-repudiation.	BS Degree OR 7 Years Exp. w/ AS Degree in IT Field; or 9 Years Exp. w/ HS Diploma
21	Information Security Analyst—IT (SENIOR)	8 Years	Provides management or senior-level support to efforts intended to protect information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction	BS Degree w certification OR 10 Years Exp. w/ BS Degree in related field or 12 Years Exp. w/ AS Degree
22	Information Security Analyst—IT (JUNIOR)	1 Year	Provides support to efforts intended to protect information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction	AS Degree OR 4 Years' Experience with HS Diploma
23	Functional Analyst—IT (PRINCIPAL)	12 Years	Provides guidance, oversight, management, or expert-level support to efforts involving analysis of process, functional issues, or similar, and proposes appropriate solutions.	MS Degree OR 14 Years Exp. w/ BS Degree in related field
24	Functional Analyst—IT (INTERMEDIATE)	5 Years	Provides intermediate-level support to efforts involving analysis of process, functional issues, or similar, and proposes or contributes to the development of appropriate solutions.	BS Degree OR 7 Years Exp. w/ AS Degree in IT Field or 9 Years Exp. w/ HS Diploma in related field
25	Functional Analyst—IT (JUNIOR)	1 Year	Provides support to efforts involving analysis of process, functional issues, or similar, and contributes to the development of appropriate solutions.	AS Degree OR 3 Years' Experience with HS Diploma

Number	Labor Category	Minimal General Experience	Functional Duties	Minimum Education
26	Data Security Specialist—IT (SENIOR)	8 Years	Provides management or senior-level support to efforts intended to ensure that data is safe from corruption and reflects a level of access control appropriate to the effort.	BS Degree w certification OR 10 Years Exp. w/ BS Degree or 12 Years Exp. w/ AS Degree & Certification in related field or HS diploma with 15 years' experience
27	Business Process Auditor—IT (SENIOR)	8 Years	Provides management or senior-level support and analysis to efforts involving collection of related, structured activities or tasks produce a specific service or product	MS Degree OR 10 Years Exp. w/ BS Degree in related field ; or 12 Years Exp. w/ AS Degree
28	Education/ Training Specialist—IT (SENIOR)	8 Years	Provides management or senior-level support under efforts requiring an educational or training component. Support may include situational analysis, process review, providing recommendations for changes, and similar.	MS Degree OR 10 Years Exp. w/ BS Degree or 12 Years Exp. w/ AS Degree
29	Education/ Training Specialist—IT (INTERMEDIATE)	5 Years	Provides intermediate-level support under efforts requiring an educational or training component. Support may include situational analysis, process review, providing recommendations for changes, and similar.	BS Degree OR 7 Years Exp. w/ AS Degree or 9 Years Exp. w/ HS Diploma
30	Database Analyst/ Web Integrator—IT (JUNIOR)	1 Year	Provides support to efforts involving the development, management, or operation of a database, which may include the integration of the database into a web-based environment.	AS Degree OR 4 Years' Experience with HS Diploma

EmeSec Incorporated
GSA Schedule 70, SIN 132-51, Information Technology
Professional Services Labor Category Rates
Applicable to Work Performed “On Site” (at Ordering Activity Location)

Number	Labor Category Title	Rate
1	Senior Information Security Engineer	\$108.97
2	Senior Network Engineer	\$85.09
3	Principal IT Specialist	\$156.61
4	Senior Engineer/Analyst	\$106.28
5	Technical Analyst	\$60.78
6	Principal Information Engineer	\$146.87
7	Senior Application Engineer	\$112.03
8	Functional Analyst	\$103.31
9	Security Analyst	\$97.24
10	HIPAA Security Manager	\$126.41
11	Senior Information Engineer	\$121.56
12	Computer Security System Engineer	\$105.97
13	Senior Security Advisor	\$164.10
14	Project/ Program Manager—IT (INTERMEDIATE)	\$106.40
15	Project/ Program Manager—IT (JUNIOR)	\$84.05
16	Analyst—IT (INTERMEDIATE)	\$87.29
17	Analyst—IT (JUNIOR)	\$70.42
18	Information Assurance Specialist—IT (PRINCIPAL)	\$163.30
19	Information Assurance Specialist—IT (SENIOR)	\$109.42
20	Information Assurance Specialist—IT (INTERMEDIATE)	\$95.96
21	Information Security Analyst—IT (SENIOR)	\$123.08
22	Information Security Analyst—IT (JUNIOR)	\$69.88
23	Functional Analyst—IT (PRINCIPAL)	\$148.02
24	Functional Analyst—IT (INTERMEDIATE)	\$108.48
25	Functional Analyst—IT (JUNIOR)	\$79.64
26	Data Security Specialist—IT (SENIOR)	\$127.26
27	Business Process Auditor—IT (SENIOR)	\$134.67
28	Education/ Training Specialist—IT (SENIOR)	\$122.04
29	Education/ Training Specialist—IT (INTERMEDIATE)	\$95.96
30	Database Analyst/ Web Integrator—IT (JUNIOR)	\$72.86