

# ***Advanced Resource Technologies, Inc.***

**General Services Administration (GSA)  
Federal Supply Service  
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 are available through GSA Advantage!, a menu-driven database system. The INTERNET address for GSA Advantage! is: [GSAAdvantage.gov](http://GSAAdvantage.gov).**

Multiple Award Schedule

FSC Group– Facilities – Facilities Solutions

## **SIN Categories**

Special Item No. 334512– Total Solution Support Products for Facilities Management Systems

Special Item No. OLM - Order Level Material

**FSC/PSC Code:** R425

**SIC/NAICS:** 334512

**Contract Number:** GS-07F-5863P

For more information on ordering from Federal Supply Schedules click on the FSS Schedules button at [fss.gsa.gov](http://fss.gsa.gov).

**Contract Period:** 07/01/2004 –06/30/2024

**Supplement No.:** A812 – dated 02/11/2020

**Prices Shown Herein Are Net (discount deducted)**

**Advanced Resource Technologies, Inc. (ARTI)  
1555 King Street, Suite 200  
Alexandria, VA 22314**

**PHONE: (703) 682-4740 ♦ FAX: (703) 682-4820 ♦ E-mail: [www.team-arti.com](http://www.team-arti.com)**

**Contract Administration: Maria B. Brown**

**Business Size:** Service-Disabled, Veteran-Owned Small Business

**TABLE OF CONTENTS**

	<u>Page</u>
Customer Information .....	1
1a. Awarded Special Item Numbers .....	1
1b. N/A.....	1
1c. See Accepted Pricelist.....	1
2. Maximum Order Guidelines .....	1
3. Minimum Order Limitation .....	1
4. Geographic Coverage (Delivery Area) .....	1
5. Point(s) of Production (City, County, and State or Foreign Country) .....	1
6. Discount from List prices or Statement of Net Price .....	1
7. Quantity Discounts.....	1
8. Prompt Payment Terms.....	2
9. Foreign Items .....	2
10a. Time of Delivery .....	2
10b. Expedited Delivery. “Items Available for Expedited Delivery are Noted in this Price List:” .....	2
10c. Overnight and 2-Day Delivery.....	2
10d. Urgent Requirements .....	2
11. F.O.B. Point(s) .....	2
12a. Ordering Address(es) .....	2
12b. Ordering Procedures .....	2
13. Payment Address(es) .....	3
14. Warranty Provision .....	3
15. Export Packing Charges.....	3
16. Terms and Conditions of Rental, Maintenance, and Repair .....	3
17. Terms and Conditions of Installation.....	3
18a. Terms and Conditions of Repair Parts Indicating Date of Parts Price Lists and Any Discounts from List Prices .....	3
18b. Terms and Conditions for Any Other Services.....	3
19. List of Service and Distribution Points.....	3
20. List of Participating Dealers .....	3
21. Preventive Maintenance.....	3

**TABLE OF CONTENTS (continued)**

	<u>Page</u>
22a. Special Attributes Such as Environmental Attributes (e.g., Recycled Content, Energy Efficiency, and/or Reduced Pollutants .....	4
22b. If Applicable, Indicate That Section 508 Compliance Information is Available on Electronic and Information Technology (EIT) Supplies and Services and Show Where full Details Can be Found (e.g., Contractor’s Website or Other Location.) The EIT Standards Can be Found at: <a href="http://www.Section508.gov/">www.Section508.gov/</a> .....	4
23. Data Universal Number System (DUNS) Number .....	4
24. Notification Regarding Registration in System for Award Management (SAM) Database .....	4
ARTI Multiple Award Schedule LABOR CATEGORY PRICE LIST .....	5
ARTI Multiple Award Schedule LABOR CATEGORY DESCRIPTIONS .....	7

---

## CUSTOMER INFORMATION

**1a. AWARDED SPECIAL ITEM NUMBERS:**

334512 – Total Solution Support Products for Facilities Management Systems  
OLM – Order Level Material (OLM)

**1b. N/A**

**1c. SEE ACCEPTED PRICELIST**

**2. MAXIMUM ORDER GUIDELINES:**

334512 – \$250,000 PER SIN/PER ORDER

“Notwithstanding paragraph (b) above, the (ARTI) Contractor shall honor any order exceeding the maximum orders in paragraph (b), unless that order (or orders) is returned to the ordering office within five (5) workdays after receipt, with written notice stating the Contractor’s intent not to ship the item (or items) called for and the reasons. Upon receiving this notice, the Government may acquire the supplies or services from another source.”

Ordering activities may request a price reduction at any time before placing an order, establishing a BPA, or in conjunction with the annual BPA review. However, the ordering activity shall seek a price reduction when the order or BPA exceeds the simplified acquisition threshold. Schedule contractors are not required to pass on to all schedule users a price reduction extended only to an individual ordering activity for a specific order or BPA.

OLM – \$100,000 OLM PER SIN/PER ORDER [Not To Exceed 33.33% of Total Order]

**3. MINIMUM ORDER LIMITATION:**

\$100.00

**4. GEOGRAPHIC COVERAGE (DELIVERY AREA):**

The 50 United States, and Washington, DC, Puerto Rico, and US Territories

**5. POINT(S) OF PRODUCTION (CITY, COUNTY, AND STATE OR FOREIGN COUNTRY):**

N/A

Services under this Schedule/Price List are available at any client location within the geographic scope on a TDY or permanent basis.

**6. DISCOUNT FROM LIST PRICES OR STATEMENT OF NET PRICE:**

All Federal Contracts

**7. QUANTITY DISCOUNTS:** Additional 2% for orders > \$2M annually

**8. PROMPT PAYMENT TERMS:** 0. 5% 20 Net 30 – Prompt payment terms cannot be negotiated out of the contractual agreement in exchange for other concessions.

**9. FOREIGN ITEMS:**

None

**10a. TIME OF DELIVERY:**

Delivery Schedule specified by Task Order. Generally, 30 Days ARO, and/or GS-FSS-920, Ordering Procedures for the Services.

**10b. EXPEDITED DELIVERY. “ITEMS AVAILABLE FOR EXPEDITED DELIVERY ARE NOTED IN THIS PRICE LIST:”**

N/A

**10c. OVERNIGHT AND 2-DAY DELIVERY:**

Schedule customer may contact the Contractor for rates for overnight and 2-day delivery.

**10d. URGENT REQUIREMENTS:**

“Urgent Requirements” clause of its contract I FSS-140-B and advise Agencies can contact the Contractor’s representative to affect a faster delivery.

**11. F.O.B. POINT(S):**

Destination

**12a. ORDERING ADDRESS(ES)**

1555 King Street, Suite 200  
Alexandria, VA 22314

**12b. ORDERING PROCEDURES:**

For supplies and services, the ordering procedures, information on Blanket Purchase Agreements (BPAs), and a sample BPA can be found at the GSA/FSS Schedule homepage ([fss.gsa.gov/schedules](http://fss.gsa.gov/schedules)).

**13. PAYMENT ADDRESS(ES):**

RCA Funding, LLC  
c/o Republic Capital Access, LLC  
2411 Dulles Corner Parkway; Suite 635  
Herndon, VA 20171

**14. WARRANTY PROVISION:**

Reference GS-FSS-920, Ordering Procedures for Services

**15. EXPORT PACKING CHARGES:**

N/A

**16. TERMS AND CONDITIONS OF RENTAL, MAINTENANCE, AND REPAIR**

N/A

**17. TERMS AND CONDITIONS OF INSTALLATION:**

N/A

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

N/A

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

N/A

**19. LIST OF SERVICE AND DISTRIBUTION POINTS:**

N/A

**20. LIST OF PARTICIPATING DEALERS:**

N/A

**21. PREVENTIVE MAINTENANCE:**

N/A

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

N/A

**22b. IF APPLICABLE, INDICATE THAT SECTION 508 COMPLIANCE INFORMATION IS AVAILABLE ON ELECTRONIC AND INFORMATION TECHNOLOGY (EIT) SUPPLIES AND SERVICES AND SHOW WHERE FULL DETAILS CAN BE FOUND (E.G., CONTRACTOR'S WEBSITE OR OTHER LOCATION.) THE EIT STANDARDS CAN BE FOUND AT [www.Section508.gov/](http://www.Section508.gov/):**

Currently not applicable, compliance with EIT Standards on a Task Order basis as required.

**23. DATA UNIVERSAL NUMBER SYSTEM (DUNS) NUMBER:**

36-068-5051

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

**MULTIPLE AWARD SCHEDULE LABOR CATEGORY PRICE LIST**

<b>Contract Line Item Number</b>	<b>Commercial Job Title</b>	<b>Government Site Rate</b>
1	Security Subject Matter Expert	\$105.47
2	Sr. Security Subject Matter Expert	\$126.11
3	Principle Security Subject Matter Expert	\$159.79
4	Forensic Computer Lab Manager	\$129.13
5	Computer Forensics Analyst I	\$84.23
6	Computer Forensics Analyst II	\$95.45
7	Computer Forensics Analyst III	\$112.29
8	Computer Forensics Analyst IV	\$121.27
9	Computer Forensics Technician I	\$58.39
10	Computer Forensics Technician II	\$72.98
11	Computer Forensics Technician III	\$89.83
12	Computer Forensics Technician IV	\$101.05
13	Budget Liaison Officer I	\$82.80
14	Budget Liaison Officer II	\$92.28
15	Budget Liaison Officer III	\$101.96
16	Security EMT Instructor I	\$47.61
17	Security EMT Instructor II	\$61.21
18	Security EMT Instructor III	\$72.73
19	IT Security Specialist I	\$79.74
20	IT Security Specialist II	\$91.43
21	IT Security Specialist III	\$103.36
22	IT Security Specialist IV	\$117.08
23	IT Security Specialist V	\$156.89
24	Logistics Coordinator I	\$49.65
25	Logistics Coordinator II	\$72.35
26	Logistics Coordinator III	\$88.50
27	Security Manager I	\$58.56
28	Security Manager II	\$68.30
29	Security Manager III	\$78.98
30	Security Manager IV	\$95.70
31	Security Manager V	\$103.21
32	Security Admin I	\$29.55
33	Security Admin II	\$38.93
34	Security Admin III	\$46.66
35	Security Admin IV	\$50.99



<b>Contract Line Item Number</b>	<b>Commercial Job Title</b>	<b>Government Site Rate</b>
36	Security Specialist I	\$55.90
37	Security Specialist II	\$62.14
38	Security Specialist III	\$63.26
39	Security Specialist IV	\$70.06
40	Security Specialist V	\$80.85
41	Sr. Tech Sec Spec I	\$83.20
42	Sr. Tech Sec Spec II	\$84.45
43	Sr. Tech Sec Spec III	\$95.34
44	Sr. Tech Sec Spec IV	\$108.04
45	Counterintelligence Specialist II	\$109.00

**ADVANCED RESOURCE TECHNOLOGIES, INC. (ARTI)  
 MULTIPLE AWARD SCHEDULE  
 LABOR CATEGORY DESCRIPTIONS**

If required, all labor categories will be subject to a Government Security Investigation and must meet eligibility for access to classified information at the appropriate clearance level at the date of hire as prescribed by the individual contract statement of work.

<b>1. SECURITY SUBJECT MATTER EXPERT</b>
<p><b>Minimum/General Experience:</b> Experience with subversive organizations and their methods of operation. Experience with national and international security practices. Experience with information security practices required to establish and maintain system integrity for safeguarding classified information in a secure environment. Experience includes achieving recognized standing in a related professional field through outstanding contribution and the ability to plan, conduct, and direct research and/or development work on complex projects necessitating the origination and application of new and unique approaches in relation to the security nature of the project.</p>
<p><b>Functional Responsibility:</b> Provide consulting services in accordance with or directly related to the security environment to members of management, the professional staff, and to the customer. Plan and initiate studies for original or advanced areas of customer problems and determines the techniques or methods involved that will accomplish the objectives. Develop and analyze analytical data, techniques and methodology for the solution of highly complex problems. Review reports and other products intended for release to the public/customers to ensure that technical merit and style of presentation reflect the highest quality. Act in advisory capacity for the approach utilized in performing security tasks of unusual difficulty or complexity, frequently involving customer relationships; plan principles and procedures for accomplishing customer studies and gives expert professional analysis of methods and objectives.</p>
<p><b>Minimum Education:</b> Graduate degree in a related scientific field preferred. 10 years of professional experience in security-related field (e.g., counterintelligence, investigations, industrial security, dignitary/VIP policy and security standard development, technical security, security countermeasures programs, access systems operation and management, personnel protection and protecting/security information, or region desk officer). With 14 years of specialized experience a degree is not required. One year of college is equivalent to one year of experience. Any related industry certification can be substituted for one year of experience.</p>

**2. SR. SECURITY SUBJECT MATTER EXPERT**

**Minimum/General Experience:** Experience with subversive organizations and their methods of operation. Experience with national and international security practices. Experience with information security practices required to establish and maintain system integrity for safeguarding classified information in a secure environment. Experience includes achieving recognized standing in a related professional field through outstanding contribution and the ability to plan, conduct, and direct research and/or development work on complex projects necessitating the origination and application of new and unique approaches in relation to the security nature of the project.

**Functional Responsibility:** Provide consulting services in accordance with or directly related to the security environment to members of management, the professional staff, and to the customer. Plan and initiate studies for original or advanced areas of customer problems and determines the techniques or methods involved that will accomplish the objectives. Develop and analyze analytical data, techniques and methodology for the solution of highly complex problems. Review reports and other products intended for release to the public/customers to ensure that technical merit and style of presentation reflect the highest quality. Act in advisory capacity for the approach utilized in performing security tasks of unusual difficulty or complexity, frequently involving customer relationships; plan principles and procedures for accomplishing customer studies and gives expert professional analysis of methods and objectives.

**Minimum Education:** Graduate degree in a related scientific field preferred. 15 years of professional experience in security-related field (e.g., counterintelligence, investigations, industrial security, dignitary/VIP policy and security standard development, technical security, security countermeasures programs, access systems operation and management, personnel protection and protecting/security information, or region desk officer). With 19 years of specialized experience a degree is not required. One year of college is equivalent to one year of experience. Any related industry certification can be substituted for one year of experience.

**3. PRINCIPLE SECURITY SUBJECT MATTER EXPERT**

**Minimum/General Experience:** Experience with subversive organizations and their methods of operation. Experience with national and international security practices. Experience with information security practices required to establish and maintain system integrity for safeguarding classified information in a secure environment. Experience includes achieving recognized standing in a related professional field through outstanding contribution and the ability to plan, conduct, and direct research and/or development work on complex projects necessitating the origination and application of new and unique approaches in relation to the security nature of the project.

**Functional Responsibility:** Provide consulting services in accordance with or directly related to the security environment to members of management, the professional staff, and to the customer. Plan and initiate studies for original or advanced areas of customer problems and determines the techniques or methods involved that will accomplish the objectives. Develop and analyze analytical data, techniques and methodology for the solution of highly complex problems. Review reports and other products intended for release to the public/customers to ensure that technical merit and style of presentation reflect the highest quality. Act in advisory capacity for the approach utilized in performing security tasks of unusual difficulty or complexity, frequently involving customer relationships; plan principles and procedures for accomplishing customer studies and gives expert professional analysis of methods and objectives.

**Minimum Education:** Graduate degree in a related scientific field preferred. 17 years of professional experience and is an acknowledged expert in a security-related field (e.g., counterintelligence, investigations, industrial security, dignitary/VIP policy and security standard development, technical security, security countermeasures programs, access systems operation and management, personnel protection and protecting/security information, or region desk officer). Published papers and applicable industry certification desired. With 21 years of specialized experience a degree is not required. One year of college is equivalent to one year of experience. Any related industry certification can be substituted for one year of experience.

<b>4. FORENSIC COMPUTER LAB MANAGER</b>
<p><b>Minimum/General Experience:</b> Provide overall management of an agency’s computer forensics laboratory and staff to include technical, administrative and professional support in accomplishing the statement of work requirements.</p>
<p><b>Functional Responsibility:</b> Manage computer forensic investigations for the lab. Must have the ability to understand the principles and technology related to forensic science; oversee the management and comprehensive operation of a modern forensic laboratory; analyze, research and evaluate new service delivery methods and techniques; make sound administrative, technological and personnel decisions; communicate effectively both orally and written; understand the budget impact and make adjustments on budgetary issues; coordinate and develop working relationships with other agencies and within the agency, and comprehend the entire crime lab operations and keep the branch Deputy Chief informed and updated on issues regarding the forensic lab. Manage, direct, supervise and coordinate all activities within the forensic laboratory which include: oversee lab testing and analysis; ensure that non-routine problems are resolved; provide guidance in the collection and analysis of evidence; testify in legal proceedings; insure that staffing, equipment and other lab resources are maximally utilized for efficient and effective laboratory operation; and maintain current awareness involving forensic analytical technology procedures and legal decisions involving computer forensic science.</p>
<p><b>Minimum Education:</b> Undergraduate degree with 10 years of specialized experience in the field of computer investigations and forensics support services. Must include 7 years’ experience managing/supervising computer investigations and computer forensics services. With 14 years of specialized experience a degree is not required. Expert experience providing computer forensic investigations on multiple hardware types and working experience with computer forensic software, such as EnCase, FTK, Ghost, etc. Experience in supervision and/or program management. Experience with network architectures and security is desired. Expert knowledge of data structures (FAT, FAT32, NTFS, UNIX, etc.) Must be well organized and possess excellent phone, interpersonal, customer service, communication, and documentation skills. A background in civil/criminal investigations and/or electronic evidence is desirable. Experience testifying in civil, criminal, or administrative proceedings is required. Travel required.</p>

<b>5. COMPUTER FORENSICS ANALYST I</b>
<p><b>Minimum/General Experience:</b> Conduct computer forensic analysis of subject media and/or analysis of networks, intrusions, or e-mail systems.</p>
<p><b>Functional Responsibility:</b> Must have the ability to understand the principles and technology related to forensic science; assist with evidence preservation processes; perform data analysis, investigator interaction, report generation, and expert witness services. Will conduct analysis in conjunction with senior level analysts. Generally, analysts will: Conduct examinations of computers and media generated by computers to develop evidence as an expert in the specialty area of forensic computer science. Use experience and knowledge of a wide variety of advanced computer technologies and theories to conduct analysis of submitted evidence. Review laboratory requests and determines the type of examination needed. In data recovery cases, determines the most appropriate method of protecting original evidence and recovering deleted, erased, hidden and encrypted data. Identifies and recommends methods and procedures for preservation, evidence recovery, and presentation of computer evidence. Perform related duties as required by management to meet the needs of the branch.</p>
<p><b>Minimum Education:</b> Undergraduate degree or 2 years of experience as a forensic examiner with related experience and training; or equivalent combination of education and experience substituting 1 year of additional experience equivalent to 1 year of education.</p>

<b>6. COMPUTER FORENSICS ANALYST II</b>
<b>Minimum/General Experience:</b> Conduct computer forensic analysis of subject media and/or analysis of networks, intrusions, or e-mail systems.
<b>Functional Responsibility:</b> Must have the ability to understand the principles and technology related to forensic science; assist with evidence preservation processes; perform data analysis, investigator interaction, report generation, and expert witness services. Will conduct analysis in conjunction with senior level analysts. Generally, analysts will: Conduct examinations of computers and media generated by computers to develop evidence as an expert in the specialty area of forensic computer science. Use experience and knowledge of a wide variety of advanced computer technologies and theories to conduct analysis of submitted evidence. Review laboratory requests and determines the type of examination needed. In data recovery cases, determines the most appropriate method of protecting original evidence and recovering deleted, erased, hidden and encrypted data. Identifies and recommends methods and procedures for preservation, evidence recovery, and presentation of computer evidence. Perform related duties as required by management to meet the needs of the branch.
<b>Minimum Education:</b> Undergraduate degree or 4 years of experience as a forensic examiner with related experience and training; or equivalent combination of education and experience substituting 1 year of additional experience equivalent to 1 year of education.

<b>7. COMPUTER FORENSICS ANALYST III</b>
<b>Minimum/General Experience:</b> Conduct computer forensic analysis of subject media and/or analysis of networks, intrusions, or e-mail systems.
<b>Functional Responsibility:</b> Must have the ability to understand the principles and technology related to forensic science; assist with evidence preservation processes; perform data analysis, investigator interaction, report generation, and expert witness services. Analysts will conduct independent analysis and/or oversee junior level analyst's work. Generally, analysts will: Conduct examinations of computers and media generated by computers to develop evidence as an expert in the specialty area of forensic computer science. Use experience and knowledge of a wide variety of advanced computer technologies and theories to conduct analysis of submitted evidence. Review laboratory requests and determines the type of examination needed. In data recovery cases, determines the most appropriate method of protecting original evidence and recovering deleted, erased, hidden and encrypted data. Identifies and recommends methods and procedures for preservation, evidence recovery, and presentation of computer evidence. Perform related duties as required by management to meet the needs of the branch.
<b>Minimum Education:</b> Undergraduate degree <u>and</u> 6 years of experience as a forensic examiner with related experience and training; or equivalent combination of education/experience substituting 1 year of additional experience equivalent to 1 year of education.

<b>8. COMPUTER FORENSICS ANALYST IV</b>
<b>Minimum/General Experience:</b> Conduct computer forensic analysis of subject media and/or analysis of networks, intrusions, or e-mail systems.
<b>Functional Responsibility:</b> Must have the ability to understand the principles and technology related to forensic science; assist with evidence preservation processes; perform data analysis, investigator interaction, report generation, and expert witness services. Analysts will conduct independent analysis and/or oversee junior level analyst’s work. Generally, analysts will: Conduct examinations of computers and media generated by computers to develop evidence as an expert in the specialty area of forensic computer science. Use experience and knowledge of a wide variety of advanced computer technologies and theories to conduct analysis of submitted evidence. Review laboratory requests and determines the type of examination needed. In data recovery cases, determines the most appropriate method of protecting original evidence and recovering deleted, erased, hidden and encrypted data. Identifies and recommends methods and procedures for preservation, evidence recovery, and presentation of computer evidence. Perform related duties as required by management to meet the needs of the branch.
The section lead directs the analytical efforts of a team of highly trained forensic computer analysts. Serving as the focal point for the section, the lead analyst develop training requirements, provide for quality assurance of work product, and ensures process integrity. Additionally, the section lead will provide primary liaison with other agency analysts as required.
<b>Minimum Education:</b> Undergraduate degree <u>and</u> 8 years of experience as a forensic examiner with related experience and training; or equivalent combination of education and experience substituting 1 year of additional experience equivalent to 1 year of education.

<b>9. COMPUTER FORENSICS TECHNICIAN I</b>
<b>Minimum/General Experience:</b> The primary functions include network maintenance/oversight, hardware/software support, evidence custodianship, analyst support, and general administrative functions.
<b>Functional Responsibility:</b> Work within a lab environment to support analysts and investigators. Technician positions are responsible for one or more specialty assignments – Network Engineer, System Administration, Evidence Technician, and Administrative support. Will normally perform the administrative and evidence custodial duties. All levels must be capable of working in a scientific environment with exacting standards; able to handle the initial processing of electronic evidence; and proficient in one or more of the forensic utilities used within the lab.
<b>Minimum Education:</b> Undergraduate degree or 2 years of related experience; or equivalent combination of education and experience substituting 1 year of additional experience equivalent to 1 year of education.

<b>10. COMPUTER FORENSICS TECHNICIAN II</b>
<b>Minimum/General Experience:</b> The primary functions include network maintenance/oversight, hardware/software support, evidence custodianship, analyst support, and general administrative functions.
<b>Functional Responsibility:</b> Work within a lab environment to support analysts and investigators. Technician positions are responsible for one or more specialty assignments – Network Engineer, System Administration, Evidence Technician, and Administrative support. Will normally perform the administrative and evidence custodial duties. All levels must be capable of working in a scientific environment with exacting standards; able to handle the initial processing of electronic evidence; and proficient in one or more of the forensic utilities used within the lab.
<b>Minimum Education:</b> Undergraduate degree or 4 years of related experience and training; or equivalent combination of education and experience substituting 1 year of additional experience equivalent to 1 year of education.

<b>11. COMPUTER FORENSICS TECHNICIAN III</b>
<b>Minimum/General Experience:</b> The primary functions include network maintenance/oversight, hardware/software support, evidence custodianship, analyst support, and general administrative functions.
<b>Functional Responsibility:</b> Work within a lab environment to support analysts and investigators. Technician positions are responsible for one or more specialty assignments – Network Engineer, System Administration, Evidence Technician, and Administrative support. Will primarily be responsible for network management and hardware/software maintenance. All levels must be capable of working in a scientific environment with exacting standards; able to handle the initial processing of electronic evidence; and proficient in one or more of the forensic utilities used within the lab.
<b>Minimum Education:</b> Undergraduate degree <u>and</u> 6 years of related experience and training; or equivalent combination of education/experience substituting 1 year of additional experience equivalent to 1 year of education.

<b>12. COMPUTER FORENSICS TECHNICIAN IV</b>
<b>Minimum/General Experience:</b> The primary functions include network maintenance/oversight, hardware/software support, evidence custodianship, analyst support, and general administrative functions.
<b>Functional Responsibility:</b> Work within a lab environment to support analysts and investigators. Technician positions are responsible for one or more specialty assignments – Network Engineer, System Administration, Evidence Technician, and Administrative support. Will primarily be responsible for network management and hardware/software maintenance. All levels must be capable of working in a scientific environment with exacting standards; able to handle the initial processing of electronic evidence; and proficient in one or more of the forensic utilities used within the lab.
The section lead directs the analytical efforts of a team of highly trained forensic computer technicians. Serving as the focal point for the section, the lead technician develop training requirements, provide for quality assurance of work product, and ensures process integrity. Additionally, the section lead will provide primary liaison with other agency analysts as required.
<b>Minimum Education:</b> Undergraduate degree <u>and</u> 8 years of related experience and training; or equivalent combination of education and experience substituting 1 year of additional experience equivalent to 1 year of education.



<b>13. BUDGET LIAISON OFFICER I</b>
<p><b>Minimum/General Experience:</b> Assist with tracking project budget with the responsibilities for justifying, obtaining, managing and tracking expenses related to the budgets for the division. Track financial operations in support of procurements, travel and project funding issues. Program areas include division's base funds for training and travel for programs, special projects, vehicles, computers, and/or other equipment, and contract staff.</p>
<p><b>Functional Responsibility:</b> Review expenditures and prepare operating budgets for department managers to ensure conformance to budgetary limits and provide discrepancies to manager. Assist with the annual budget process and report and analyze operational expenses for each program area. Prepare department operating budget reports as needed. Assist with monitoring the budget data against plans, forecasts, and budgets tracking burn rates of allocated funds and report the status to the appropriate manager. Follows the established operating procedures and reporting instructions.</p>
<p><b>Minimum Education:</b> Undergraduate degree in Accounting, Finance, or Business Administration with 4 years of specialized experience in the areas of auditing, budgeting, or financial management required. With 8 years of specialized experience a degree is not required. One year of college is equivalent to one year of experience. Any related industry certification can be substituted for one year of experience. Thorough knowledge of accounting theories, practices, regulations, and financial concepts relative to profitability and financial ratios. Knowledgeable of U. S. Government fiscal and budget policies and procedures.</p>

<b>14. BUDGET LIAISON OFFICER II</b>
<p><b>Minimum/General Experience:</b> Assist with tracking project budget with the responsibilities for justifying, obtaining, managing and tracking expenses related to the budgets for the division. Track financial operations in support of procurements, travel and project funding issues.</p>
<p><b>Functional Responsibility:</b> Review, analyze, and interpret financial data. Review expenditures and prepare operating budgets for department managers to ensure conformance to budgetary limits and provide discrepancies to manager. Examine and track the budget estimates or proposals for completeness, accuracy, and conformance with established procedures, regulations, and organizational objectives. Assist with cost-benefit analysis to review financial requests, assess program trade-offs, and examine past budget activities. Assist with the annual budget process and report and analyze operational expenses for each program area. Prepare department operating budget reports and perform analyses of related data as needed. Prepare detailed reports and presentations for manager. Assist with monitoring the budget data against plans, forecasts, and budgets tracking burn rates of allocated funds and report the status to the appropriate manager. Follows the established operating procedures and reporting instructions.</p>
<p><b>Minimum Education:</b> Undergraduate degree in Accounting, Finance, or Business Administration with 6 years of specialized experience in the areas of auditing, budgeting, or financial management required. With 10 years of specialized experience a degree is not required. One year of college is equivalent to one year of experience. Any related industry certification can be substituted for one year of experience. Experience with accounting theories, practices, regulations, and financial concepts relative to profitability and financial ratios. Knowledgeable of U. S. Government fiscal and budget policies and procedures.</p>

<b>15. BUDGET LIAISON OFFICER III</b>
<p><b>Minimum/General Experience:</b> Manage and track project budget with the responsibilities for justifying, obtaining, managing and tracking expenses related to the budgets for the division. Track financial operations in support of procurements, travel and project funding issues. Program areas include division’s base funds for training and travel for programs, special projects, vehicles, computers, and/or other equipment, and contract staff. Provide justification for new budget items, regular reporting of current budget to include status explanations, end of the year closeout reports, and audit reporting details.</p>
<p><b>Functional Responsibility:</b> Supervise subordinate Budget Analyst staff. Review, analyze, and interpret financial data. Review expenditures and prepare operating budgets for department managers to ensure conformance to budgetary limits and provide discrepancies to manager. Examine and track the budget estimates or proposals for completeness, accuracy, and conformance with established procedures, regulations, and organizational objectives. Perform cost-benefit analysis to review financial requests, assess program trade-offs, and examine past budget activities. Manage the annual budget process, and report and analyze operational expenses for each program area. Prepare department operating budget reports and perform analyses of related data as needed. Prepare detailed reports and makes presentations to senior management. Monitor the budget data against plans, forecasts, and budgets tracking burn rates of allocated funds and report the status to the appropriate manager. Update and train staff on the established operating procedures and reporting instructions.</p>
<p><b>Minimum Education:</b> Graduate degree in Accounting, Finance, or Business Administration with 6 years or Undergraduate degree with 8 years of specialized experience in the areas of auditing, budgeting, or financial management required. With 12 years of specialized experience a degree is not required. One year of college is equivalent to one year of experience. Any related industry certification can be substituted for one year of experience. Advanced experience of accounting theories, practices, regulations, and financial concepts relative to profitability and financial ratios. Experienced with U. S. Government fiscal and budget policies and procedures.</p>

<b>16. SECURITY EMT INSTRUCTOR I</b>
<p><b>Minimum/General Experience:</b> Develop and present EMT related training to medical and non-medical personnel in a formal classroom setting.</p>
<p><b>Functional Responsibility:</b> Develop and prepare course outlines, training aids, and classroom materials for the Program Office and other related training as designated by the Contracting Officer's Representative (COR). Present training in a formal classroom environment to a diverse audience. Class duration may vary from three to fifteen days in duration. As appropriate, work with local military and related agencies in coordinating the training, logistics, and any equipment needed. Review department policies, procedures and manuals provide update information as requested.</p>
<p><b>Minimum Education:</b> A minimum of 5 years’ experience in providing training to related medical or security professionals in a formal classroom setting. One year of college is equivalent to one year of experience. Any related industry certification can be substituted for one year of experience. As applicable must possess current industry certification for the training subject matter.</p>

<b>17. SECURITY EMT INSTRUCTOR II</b>
<b>Minimum/General Experience:</b> Develop and present EMT related training to medical and non-medical personnel in a formal classroom setting and in overseas field offices.
<b>Functional Responsibility:</b> Develop and prepare course outlines, training aids, and classroom materials for the Program Office and other related training as designated by the Contracting Officer's Representative (COR Present courses of emergency medical training to classes composed of Regional Security Officers, New Agents, Couriers, SEABEES, Construction Security Guards, Security Engineering Officers, Embassy/Mission Personnel, and designated Foreign Services Institute groups. Class duration may vary from three to fifteen days in duration. As appropriate, work with local military and related agencies in coordinating the training, logistics and any equipment needed. Provide medical or security support for training missions. Review and update department policies, procedures, and manuals to ensure they meet current medical standards and practices.
<b>Minimum Education:</b> A minimum of 8 years' experience in providing training to both related medical or security professionals. One year of college is equivalent to one year of experience. Any related industry certification can be substituted for one year of experience. Must have experience training and evaluating other instructors. Combat experience a plus. As applicable, must possess current industry certifications for the training subject matter.

<b>18. SECURITY EMT INSTRUCTOR III</b>
<b>Minimum/General Experience:</b> Develop and present EMT related training to medical and non-medical personnel in a formal classroom setting and in overseas field offices.
<b>Functional Responsibility:</b> Supervise and coordinate all activities within the training facility. Develop and prepare course outlines, training aids, and classroom materials for the Program Office and other related training as designated by the Contracting Officer's Representative (COR). Present training in a classroom setting to a diverse audience Class duration may vary from three to 15 days in duration. As appropriate, work with local military and related agencies in coordinating the training, logistics and any equipment needed. Provide medical or security support for training missions. Review and update department policies, procedures, and manuals to ensure they meet current medical standards and practices.
<b>Minimum Education:</b> A minimum of 10 years' experience in providing training to related medical or security professionals in a classroom setting. One year of college is equivalent to one year of experience. Any related industry certification can be substituted for one year of experience. Experience must include 2 years supervising subordinate instructors. Must have experience training and evaluating other instructors. Combat experience a plus. As applicable, must possess current industry certifications for the training subject matter.

<b>19. IT SECURITY SPECIALIST I</b>
<p><b>Minimum/General Experience:</b> In support of an IT Security Program will assist in the development, coordination and documenting plans, procedures, and architecture to include Certification &amp; Accreditation of systems, and NIST self-assessments. Assist in the development, promulgation, and review of security and policy elements for the IT Security Program.</p>
<p><b>Functional Responsibility:</b> Assist in the development and administration of the entity-wide Security Plan using the existing documentation, and industry standards and federal government legislation. Develop and maintain the entity-wide Concept of Operation Plan (COOP) update for critical operations. Update and maintain organizational Certification and Accreditation documentation. Develop government security policy documentation. Develop and maintain Systems and Infrastructure Security Plan. Assist with the development and maintenance of the IT Security Architecture Plan.</p>
<p><b>Minimum Education:</b> Undergraduate degree in related field and 5 years specialized experience. With 9 years of specialized experience a degree is not required. One year of college is equivalent to one year of experience. Any related industry certification can be substituted for one year of experience. Understanding of computer security requirements and practices in the civilian sector of the federal government. Must have in depth knowledge consistent with security principles and best practices as reflected in the NIST-800-18, OMB A-130, and NIST-800-26 and other applicable Federal regulations and guidelines. Must have knowledge of FISMA.</p>

<b>20. IT SECURITY SPECIALIST II</b>
<p><b>Minimum/General Experience:</b> In support of the IT Security Program will perform tasks to develop, coordinate and document plans, procedures, and architecture to include Certification &amp; Accreditation of systems, and NIST self-assessments. Develop, promulgate, and review security and policy elements of the IT Security Program.</p>
<p><b>Functional Responsibility:</b> Develop, analyze, and administer the entity-wide Security Plan using the existing documentation, and industry standards and federal government legislation. Develop, and analyze IT security models, and maintain methodology to track Security Plans for each sensitive/critical major application and general support system within the organization. Develop, analyze, and maintain the entity-wide Concept of Operation Plan (COOP) update for critical operations. Conduct and write Certification &amp; Accreditation of systems. Conduct NIST self-assessments. Design, implement, document, and evaluate government computer security programs. Develop government security policy documentation. Develop and maintain Systems and Infrastructure Security Plan. Develop and maintain IT Security Architecture Plan. Develop and evaluate plans, principles, and procedures for accomplishing customer IT security studies and provide professional analysis of methods and objectives.</p>
<p><b>Minimum Education:</b> Undergraduate degree in related field and 7 years specialized experience. With 11 years of specialized experience a degree is not required. One year of college is equivalent to one year of experience. Any related industry certification can be substituted for one year of experience. CISSP or related industry certification desired. Thorough understanding of computer security requirements and practices in the civilian sector of the federal government. Must have experience in conducting and writing Certification &amp; Accreditation of systems. Must have experience conducting NIST self-assessments. Must have demonstrated experience and/or in depth knowledge consistent with security principles and best practices as reflected in the NIST-800-18, OMB A-130, and NIST-800-26 and other applicable Federal regulations and guidelines. Must have knowledge of FISMA.</p>

**21. IT SECURITY SPECIALIST III**

**Minimum/General Experience:** In support of the IT Security Program will perform tasks to develop, coordinate and document plans, procedures, and architecture to include Certification & Accreditation of systems, and NIST self-assessments. Develop, promulgate, and review security and policy elements of the IT Security Program.

**Functional Responsibility:** Develop, analyze, and administer the entity-wide Security Plan using the existing documentation, and industry standards and federal government legislation. Develop and analyze IT security models and maintain methodology to track Security Plans for each sensitive/critical major application and general support system within the organization. Develop, analyze, and maintain the entity-wide Concept of Operation Plan (COOP) update for critical operations. Conduct and write Certification & Accreditation of systems. Conduct NIST self-assessments. Design, implement, document, and evaluate government computer security programs. Develop government security policy documentation. Develop and maintain Systems and Infrastructure Security Plan. Develop and maintain IT Security Architecture Plan. Develop and evaluate plans, principles, and procedures for accomplishing customer IT security studies and provide professional analysis of methods and objectives.

**Minimum Education:** Undergraduate degree in related field and 9 years specialized experience. With 13 years of specialized experience a degree is not required. One year of college is equivalent to one year of experience. Any related industry certification can be substituted for one year of experience. CISSP or related industry certification desired. Thorough understanding of computer security requirements and practices in the civilian sector of the federal government. Must have experience in conducting and writing Certification & Accreditation of systems. Must have experience conducting NIST self-assessments. Must have demonstrated experience and/or in depth knowledge consistent with security principles and best practices as reflected in the NIST-800-18, OMB A-130, and NIST-800-26 and other applicable Federal regulations and guidelines. Experience with designing, implementing, documenting, and evaluating government computer security programs. Experience with writing government computer security policy documentation.

Thorough understanding of and hands-on experience with computer operations and systems of various types as well as an understanding of computer security.

**22. IT SECURITY SPECIALIST IV**

**Minimum/General Experience:** In support of the IT Security Program will perform tasks to develop, coordinate and document plans, procedures and architecture for the Security and Policy Program office to include Certification & Accreditation of systems, and NIST self-assessments. Develop, promulgate, and review security and policy elements of the IT Security Program.

**Functional Responsibility:** Develop, analyze, and administer the entity-wide Security Plan using the existing documentation, and industry standards and federal government legislation. Develop, and analyze IT security models, and maintain methodology to track Security Plans for each sensitive/critical major application and general support system within the organization. Develop, analyze, and maintain the entity-wide Concept of Operation Plan (COOP) update for critical operations. Conduct and write Certification & Accreditation of systems. Conduct NIST self-assessments. Design, implement, document, and evaluate government computer security programs. Develop government security policy documentation. Develop and maintain Systems and Infrastructure Security Plan. Develop and maintain IT Security Architecture Plan. Conduct technical briefings to senior level government officials. Develop and evaluate plans, principles, and procedures for accomplishing customer IT security studies and provide professional analysis of methods and objectives. May supervise IT Security team.

**Minimum Education:** Undergraduate degree in related field and 11 years specialized experience. With 15 years of specialized experience a degree is not required. One year of college is equivalent to one year of experience. Any related industry certification can be substituted for one year of experience. CISSP or related industry certification desired. Subject matter expert of computer security requirements and practices in the civilian sector of the federal government. Must have experience in conducting and writing Certification & Accreditation of systems. Must have experience conducting NIST self-assessments. Must have demonstrated experience and/or in depth knowledge consistent with security principles and best practices as reflected in the NIST-800-18, OMB A-130, and NIST-800-26 and other applicable Federal regulations and guidelines. Experience with designing, implementing, documenting, and evaluating government computer security programs. Experience with writing government computer security policy documentation.

Experience with designing, implementing, documenting, and evaluating government computer security programs. Thorough understanding of and hands-on experience with computer operations and systems of various types as well as an understanding of computer security.

**23. IT SECURITY SPECIALIST V**

**Minimum/General Experience:** In support of the IT Security Program will perform tasks to develop, coordinate and document plans, procedures, and architecture to include Certification & Accreditation of systems, and NIST self-assessments. Develop, promulgate, and review security and policy elements of the IT Security Program.

**Functional Responsibility:** Develop, analyze, and administer the entity-wide Security Plan using the existing documentation, and industry standards and federal government legislation. Develop, and analyze IT security models, and maintain methodology to track Security Plans for each sensitive/critical major application and general support system within the organization. Develop, analyze, and maintain the entity-wide Concept of Operation Plan (COOP) update for critical operations. Evaluate and analyze the critical technology processing needs of the related services. Develop, analyze, and maintain Personnel Suitability Procedures for access and operate sensitive government computer systems. Conduct and write Certification & Accreditation of systems. Conduct NIST self-assessments. Research, develop, document, and implement tracking and inventory methodologies for maintaining inventory of critical assets (human resources, hardware, and software). Design, implement, document, and evaluate government computer security programs. Develop government security policy documentation. Develop and maintain Systems and Infrastructure Security Plan. Develop and maintain IT Security Architecture Plan. Present technical briefings to senior level government officials. Develop and evaluate plans, principles, and procedures for accomplishing customer IT security studies and provide professional analysis of methods and objectives. May supervise IT Security team.

**Minimum Education:** Undergraduate degree in related field and 13 years specialized experience. With 17 years of specialized experience a degree is not required. One year of college is equivalent to one year of experience. Any related industry certification can be substituted for one year of experience. CISSP or related industry certification desired. Subject matter expert of computer security requirements and practices in the civilian sector of the federal government. Must have experience in conducting and writing Certification & Accreditation of systems. Must have experience conducting NIST self-assessments. Must have demonstrated experience and/or in depth knowledge consistent with security principles and best practices as reflected in the NIST-800-18, OMB A-130, and NIST-800-26 and other applicable Federal regulations and guidelines. Experience with designing, implementing, documenting, and evaluating government computer security programs. Experience with writing government computer security policy documentation.

Experience with designing, implementing, documenting, and evaluating government computer security programs. Thorough understanding of and hands-on experience with computer operations and systems of various types as well as an understanding of computer security.

**24. LOGISTICS COORDINATOR I**

**Minimum/General Experience:** Will maintain and control a system of records relative to purchasing and/or logistics for all contracting activities. Maintains and adheres to the agency’s purchasing policies. Maintains and controls the Fixed Asset Inventory. Review and maintains the Purchase Order module of the in-house Accounting System.

**Functional Responsibility: Purchasing:** Process purchase requisitions, purchase orders, and paperwork related to the purchase of materials and services for the Division. Select, justify, and negotiate the selection of vendors/subcontractors to provide supplies and services. Maintain and adhere to the Department's Procurement Manual and Purchasing Policy. Maintain the appropriate files and logs to support the purchasing function and contracting activities. Develop and implement procedures for Project Managers to follow in processing requisitions.

**Logistics:** Maintain the records and control the fixed asset inventory. Direct the accurate preparation and maintenance of stock record accounts, property registers, and source documents. Establish stock control levels to maintain the appropriate inventory level. Control all requisitioned items back orders, and due-in and due-out records to ensure proper procurement identification. Authorize and direct the preparation of requests for local direct purchase transactions and work with Federal purchasing groups. Determine the status of repairable items with respect to rework, salvage, or final disposition. Maintain contact with customer representatives and other Government contractors in answering questions about Government property.

**Minimum Education:** Undergraduate degree desired. 4 years of related finance, budget, logistics, office management, or procurement experience may be substituted for the degree requirements. One year of college is equivalent to one year of experience. Any related industry certification can be substituted for one year of experience. Must have 1 year specialized procurement and logistics experience. Must be proficient with excel and a database program to support reporting, budgeting, and tracking work activities. Must have sufficient computer and word processor skills to accomplish basic inventory and records keeping entries into supply forms in use. Ability to communicate, orally and in writing, and coordinate actions effectively with individuals at all organizational and management levels within, and external to, the Department.



**25. LOGISTICS COORDINATOR II**

**Minimum/General Experience:** Will maintain and control a system of records relative to purchasing and/or logistics for all contracting activities. Maintains and adheres to the agency’s purchasing policies. Maintains and controls the Fixed Asset Inventory. Review and maintains the Purchase Order module of the in-house Accounting System.

**Functional Responsibility: Purchasing:** Process purchase requisitions, purchase orders, and paperwork related to the purchase of materials and services for the Division. Select, justify, and negotiate the selection of vendors/subcontractors to provide supplies and services Maintain and adhere to the Department's Procurement Manual and Purchasing Policy. Maintain the appropriate files and logs to support the purchasing function and contracting activities. Develop and implement procedures for Project Managers to follow in processing requisitions.

**Logistics:** Maintain the records and control the fixed asset inventory. Direct the accurate preparation and maintenance of stock record accounts, property registers, and source documents. Establish stock control levels in order to maintain the appropriate inventory level. Control all requisitioned items back orders, and due-in and due-out records to ensure proper procurement identification. Authorize and direct the preparation of requests for local direct purchase transactions and work with Federal purchasing groups. Determine the status of repairable items with respect to rework, salvage, or final disposition. Maintain contact with customer representatives and other Government contractors in answering questions about Government property.

**Minimum Education:** Undergraduate degree desired. 7 years of related finance, budget, logistics, office management, or procurement experience may be substituted for the degree requirements. One year of college is equivalent to one year of experience. Any related industry certification can be substituted for one year of experience. Must have 3 years specialized procurement and logistics experience. Must be proficient with excel and a database program to support reporting, budgeting, and tracking work activities. Must have sufficient computer and word processor skills to accomplish basic inventory and records keeping entries into supply forms in use. Ability to communicate, orally and in writing, and coordinate actions effectively with individuals at all organizational and management levels within, and external to, the Department.

**26. LOGISTICS COORDINATOR III**

**Minimum/General Experience:** Will maintain and control a system of records relative to purchasing and/or logistics for all contracting activities. Maintains and adheres to the agency’s purchasing policies. Maintains and controls the Fixed Asset Inventory. Review and maintains the Purchase Order module of the in-house Accounting System.

**Functional Responsibility: Purchasing:** Process purchase requisitions, purchase orders, and paperwork related to the purchase of materials and services for the Division. Select, justify, and negotiate the selection of vendors/subcontractors to provide supplies and services. Maintain and adhere to the Department's Procurement Manual and Purchasing Policy. Maintain the appropriate files and logs to support the purchasing function and contracting activities. Develop and implement procedures for Project Managers to follow in processing requisitions.

**Logistics:** Maintain the records and control the fixed asset inventory. Direct the accurate preparation and maintenance of stock record accounts, property registers, and source documents. Establish stock control levels in order to maintain the appropriate inventory level. Control all requisitioned items back orders, and due-in and due-out records to ensure proper procurement identification. Authorize and direct the preparation of requests for local direct purchase transactions and work with Federal purchasing groups. Determine the status of repairable items with respect to rework, salvage, or final disposition. Maintain contact with customer representatives and other Government contractors in answering questions about Government property.

**Minimum Education:** Supervise subordinate Logistics personnel. Undergraduate degree desired. 9 years of related finance, budget, logistics, office management, or procurement experience may be substituted for the degree requirements. One year of college is equivalent to one year of experience. Any related industry certification can be substituted for one year of experience. Must have 5 years specialized procurement and logistics experience. Must be proficient with excel and a database program to support reporting, budgeting, and tracking work activities. Must have sufficient computer and word processor skills to accomplish basic inventory and records keeping entries into supply forms in use. Ability to communicate, orally and in writing, and coordinate actions effectively with individuals at all organizational and management levels within, and external to, the Department.

**27. SECURITY MANAGER I**

**Minimum/General Experience:** Will work under limited supervision in performing program security support. Conducts duties and responsibilities IAW agency policies and applicable security regulations. Possess a technical proficiency, specialized experience, and management in the area(s) of the project's statement of work. Possesses analytical and specialized technical skills, which will enable him/her to perform all aspect of the job to include security project management and policy issues agency-wide, formulate strategies, and establish priorities for their resolution in a timely, responsive manner.

**Functional Responsibility:** For the Security Division or Program Office, manage the project in accordance with the statement of work, budget and scheduled deliverables. Provide recommendations regarding project management and participate in the development of project management practices, procedures, and processes. Provide a managed structure of data for decision making and recommend courses of action. Track, update and prepare reports on various specialized projects. Receive and review biweekly reports. Review project performance reviews and other documents. Prepare monthly status reports in prescribed format for management review. Update and review project schedule information. Forecast future progress based project data. Develop agendas in coordination with managers, facilitate meetings as requested, and edit minutes of management meetings. Assist with special projects to include special presentation charts, model development, forms development, and project management training.

**Minimum Education:** Undergraduate in an associated technical, security or management discipline, with a minimum of 1 year related specialized security experience. 5 years of specialized experience can be substituted for the degree requirement. One year of college is equivalent to one year of experience. Any related industry certification can be substituted for one year of experience. 1 year of direct Government contracting experience at task/project management level desired. Applicable Industry Certification desired.

Specialized experience is directly related to duties and responsibilities to include policy and security standard development, or security project management planning responsibilities. Experience with applicable security requirements and practices in the civilian sector of the federal government. Must have demonstrated experience consistent with security principles and best practices with applicable Federal regulations and guidelines.

**28. SECURITY MANAGER II**

**Minimum/General Experience:** Will work under limited supervision in performing program security support. Conducts duties and responsibilities IAW agency policies and applicable security regulations. Possess a technical proficiency, specialized experience, and management in the area(s) of the project's statement of work. Possesses analytical and specialized technical skills which will enable him/her to perform all aspect of the job to include security project management and policy issues agency-wide, formulate strategies, and establish priorities for their resolution in a timely, responsive manner.

**Functional Responsibility:** For the Security Division or Program Office, manage the project in accordance with the statement of work, budget, and scheduled deliverables. Provide recommendations regarding project management and participate in the development of project management practices, procedures, and processes. Provide a managed structure of data for decision making and recommend courses of action. Track, update and prepare reports on various specialized projects. Receive and review biweekly reports. Review project performance reviews and other documents. Prepare monthly status reports in prescribed format for management review. Update and review project schedule information. Forecast future progress based project data. Develop agendas in coordination with managers, facilitate meetings as requested, and edit minutes of management meetings. Assist with special projects to include special presentation charts, model development, forms development, and project management training.

**Minimum Education:** Undergraduate in an associated technical, security or management discipline, with a minimum of 3 years related specialized security experience with a Graduate degree, must have a minimum of 1 year related specialized experience. One year of college is equivalent to one year of experience. Any related industry certification can be substituted for one year of experience. 2 years of direct Government contracting experience at task/project management level desired. Applicable Industry Certification desired.

Specialized experience is directly related to duties and responsibilities to include policy and security standard development, or security project management planning responsibilities. Experience with applicable security requirements and practices in the civilian sector of the federal government. Must have demonstrated experience consistent with security principles and best practices with applicable Federal regulations and guidelines.

**29. SECURITY MANAGER III**

**Minimum/General Experience:** Will work under minimal supervision in performing program security support. Conducts duties and responsibilities IAW agency policies and applicable security regulations. Possess a technical proficiency, specialized experience, and management in the area(s) of the project's statement of work. Possesses analytical and specialized technical skills, which will enable him/her to perform all aspect of the job to include security project management and policy issues agency-wide, formulate strategies, and establish priorities for their resolution in a timely, responsive manner.

**Functional Responsibility:** For the Security Division or Program Office, manage the project in accordance with the statement of work, budget and scheduled deliverables. Provide recommendations regarding project management and participate in the development of project management practices, procedures, and processes. Provide a managed structure of data for decision making and recommend courses of action. Track, update and prepare reports on various specialized projects. Receive and review biweekly reports. Review project performance reviews and other documents. Prepare monthly status reports in prescribed format for management review. Update and review project schedule information. Forecast future progress based project data. Develop agendas in coordination with managers, facilitate meetings as requested, and edit minutes of management meetings. Assist with special projects to include special presentation charts, model development, forms development, and project management training.

**Minimum Education:** Undergraduate in an associated technical or management discipline, with a minimum of 5 years related specialized security experience and 1 year management experience. With a Graduate degree, must have a minimum of 3 years related specialized experience. One year of college is equivalent to one year of experience. Any related industry certification can be substituted for one year of experience. 3 years of direct Government contracting experience at task/project management level desired. Applicable Industry Certification desired.

Specialized experience is directly related to duties and responsibilities to include policy and security standard development, or security, project management planning responsibilities. Experience with applicable security requirements and practices in the civilian sector of the federal government. Must have demonstrated experience consistent with security principles and best practices with applicable Federal regulations and guidelines.

**30. SECURITY MANAGER IV**

**Minimum/General Experience:** The project manager serves as the primary point of contact to the contract officer technical representative (COTR) and as the advisor to the staff elements and contractor representatives. Possess a technical proficiency, specialized IT security experience, and management in the area(s) of the project's statement of work. Provide overall corporate management of employees in support of contract performance, to include costs, time management, conflict resolution, task performance, vacancies, disciplinary actions, and evaluations.

**Functional Responsibility:** Supervise the IT Security Team and manage the project in accordance with the statement of work, budget and scheduled deliverables. Develop and formally documents the security procedures and practices both in-place and under development; write system security plans, an entity-wide security program, and contingency plan for mission critical systems; design and teach computer security awareness program; and develop recommendations for organizational changes to enhance the automated information security posture in response to agency audits. Conduct IT security reviews, audits and tests. Submit project reports on a regular basis to the client. Prepare and present project briefings to senior level agency officials.

**Minimum Education:** Undergraduate in an associated technical or management discipline, with a minimum of 7 years related specialized Security experience and 2 years management experience. With a Graduate degree, must have a minimum of 5 years related specialized experience and 1 year management experience. One year of college is equivalent to one year of experience. Any related industry certification can be substituted for one year of experience. 5 years of direct Government contracting experience at task/project management level desired. Applicable Industry Certification desired.

Experience in the following areas is highly desired: complete IT security project development from inception to full implementation and demonstrated ability to provide guidance and direction in IT security tasks. Subject matter expert of computer security requirements and practices in the civilian sector of the federal government. Must have demonstrated experience consistent with security principles and best practices as reflected in FISMA, NIST-800-18, OMB A-130, and NIST-800-26 and other applicable Federal regulations and guidelines.

<b>31. SECURITY MANAGER V</b>
<p><b>Minimum/General Experience:</b> The project manager serves as the primary point of contact to the contract officer technical representative (COTR) and as the advisor to the staff elements and contractor representatives. Possess a technical proficiency, specialized IT security experience, and management in the area(s) of the project's statement of work. Provide overall corporate management of employees in support of contract performance, to include costs, time management, conflict resolution, task performance, vacancies, disciplinary actions, and evaluations.</p>
<p><b>Functional Responsibility:</b> Supervise the IT Security Team and manage the project in accordance with the statement of work, budget, and scheduled deliverables. Develop and formally documents the security procedures and practices both in-place and under development; writes system security plans, an entity-wide security program, and contingency plan for mission critical systems; designs and teaches computer security awareness program; and develop recommendations for organizational changes to enhance the automated information security posture in response to agency audits. Conduct IT security reviews, audits, and tests. Submit project reports on a regular basis to the client. Prepare and present project briefings to senior level agency officials.</p>
<p><b>Minimum Education:</b> Undergraduate in an associated technical or management discipline, with a minimum of 9 years related specialized Security experience and 3 years management experience. With a Graduate degree, must have a minimum of 7 years related specialized experience and 4 years management experience. One year of college is equivalent to one year of experience. Any related industry certification can be substituted for one year of experience. 7 years of direct Government contracting experience at task/project management level desired. Applicable Industry Certification desired.</p> <p>Experience in the following areas is highly desired: complete IT security project development from inception to full implementation and demonstrated ability to provide guidance and direction in IT security tasks. Subject matter expert of computer security requirements and practices in the civilian sector of the federal government. Must have demonstrated experience consistent with security principles and best practices as reflected in FISMA, NIST-800-18, OMB A-130, and NIST-800-26 and other applicable Federal regulations and guidelines.</p>

<b>32. SECURITY ADMINISTRATOR I</b>
<p><b>Minimum/General Experience:</b> Provide administrative support to a Security Program Office with responsibilities to include checking, updating and running reports in various security databases. Perform clerical duties in processing security forms and reports, does filing and other routine administrative duties, and maintain and order office supplies.</p>
<p><b>Functional Responsibility:</b> Perform data entry by keying data into a computer and verifying data from a wide variety of source documents such as computer generated reports, program coding sheets, time and attendance records, and other narrative and statistical information. Detects and rejects illegible or incomplete source documents and information. Verifies accuracy of data entered and corrects keying errors. Prepare periodic or special reports of workload and information from records and files to assist Program Manager and other technical staff. Perform general office related clerical duties such as answering telephones, referring callers or furnishing information, maintaining hard and electronic files, courier, and distributing completed documents.</p>
<p><b>Minimum Education:</b> High school diploma or GED equivalent and 2 years general office experience required. One year of college is equivalent to one year of experience. Any related industry certification can be substituted for one year of experience. Must have strong computer skills to include database experience and possess a proficiency in data entry. Knowledge and ability to follow database guidelines.</p>

<p><b>33. SECURITY ADMINISTRATOR II</b></p> <p><b>Minimum/General Experience:</b> Provide administrative and coordination support for a division or department. Provide general administrative support to the division manager and maintains various administrative reports.</p> <p><b>Functional Responsibility:</b> Maintain office records and interfaces with various levels of personnel in the agency on office policies, budget, personnel matters and procedures related to the day-to-day operation of the office. Provide administrative support for the manager for general administration, department reports, rosters, action tracking, and special projects. Serves as the administrative point of contact for forms related to the office operations. Prepare the office files each year; maintain them throughout the year, and annual archiving. Order and maintain office supplies for the division. Maintain office equipment, property/equipment inventories, and office vehicles as assigned by the Department. Place calls for equipment repair requests and physical plant problems.</p> <p><b>Minimum Education:</b> High school diploma or GED equivalent and 3 years specialized administrative experience required. One year of college is equivalent to one year of experience. Any related industry certification can be substituted for one year of experience. Must be proficient with Microsoft Word; have basic skills with Excel and PowerPoint; and other database software experience desired.</p>
--

<p><b>34. SECURITY ADMINISTRATOR III</b></p> <p><b>Minimum/General Experience:</b> Will support the division Manager and members of the team in the daily office administration, personnel, financial, database administration, and project requirements. Considerable coordination will be required within the division and with departments throughout the agency.</p> <p><b>Functional Responsibility:</b> Provide administrative support for status reports, briefing presentations and special projects. Use work breakdown structures to track project activities. Prepare charts, tables, graphs, and diagrams to assist in tracking and reporting program activities. Assist in technical and programmatic input to support client briefings, status reports, and deliverable preparation. Coordinate and assist the office personnel to complete tasks within the following areas: security/clearance processing, timesheet reporting, purchasing, travel, training, material reproduction, inventory, etc. Assist/review the preparation of all reports and tracking documents to include budgets, monthly reports, travel expense reports, and personnel tracking, etc.</p> <p><b>Minimum Education:</b> Undergraduate degree and 3 years specialized administrative experience. Without a degree, must have 7 years of specialized administrative experience. One year of college is equivalent to one year of experience. Any related industry certification can be substituted for one year of experience. Specialized experience includes office management, suspense tracking, review of executive level correspondence, database administration, financial and project status tracking and reporting, monthly reports, and maintaining operating procedures. Thorough knowledge of electronic database operations management, administrative and correspondence processing procedures, and understanding of procedures required for processing actions for review, approval and release. Must be proficient with Microsoft Word; have basic skills with Excel and PowerPoint; database software experience required; and MS Project experience a plus.</p>
---



**35. SECURITY ADMINISTRATOR IV**

**Minimum/General Experience:** Will support the division Manager and members of the team in the daily office administration, personnel, financial, database administration, and project requirements. Considerable coordination will be required within the division and with departments throughout the agency.

**Functional Responsibility:** Provide administrative support for status reports, briefing presentations and special projects. Use work breakdown structures to track project activities. Prepare charts, tables, graphs, and diagrams to assist in tracking and reporting program activities. Coordinate the technical and programmatic input to support client briefings, status reports, and deliverable preparation. Coordinate and assist the office personnel to complete tasks within the following areas: security/clearance processing, timesheet reporting, purchasing, travel, training, material reproduction, inventory, etc. Prepare and maintain various budgetary spreadsheets for each project and provide summary and analysis as requested. Prepare monthly Status Reports for review and coordination with the appropriate manager. Track required information from other departments and update spreadsheets bi-monthly

**Minimum Education:** Undergraduate degree and 5 years specialized office experience. Without a degree, must have 5 years of specialized administrative experience. One year of college is equivalent to one year of experience. Any related industry certification can be substituted for one year of experience. Specialized experience includes office management, suspense tracking, review of executive level correspondence, database administration, financial and project status tracking and reporting, monthly reports, and maintaining operating procedures. Thorough knowledge of electronic database operations management, administrative and correspondence processing procedures, and understanding of procedures required for processing actions for review, approval and release. Must be proficient with Microsoft Word; have basic skills with Excel and PowerPoint; database software experience required; and MS Project experience a plus.

**36. SECURITY SPECIALIST I**

**Minimum/General Experience:** Overall program management support to an agency in support of specific security requirements. Responsibilities include industrial security, security policy review and research; working group assistance; security training; security program development; protection, acquisition and management of goods and services; investigations and inspections, security program review, development, and implementation; and liaison with other Government and/or private agencies.

**Functional Responsibility:** Assist in the development and issuance of policy standards for a specific division with a specialized security function in support of division, organization, or agency. Assist in the development, preparation, and issuance of program guides for Departmental programs. Monitor, analyze and investigate security violations to determine causes, highlight program weaknesses, pinpoint responsibility/culpability, and recommending corrective action as appropriate. Liaison with Senior Officers, Intelligence Community and other security agencies on office security programs as required. Provide support services for a comprehensive security awareness program designed to educate employees conducted through the use of briefings, lectures, audio-visual presentations, and printed media. Assist in developing and producing security awareness media to include posters, handbooks, and similar materials. Provide input/review of proposed briefing and training packages. Work independently, with oversight, to advise and assist office personnel on matters of security policy, procedures, and regulations. Conduct needs surveys and provide a report of findings for each survey conducted. Ensure that security policies are implemented according to procedures without undue interruption of normal operations. Provide research services and advise office personnel on national and international security developments. Prepare input for department briefings to senior level officials. Review outgoing office correspondence for appropriate office personnel. Travel domestically and overseas as required in support of program reviews, investigations, and security briefings.

**Minimum Education:** Undergraduate degree with 4 years specialized experience in one of the following areas: counterintelligence, investigations, industrial security, dignitary/VIP policy and security standard development, OPSEC, COMSEC, INFOSEC, security countermeasures programs, access systems operation and management, personnel protection and protecting classified information, or region desk officer. With 8 years of specialized experience a degree is not required. One year of college is equivalent to one year of experience. Any related industry certification can be substituted for one year of experience. Knowledge of NISPOM and, national and international security requirements. Understanding of and experience-based familiarity with the U.S. Federal Government and DoD agencies and their security practices.

**37. SECURITY SPECIALIST II**

**Minimum/General Experience:** Overall program management support to an agency in support of specific security requirements. Responsibilities include industrial security, security policy review and research; working group assistance; security training; security program development; protection, acquisition and management of goods and services; investigations and inspections, security program review, development, and implementation; and liaison with other Government and/or private agencies.

**Functional Responsibility:** Assist in the development and issuance of policy standards for a specific division with a specialized security function in support of division, organization, or agency. Assist in the development, preparation, and issuance of program guides for Departmental programs. Monitor, analyze and investigate security violations to determine causes, highlight program weaknesses, pinpoint responsibility/culpability, and recommending corrective action as appropriate. Liaison with Senior Officers, Intelligence Community and other security agencies on office security programs as required. Provide support services for a comprehensive security awareness program designed to educate employees conducted through the use of briefings, lectures, audio-visual presentations, and printed media. Assist in developing and producing security awareness media to include posters, handbooks, and similar materials. Provide input/review of proposed briefing and training packages. Work independently, with oversight, to advise and assist office personnel on matters of security policy, procedures, and regulations. Conduct needs surveys and provide a report of findings for each survey conducted. Ensure that security policies are implemented according to procedures without undue interruption of normal operations. Provide research services and advise office personnel on national and international security developments. Prepare input for department briefings to senior level officials. Review outgoing office correspondence for appropriate office personnel. Travel domestically and overseas as required in support of program reviews, investigations, and security briefings.

**Minimum Education:** Undergraduate degree with 6 years specialized experience in one of the following areas: counterintelligence, investigations, industrial security, dignitary/VIP policy and security standard development, OPSEC, COMSEC, INFOSEC, security countermeasures programs, access systems operation and management, personnel protection and protecting classified information, or region desk officer. With 10 years of specialized experience a degree is not required. One year of college is equivalent to one year of experience. Any related industry certification can be substituted for one year of experience. Knowledge of NISPOM and, national and international security requirements. Understanding of and experience-based familiarity with the U.S. Federal Government and DoD agencies and their security practices.

**38. SECURITY SPECIALIST III**

**Minimum/General Experience:** Overall program management support to an agency in support of specific security requirements. Responsibilities include industrial security, security policy review and research; working group assistance; security training; security program development; protection, acquisition and management of goods and services; investigations and inspections, security program review, development, and implementation; and liaison with other Government and/or private agencies.

**Functional Responsibility:** Interpret management directives and guidance as it relates to security programs/operations and make appropriate implementation recommendations. Assist in the development, preparation, and issuance of program guides for Departmental programs. Monitor, analyze and investigate security violations to determine causes, highlight program weaknesses, pinpoint responsibility/culpability, and recommending corrective action as appropriate. Liaison with Senior Officers, Intelligence Community and other security agencies on office security programs as required. Provide support services for a comprehensive security awareness program designed to educate employees conducted through the use of briefings, lectures, audio-visual presentations, and printed media. Assist in developing and producing security awareness media to include posters, handbooks, and similar materials. Provide input/review of proposed briefing and training packages. Work independently, with oversight, to advise and assist office personnel on matters of security policy, procedures, and regulations. Conduct needs surveys and provides a report of findings for each survey conducted. Ensure that security policies are implemented according to procedures without undue interruption of normal operations. Provide research services and advise office personnel on national and international security developments. Prepare input for department briefings to senior level officials. Review outgoing office correspondence for appropriate office personnel. Travel domestically and overseas as required in support of program reviews, investigations, and security briefings.

**Minimum Education:** Undergraduate degree with 8 years specialized experience in one of the following areas: counterintelligence, investigations, industrial security, dignitary/VIP policy and security standard development, OPSEC, COMSEC, INFOSEC, security countermeasures programs, access systems operation and management, personnel protection and protecting classified information, or region desk officer. With 12 years of specialized experience a degree is not required. One year of college is equivalent to one year of experience. Any related industry certification can be substituted for one year of experience. Knowledge of NISPOM and, national and international security requirements. Understanding of and experience-based familiarity with the U.S. Federal Government and DoD agencies and their security practices.

**39. SECURITY SPECIALIST IV**

**Minimum/General Experience:** Overall program management support to an agency in support of specific security requirements. Responsibilities include industrial security, security policy review and research; working group assistance; security training; security program development; protection, acquisition and management of goods and services; investigations and inspections, security program review, development, and implementation; and liaison with other Government and/or private agencies.

**Functional Responsibility:** Interpret management directives and guidance as it relates to security programs/operations and make appropriate implementation recommendations. Assist in the development, preparation, and issuance of program guides for Departmental programs. Monitor, analyze and investigate security violations to determine causes, highlight program weaknesses, pinpoint responsibility/culpability, and recommending corrective action as appropriate. Liaison with Senior Officers, Intelligence Community and other security agencies on office security programs as required. Provide management services for a comprehensive security awareness program designed to educate employees conducted through the use of briefings, lectures, audio-visual presentations, and printed media. Assist in developing and producing security awareness media to include posters, handbooks, and similar materials. Provide input/review of proposed briefing and training packages. Work independently, with oversight, to advise and assist office personnel on matters of security policy, procedures, and regulations. Conducts needs surveys and provide a report of findings for each survey conducted. Ensure that security policies are implemented according to procedures without undue interruption of normal operations. Provide research services and advise office personnel on national and international security developments. Prepare and present department briefings to senior level officials. Review outgoing office correspondence for appropriate office personnel. Travel domestically and overseas as required in support of program reviews, investigations, and security briefings.

**Minimum Education:** Undergraduate degree with 10 years specialized experience in one of the following areas: counterintelligence, investigations, industrial security, dignitary/VIP policy and security standard development, OPSEC, COMSEC, INFOSEC, security countermeasures programs, access systems operation and management, personnel protection and protecting classified information, or region desk officer. With 14 years of specialized experience a degree is not required. One year of college is equivalent to one year of experience. Any related industry certification can be substituted for one year of experience. Knowledge of NISPOM and, national and international security requirements. Understanding of and experience-based familiarity with the U.S. Federal Government and DoD agencies and their security practices.

**40. SECURITY SPECIALIST V**

**Minimum/General Experience:** Overall program management support to an agency in support of specific security requirements. Responsibilities include industrial security, security policy review and research; working group assistance; security training; security program development; protection, acquisition and management of goods and services; investigations and inspections, security program review, development, and implementation; and liaison with other Government and/or private agencies.

**Functional Responsibility:** Interpret management directives and guidance as it relates to security programs/operations and make appropriate implementation recommendations. Serve as lead in the development, preparation, and issuance of program guides for Departmental programs. Monitor, analyze and investigate security violations to determine causes, highlight program weaknesses, pinpoint responsibility/culpability, and recommending corrective action as appropriate. Liaison with Senior Officers, Intelligence Community and other security agencies on office security programs as required. Provide management services for a comprehensive security awareness program designed to educate employees conducted through the use of briefings, lectures, audio-visual presentations, and printed media. Assist in developing and producing security awareness media to include posters, handbooks, and similar materials. Provide input/review of proposed briefing and training packages. Work independently, with oversight, to advise and assist office personnel on matters of security policy, procedures, and regulations. Conduct needs surveys and provides a report of findings for each survey conducted. Ensure that security policies are implemented according to procedures without undue interruption of normal operations. Provide research services and advise office personnel on national and international security developments. Prepare and present department briefings to senior level officials. Review outgoing office correspondence for appropriate office personnel. Travel domestically and overseas as required in support of program reviews, investigations, and security briefings.

**Minimum Education:** Undergraduate degree with 12 years specialized experience in one of the following areas: counterintelligence, investigations, industrial security, dignitary/VIP policy and security standard development, OPSEC, COMSEC, INFOSEC, security countermeasures programs, access systems operation and management, personnel protection and protecting classified information, or region desk officer. With 16 years of specialized experience a degree is not required. One year of college is equivalent to one year of experience. Any related industry certification can be substituted for one year of experience. Knowledge of NISPOM and, national and international security requirements. Understanding of and experience-based familiarity with the U.S. Federal Government and DoD agencies and their security practices.

**41. SR. TECHNICAL SECURITY SPECIALIST I**

**Minimum/General Experience:** Utilizing state-of-the-art technical equipment, the Sr. Technical Security Specialist will be responsible for Technical Surveillance Countermeasures (TSCM) investigations, inspections, in-conference security monitoring services, pre-construction advice, and assistance missions. Provide advice and research on technology solutions and equipment for the TSCM program. Conduct technical briefings to senior level government officials. Ability to read and understand design plans for purposed technical security upgrades. Knowledge of subversive organizations and their methods of operation. Knowledge of national and international security technology. Understanding of, and experience-based familiarity with, information and technical security practices within the Information Technology environment required to establish and maintain system integrity for safeguarding classified information in a secure environment. Ability to communicate and coordinate actions effectively with individuals at all organizational and management levels.

**Functional Responsibility:** Serve as the technical subject matter expert providing oversight and advice to office personnel on matters of technical security policy, procedures, and regulations. Provide support services for a comprehensive technical security program designed to protect facilities and employees. Assist in developing and reviewing technical security designs for the agency's facilities. Providing input/review of proposed policies. Apply technical procedures in conducting needs surveys for preventing unauthorized access to, and possible disclosure of, classified information. Provide a report of findings for each survey conducted. Ensure that security policies are implemented according to procedures without undue interruption of normal operations. Provide research services and advising office personnel on national and international developments in commercial, state-of-the-art, security technology.

**Minimum Education:** Undergraduate degree in an information technology, electronics, business, security or a related discipline with 4 years specialized experience in the areas of technical security programs, access systems operation and management, and RF/signal analysis with a background in electronics intelligence. Knowledge of automated information and on-line systems and tools. With 8 years of specialized experience a degree is not required. One year of college is equivalent to one year of experience. Any related industry certification can be substituted for one year of experience.

Must have training and experience in Technical Surveillance Countermeasures (TSCM) and related fields to include graduation from a formal Federal TSCM training course; graduation from a formal Federal intelligence and/or counterintelligence course, and field experience with a Federal agency in TSCM, intelligence and counterintelligence activities. **Must possess a current clearance at the required contract level.**

**42. SR. TECHNICAL SECURITY SPECIALIST II**

**Minimum/General Experience:** Utilizing state-of-the-art technical equipment, the Sr. Technical Security Specialist will be responsible for Technical Surveillance Countermeasures (TSCM) investigations, inspections, in-conference security monitoring services, pre-construction advice, and assistance missions. Provide advice and research on technology solutions and equipment for the TSCM program. Conduct technical briefings to senior level government officials. Ability to read and understand design plans for purposed technical security upgrades. Knowledge of subversive organizations and their methods of operation. Knowledge of national and international security technology. Understanding of, and experience-based familiarity with, information and technical security practices within the Information Technology environment required to establish and maintain system integrity for safeguarding classified information in a secure environment. Ability to communicate and coordinate actions effectively with individuals at all organizational and management levels.

**Functional Responsibility:** Serve as the technical subject matter expert providing oversight and advice to office personnel on matters of technical security policy, procedures, and regulations. Provide support services for a comprehensive technical security program designed to protect facilities and employees. Assist in developing and reviewing technical security designs for the agency's facilities. Providing input/review of proposed policies. Apply technical procedures in conducting needs surveys for preventing unauthorized access to, and possible disclosure of, classified information. Provide a report of findings for each survey conducted. Ensure that security policies are implemented according to procedures without undue interruption of normal operations. Provide research services and advising office personnel on national and international developments in commercial, state-of-the-art, security technology.

**Minimum Education:** Undergraduate degree in an information technology, electronics, business, security or a related discipline with 6 years specialized experience in the areas of technical security programs, access systems operation and management, and RF/signal analysis with a background in electronics intelligence. Knowledge of automated information and on-line systems and tools. With 10 years of specialized experience a degree is not required. One year of college is equivalent to one year of experience. Any related industry certification can be substituted for one year of experience.

Must have training and experience in Technical Surveillance Countermeasures (TSCM) and related fields to include graduation from a formal Federal TSCM training course; graduation from a formal Federal intelligence and/or counterintelligence course, and field experience with a Federal agency in TSCM, intelligence and counterintelligence activities. **Must possess a current clearance at the required contract level.**



**43. SR. TECHNICAL SECURITY SPECIALIST III**

**Minimum/General Experience:** Utilizing state-of-the-art technical equipment, the Sr. Technical Security Specialist will be responsible for Technical Surveillance Countermeasures (TSCM) investigations, inspections, in-conference security monitoring services, pre-construction advice, and assistance missions. Provide advice and research on technology solutions and equipment for the TSCM program. Conduct technical briefings to senior level government officials. Ability to read and understand design plans for purposed technical security upgrades. Knowledge of subversive organizations and their methods of operation. Knowledge of national and international security technology. Understanding of, and experience-based familiarity with, information and technical security practices within the Information Technology environment required to establish and maintain system integrity for safeguarding classified information in a secure environment. Ability to communicate and coordinate actions effectively with individuals at all organizational and management levels.

**Functional Responsibility:** Serve as the technical subject matter expert providing oversight and advice to office personnel on matters of technical security policy, procedures, and regulations. Provide support services for a comprehensive technical security program designed to protect facilities and employees. Assist in developing and reviewing technical security designs for the agency's facilities. Providing input/review of proposed policies. Apply technical procedures in conducting needs surveys for preventing unauthorized access to, and possible disclosure of, classified information. Provide a report of findings for each survey conducted. Ensure that security policies are implemented according to procedures without undue interruption of normal operations. Provide research services and advising office personnel on national and international developments in commercial, state-of-the-art, security technology.

**Minimum Education:** Undergraduate degree in an information technology, electronics, business, security or a related discipline with 8 years specialized experience in the areas of technical security programs, access systems operation and management, and RF/signal analysis with a background in electronics intelligence. Knowledge of automated information and on-line systems and tools. With 12 years of specialized experience a degree is not required. One year of college is equivalent to one year of experience. Any related industry certification can be substituted for one year of experience.

Must have training and experience in Technical Surveillance Countermeasures (TSCM) and related fields to include graduation from a formal Federal TSCM training course; graduation from a formal Federal intelligence and/or counterintelligence course, and field experience with a Federal agency in TSCM, intelligence and counterintelligence activities. **Must possess a current clearance at the required contract level.**

**44. SR. TECHNICAL SECURITY SPECIALIST IV**

**Minimum/General Experience:** Utilizing state-of-the-art technical equipment, the Sr. Technical Security Specialist will be responsible for Technical Surveillance Countermeasures (TSCM) investigations, inspections, in-conference security monitoring services, pre-construction advice, and assistance missions. Provide advice and research on technology solutions and equipment for the TSCM program. Conduct technical briefings to senior level government officials. Ability to read and understand design plans for purposed technical security upgrades. Knowledge of subversive organizations and their methods of operation. Knowledge of national and international security technology. Understanding of, and experience-based familiarity with, information and technical security practices within the Information Technology environment required to establish and maintain system integrity for safeguarding classified information in a secure environment. Ability to communicate and coordinate actions effectively with individuals at all organizational and management levels.

**Functional Responsibility:** Serve as the technical subject matter expert providing oversight and advice to office personnel on matters of technical security policy, procedures, and regulations. Supervise and coordinate all TSCM activities within the department. Provide support services for a comprehensive technical security program designed to protect facilities and employees. Assist in developing and reviewing technical security designs for the agency's facilities. Providing input/review of proposed policies. Apply technical procedures in conducting needs surveys for preventing unauthorized access to, and possible disclosure of, classified information. Provide a report of findings for each survey conducted. Ensure that security policies are implemented according to procedures without undue interruption of normal operations. Provide research services and advising office personnel on national and international developments in commercial, state-of-the-art, security technology.

**Minimum Education:** Undergraduate degree in an information technology, electronics, business, security, or a related discipline with 10 years specialized experience in the areas of technical security programs, access systems operation and management, and RF/signal analysis with a background in electronics intelligence. Knowledge of automated information and on-line systems and tools. With 14 years of specialized experience a degree is not required. One year of college is equivalent to one year of experience. Any related industry certification can be substituted for one year of experience.

Must have training and experience in Technical Surveillance Countermeasures (TSCM) and related fields to include graduation from a formal Federal TSCM training course; graduation from a formal Federal intelligence and/or counterintelligence course, and field experience with a Federal agency in TSCM, intelligence and counterintelligence activities. **Must possess a current clearance at the required contract level.**

**45. COUNTERINTELLIGENCE SPECIALIST II**

**Minimum/General Experience:** Overall program management support to an agency in support of specific counterintelligence security requirements. Responsibilities include developing, implementing, and overseeing a federal government or defense agency’s security policies, programs, and standards. Provides specialized security program support that may include security training and education. May work with various departments and other agencies in support of the security mission. Must be eligible for Top Secret level clearance.

**Functional Responsibility:** Management responsibility for specific investigations or counterintelligence details. Leads and plans counter threat investigations. Monitors, collects, collates, analyzes, and disseminates intelligence utilizing security databases. Manages and conducts investigations and interrogations. Analyzes raw intelligence and finished intelligence products from a wide variety of sources. Produces intelligence analyses reports. Collects and analyzes all intelligence and counterintelligence data to determine foreign intelligence service interests in sensitive research or technologies or terrorist targeting of personnel/facilities. Briefs senior level officials on investigations / intelligence results. Liaison with local, state, federal, and international law enforcement. May manage a security program office. May have subject matter expertise in a specialized security area.

**Minimum Education:** Graduate degree with 5 years of specialized experience or undergraduate degree with 7 years specialized experience in the following areas: counterintelligence, HUMINT, counterespionage, anti-terrorism, intelligence, counter surveillance and/or security investigations. With 11 years of specialized experience a degree is not required. Any combined 6 months of military security related training is equivalent to 1 semester of college or 6 months of additional experience and can be substituted for specialized experience requirement. Knowledge of counterintelligence and investigative security requirements. Understanding of and experience-based familiarity with the U.S. Federal Government and DoD agencies and their security practices.