# ADVANCED RESOURCE TECHNOLOGIES, INC.

# CORPORATE COMMERCIAL PRICELIST

# FOR

# SECURITY SERVICES

## EFFECTIVE 01 MARCH 2021

# TABLE OF CONTENTS

**Page**

## COMMERCIAL PRICE LIST

| Contract Line Item Number | Commercial Job Title | 2021 ARTI Hourly Rate |
|---|---|---|
| 1 | Security Subject Matter Expert | $117.24 |
| 2 | Sr. Security Subject Matter Expert | $140.18 |
| 3 | Principle Security Subject Matter Expert | $177.62 |
| 4 | Forensic Computer Lab Manager | $143.54 |
| 5 | Computer Forensics Analyst I | $93.63 |
| 6 | Computer Forensics Analyst II | $106.10 |
| 7 | Computer Forensics Analyst III | $124.82 |
| 8 | Computer Forensics Analyst IV | $134.80 |
| 9 | Computer Forensics Technician I | $64.91 |
| 10 | Computer Forensics Technician II | $81.12 |
| 11 | Computer Forensics Technician III | $99.86 |
| 12 | Computer Forensics Technician IV | $112.33 |
| 13 | Budget Liaison Officer I | $92.04 |
| 14 | Budget Liaison Officer II | $102.58 |
| 15 | Budget Liaison Officer III | $113.34 |
| 16 | Security EMT Instructor I | $52.92 |
| 17 | Security EMT Instructor II | $68.04 |
| 18 | Security EMT Instructor III | $80.85 |
| 19 | IT Security Specialist I | $88.64 |
| 20 | IT Security Specialist II | $101.63 |
| 21 | IT Security Specialist III | $114.89 |
| 22 | IT Security Specialist IV | $130.15 |
| 23 | IT Security Specialist V | $174.40 |
| 24 | Logistics Coordinator I | $55.19 |
| 25 | Logistics Coordinator II | $80.42 |
| 26 | Logistics Coordinator III | $98.38 |
| 27 | Security Manager I | $65.10 |
| 28 | Security Manager II | $75.92 |
| 29 | Security Manager III | $87.79 |
| 30 | Security Manager IV | $106.38 |
| 31 | Security Manager V | $114.73 |
| 32 | Security Admin I | $32.85 |
| 33 | Security Admin II | $43.27 |
| 34 | Security Admin III | $51.87 |
| 35 | Security Admin IV | $56.68 |
| 36 | Security Specialist I | $62.14 |
| 37 | Security Specialist II | $69.07 |
| 38 | Security Specialist III | $70.32 |
| 39 | Security Specialist IV | $77.88 |
| 40 | Security Specialist V | $89.87 |
| 41 | Sr. Tech Sec Spec I | $92.49 |
| 42 | Sr. Tech Sec Spec II | $93.87 |
| 43 | Sr. Tech Sec Spec III | $105.98 |
| 44 | Sr. Tech Sec Spec IV | $120.10 |

| Contract Line Item Number | Commercial Job Title | 2021 ARTI Hourly Rate |
|---|---|---|
| 45 | Counterintelligence Specialist II | $121.16 |
| 46 | IT Security Analyst I | $105.79 |
| 47 | IT Security Analyst II | $115.49 |
| 48 | IT Security Analyst III | $125.30 |
| 49 | IT Security Analyst IV | $143.33 |
| 50 | IT Security Expert – Project Manager | $189.88 |
| 51 | IT Security Engineer – Penetration Tester | $151.89 |
| 52 | RF Engineer [Digital] | $121.10 |
| 53 | Sr. RF Engineer [Digital] | $127.14 |
| 54 | Intelligence Analyst | $57.30 |

## ADVANCED RESOURCE TECHNOLOGIES, INC. (ARTI)
## 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.

| 1. 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. 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). |

| 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. A Doctoral degree is desired. 20 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). |

| 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. Must be able to work independently of any direct supervision and provide technical direction and guidance to lower-level professional/technical personnel. |
| **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. A Doctoral degree is desired. 20+ 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. |

| 4. FORENSIC COMPUTER LAB MANAGER |
|---|
| **Minimum/General Experience:** 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. |
| **Functional Responsibility:** 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. |
| **Minimum Education:** 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. |

| 5. COMPUTER FORENSICS ANALYST I |
|---|
| **Minimum/General Experience:** Conduct computer forensic analysis of subject media and/or analysis of networks, intrusions, or e-mail systems. |
| **Functional Responsibility:** 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. |
| **Minimum Education:** 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. |

| 6. COMPUTER FORENSICS ANALYST II |
|---|
| **Minimum/General Experience:** Conduct computer forensic analysis of subject media and/or analysis of networks, intrusions, or e-mail systems. |
| **Functional Responsibility:** 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. |
| **Minimum Education:** 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. |

| 7. COMPUTER FORENSICS ANALYST III |
|---|
| **Minimum/General Experience:** Conduct computer forensic analysis of subject media and/or analysis of networks, intrusions, or e-mail systems. |
| **Functional Responsibility:** 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. |
| **Minimum Education:** Undergraduate degree and 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. |

| 8. COMPUTER FORENSICS ANALYST IV |
|---|
| **Minimum/General Experience:** Conduct computer forensic analysis of subject media and/or analysis of networks, intrusions, or e-mail systems. |
| **Functional Responsibility:** 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 develops training requirements, provides for quality assurance of work product, and ensures process integrity. Additionally, the section lead will provide primary liaison with other agency analysts as required. |
| **Minimum Education:** Undergraduate degree plus 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. |

| 9. COMPUTER FORENSICS TECHNICIAN I |
|---|
| **Minimum/General Experience:** The primary functions include network maintenance/oversight, hardware/software support, evidence custodianship, analyst support, and general administrative functions. |
| **Functional Responsibility:** 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. |
| **Minimum Education:** 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. |

| 10. COMPUTER FORENSICS TECHNICIAN II |
|---|
| **Minimum/General Experience:** The primary functions include network maintenance/oversight, hardware/software support, evidence custodianship, analyst support, and general administrative functions. |
| **Functional Responsibility:** 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. |
| **Minimum Education:** 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. |

| 11. COMPUTER FORENSICS TECHNICIAN III |
|---|
| **Minimum/General Experience:** The primary functions include network maintenance/oversight, hardware/software support, evidence custodianship, analyst support, and general administrative functions. |
| **Functional Responsibility:** 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. |
| **Minimum Education:** Undergraduate degree plus 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. |

| 12. COMPUTER FORENSICS TECHNICIAN IV |
|---|
| **Minimum/General Experience:** The primary functions include network maintenance/oversight, hardware/software support, evidence custodianship, analyst support, and general administrative functions. |
| **Functional Responsibility:** 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 develops training requirements, provides for quality assurance of work product, and ensures process integrity. Additionally, the section lead will provide primary liaison with other agency analysts as required. |
| **Minimum Education:** Undergraduate degree and 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. |

| 13. BUDGET LIAISON OFFICER I |
|---|
| **Minimum/General Experience:** 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. |
| **Functional Responsibility:** 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. |
| **Minimum Education:** 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. 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. |

| 14. BUDGET LIAISON OFFICER II |
|---|
| **Minimum/General Experience:** 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. |
| **Functional Responsibility:** 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. |
| **Minimum Education:** 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. 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. |

| 15. BUDGET LIAISON OFFICER III |
|---|
| **Minimum/General Experience:** 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. |
| **Functional Responsibility:** 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. |
| **Minimum Education:** 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. 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. |

| 16. SECURITY EMT INSTRUCTOR I |
|---|
| **Minimum/General Experience:** Develop and present EMT related training to medical and non-medical personnel in a formal classroom setting. |
| **Functional Responsibility:** 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 training environment to a diverse audience. Class duration may vary from 3 to 15 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. |
| **Minimum Education:** 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 certifications for the training subject matter. |

| 17. SECURITY EMT INSTRUCTOR II |
|---|
| **Minimum/General Experience:** Develop and present related training to personnel in a formal classroom setting and in overseas field offices. |
| **Functional Responsibility:** 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 3 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. |
| **Minimum Education:** A minimum of 8 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. Must have experience training and evaluating other instructors. Combat experience a plus. As applicable must possess current industry certifications for the training subject matter. |

| 18. SECURITY EMT INSTRUCTOR III |
|---|
| **Minimum/General Experience:** Develop and present related training to personnel in a formal classroom setting and in overseas field offices. |
| **Functional Responsibility:** 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 formal classroom setting 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. 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. |
| **Minimum Education:** A minimum of 10 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. 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. |

| 19. IT SECURITY SPECIALIST I |
|---|
| **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 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 & 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. |

| 20. IT SECURITY SPECIALIST II |
|---|
| **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. |

| 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 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. The office conducts independent and objective audits, evaluations, and investigations. 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 & other Government contractors in answering questions about Government property. |
| **Minimum Education:** Undergraduate degree desired. Four 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 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. Seven 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 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. Nine 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 i. 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. Five 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. One 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, 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 aspects 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. 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. Two 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 aspects 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. 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. Three years of direct Government contracting experience at task/project management level desired. Applicable Industry Certification desired.<br>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. Five 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. |

| 31. SECURITY MANAGER V |
|---|
| **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; 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. |
| **Minimum Education:** Undergraduate in an associated technical or management discipline, with a minimum of 14 years related specialized Security experience and 8 years management experience. With a Graduate degree, must have a minimum of 12 years related specialized experience and 6 years management experience. 7 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. |

| 32. SECURITY ADMINISTRATOR I |
|---|
| **Minimum/General Experience:** 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. |
| **Functional Responsibility:** 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. |
| **Minimum Education:** High school diploma or GED equivalent and 2 years general office experience required. Must have strong computer skills to include database experience, and possess a proficiency in data entry. Knowledge and ability to follow database guidelines. |

| 33. SECURITY ADMINISTRATOR II |
|---|
| **Minimum/General Experience:** Provide administrative and coordination support for a division or department. Provide general administrative support to the division manager, and maintains various administrative reports. |
| **Functional Responsibility:** 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. |
| **Minimum Education:** High school diploma or GED equivalent and 3 years specialized administrative experience required. Each year college can be substituted for 1 year of experience. Must be proficient with Microsoft Word; have basic skills with Excel and PowerPoint; and other database software experience desired. |

| 34. SECURITY ADMINISTRATOR III |
|---|
| **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. 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. |
| **Minimum Education:** Undergraduate degree and 3 years specialized administrative experience. Without a degree, must have 7 years of specialized administrative 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. |

| 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. 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 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 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. 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 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 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. 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. 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. 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. 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. 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. 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 & 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. 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. Experience must include 2 years supervising subordinate TSCM Specialists. Knowledge of automated information and on-line systems and tools. With 14 years of specialized experience a degree is not required. 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. |

| 46. IT SECURITY ANALYST I |
|---|
| **Minimum/General Experience:** In support of an IT Security Program will assist in the development, coordination and documenting plans, procedures and architecture to include Certification & Accreditation of systems, and NIST self-assessments. Assist in the development, promulgation, and review of security and policy elements for the IT Security Program. Assist in writing and testing contingency plans and disaster recovery plans. |
| **Functional Responsibility:** 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. Design, implement, document, and evaluate government computer security programs. Possess a general understanding of IT security requirements and demonstrated experience in IT security writing and presenting reports to executive level personnel. 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, NIST 800-53, NIST 800-30, NIST 800-34 and NIST-800-37 Rev 1, and other applicable Federal regulations and guidelines. Must have knowledge of FISMA and NIST Risk Management Framework (RMF). Proficient with Microsoft Office Suite. |
| **Minimum Education:** Undergraduate degree in related field and 4 years specialized experience. 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 possess a current clearance at the required contract level. |

| 47. IT SECURITY ANALYST II |
|---|
| **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. Assist in writing and testing contingency plans, disaster recovery plans and continuity of operations plans. Experience conducting risk assessments, privacy impact assessments and conducting ST&Es. Thorough understanding of and hands-on experience with computer operations and systems of various types as well as an understanding of computer security. |
| **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. Possess a general understanding of IT security requirements and demonstrated experience in IT security writing and presenting reports to executive level personnel. CISSP, CBCP, MBCP, CISA, CISM, 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, NIST 800-53 Rev 3, NIST 800-53A Rev 1, NIST 800-30, NIST 800-34 and NIST-800-37 Rev 1, NIST 800-60 Rev 1, NIST 800-137 and other applicable Federal regulations and guidelines. Must have knowledge of FISMA and NIST Risk Management Framework (RMF). Proficient with Microsoft Office Suite. Knowledge of security implications of HSPD-12, PKI, Active Directory, systems architecture, and related activities desired. Experience conducting FIPS 199 requirements analysis. |
| **Minimum Education:** Undergraduate degree in related field and 6 years specialized experience. 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 possess a current clearance at the required contract level. |

| 48. IT SECURITY ANALYST 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. Assist in writing and testing contingency plans and disaster recovery plans. Experience conducting risk assessments, privacy impact assessments and conducting ST&Es. Thorough understanding of and hands-on experience with computer operations and systems of various types as well as an understanding of computer security. |
| 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. Possess a general understanding of IT security requirements and demonstrated experience in IT security writing and presenting reports to executive level personnel. CISSP, CBCP, MBCP, CISA, CISM, 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; conducting NIST self assessments; demonstrated experience and/or in depth knowledge consistent with security principles and best practices as reflected in the NIST-800-18, OMB A-130, NIST 800-53 Rev 3, NIST 800-53A Rev 1, NIST 800-30, NIST 800-34 and NIST-800-37 Rev 1, NIST 800-60 Rev 1, NIST 800-137 and other applicable Federal regulations and guidelines. Must have knowledge of FISMA and NIST Risk Management Framework (RMF). Proficient with Microsoft Office Suite. Knowledge of security implications of HSPD-12, PKI, Active Directory, systems architecture, and related activities desired. Experience conducting FIPS 199 requirements analysis. |
| **Minimum Education:** Undergraduate degree in related field and 8 years specialized experience. 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 possess a current clearance at the required contract level. |

| 49. IT SECURITY ANALYST IV |
|---|
| **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. Assist in writing and testing contingency plans and disaster recovery plans. Experience conducting risk assessments, privacy impact assessments and conducting ST&Es. Thorough understanding of and hands-on experience with computer operations and systems of various types as well as an understanding of computer security. |
| **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. Possess a general understanding of IT security requirements and demonstrated experience in IT security writing and presenting reports to executive level personnel. CISSP, CBCP, MBCP, CISA, CISM or related industry certification required. 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; conducting NIST self assessments; demonstrated experience and/or in depth knowledge consistent with security principles and best practices as reflected in the NIST-800-18, OMB A-130, NIST 800-53 Rev 3, NIST 800-53A Rev 1, NIST 800-30, NIST 800-34 and NIST-800-37 Rev 1, NIST 800-60 Rev 1, NIST 800-137 and other applicable Federal regulations and guidelines. Must have knowledge of FISMA and NIST Risk Management Framework (RMF). Experience with designing, implementing, documenting, and evaluating government computer security programs. Experience with writing government computer security policy documentation. Proficient with Microsoft Office Suite. Knowledge of security implications of HSPD-12, PKI, Active Directory, systems architecture, and related activities desired. Experience conducting FIPS 199 requirements analysis. |
| **Minimum Education:** Undergraduate degree in related field and 10 years specialized experience. With 14 years of specialized experience a degree is not required. Minimum of 3-5 years of management/supervisory experience and a basic understanding of contract administration experience with the Federal Government. One year of college is equivalent to one year of experience. Any related industry certification can be substituted for one year of experience. Must possess a current clearance at the required contract level. |

| 50. IT SECURITY EXPERT – PROJECT MANAGER |
|---|
| **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. Experience in writing and testing contingency plans, disaster recovery plans and continuity of operations plans. Experience conducting risk assessments, privacy impact assessments and conducting ST&Es. |
| **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. Possess a general understanding of IT security requirements and demonstrated experience in IT security writing and presenting reports to executive level personnel. Direct the efforts of a team of 7-15 employees to ensure all contract requirements are satisfied; assign/review work; complete Performance Reviews and other management related tasks. Must have experience in conducting and writing Certification & Accreditation of systems, conducting NIST self-assessments, privacy impact assessments and risk 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, NIST 800-53, and NIST-800-37 Rev 1, and other applicable Federal regulations and guidelines. Must have knowledge of FISMA and NIST Risk Management Framework (RMF). Experience with designing, implementing, documenting, and evaluating government computer security programs. Experience with writing government computer security policy documentation. Proficient with Microsoft Office Suite. Knowledge of security implications of HSPD-12, PKI, Active Directory, systems architecture, and related activities desired. Experience conducting FIPS 199 requirements analysis. 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. |
| **Minimum Education:** Undergraduate degree in related field and 10 years specialized experience. Minimum of 6-8 years of management/supervisory experience and a basic understanding of contract administration experience with the Federal Government. 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, CISA, CISM or related industry certification required. Must possess a current clearance at the required contract level. |

| 51. IT SECURITY ENGINEER – PENETRATION TESTER |
|---|
| **Minimum/General Experience:** In support of the IT Security Program will perform tasks as part of a team to develop, coordinate and document plans, procedures and testing for the Security and Policy Program office to include Security Accreditation ( Certification & Accreditation) of systems, security testing, and annual security reviews, as well as, vulnerability scanning and penetration testing. |
| **Functional Responsibility:** Develop and write Security Accreditation (Certification and Accreditation) documentation, perform independent ST&E evaluations, and conduct annual security reviews in accordance with NIST Special Publication 800-37 Rev 1 and other NIST guidance. Perform vulnerability scanning and penetration testing using standard tools (Nmap, Nessus, Core Impact, NTO Spider, Burp Proxy, DISA SRR scripts). Develop and track corrective actions for audit findings and manage the POA&M reporting process for the agency. Develop and test disaster recovery / contingency plans and continuity of operation plans for IT systems. Develop and evaluate plans, principles, and procedures for accomplishing customer IT security studies and provide professional analysis of methods and objectives. Assist in the collection and presentation of security documentation in response to audit requirements. 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. Evaluate and analyze the critical technology processing needs of the related services. Review policy documents issued by the Federal Agency and assist in transferring policy requirements into various templates. Research, develop, document, and implement tracking and inventory methodologies for maintaining inventory of critical assets (human resources, hardware, and software). Must have experience in conducting and writing Certification & Accreditation (C&A) of systems; conducting Security Tests and Evaluations (ST&E); writing and testing contingency plans/disaster recovery plans; conducting NIST self-assessments, privacy impact assessments and risk assessments. Must have demonstrated experience and/or in depth knowledge consistent with security principles and best practices as reflected in the NIST 800-37 Rev 1, NIST 800-53 Rev 3, NIST 800-53A Rev 1, NIST-800-18, NIST 800-30, NIST 800-34 Rev 1, NIST 800-60 Rev1, NIST 800-137. OMB A-130, FISMA requirements, and other applicable Federal regulations and guidelines. Must have knowledge of FISMA and NIST Risk Management Framework (RMF). Experience with designing, implementing, documenting, and evaluating and testing government computer security programs. Experience with writing government computer security policy documentation. Proficient with Microsoft Office Suite to prepare all documents and presentations in their final form. Knowledge of security implications of HSPD-12, PKI, Active Directory, systems architecture, and related activities desired. Must have a general understanding of IT security requirements and demonstrated experience in IT security writing and presenting reports to executive level personnel. Experience conducting FIPS 199 requirements analysis. Familiarity with RSAM is a plus. |
| **Minimum Education:** Undergraduate degree in related field and 6 years specialized experience. 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. CISSP, CEH, CISA, CISM or related industry certification required. Must possess a current clearance at the required contract level. |

| 52. RF ENGINEER [DIGITAL] |
|---|
| **Minimum/General Experience:** Responsible for leading the radio frequency (RF) engineering staff in evaluating new Original Equipment Manufacturers (OEM) RF technologies, both hardware and software based radios and information technologies found in the general office environment and for the mobile employee. Responsible for the evaluation of new technologies to include RF and optical, providing technical reports to senior government officials, as well as highlighting possible security vulnerabilities while making appropriate recommendations. Conduct open source research on emergent technologies. Report on vulnerabilities and potential countermeasures. Generate RF environment baselines (worldwide). |
| **Functional Responsibility:** Document selected vulnerabilities via laboratory testing. Assisting in the drafting and review of technical security policies and guidelines involving state of the art information technologies and its implementation in Department of State resources. Responsible for gathering information on new technologies and any previous associated research found on those technologies, identify emanations found not previously recognized, and to implement and maintain a database of signal parameters for future easy recognition. Assist in various laboratory testing to determine the vulnerabilities associated with, but not limited to GSM, GPRS, CDMA, IEEE 802.15, IEEE 802.11a/b/g/n/ac (Wi-Fi), Free Space Optical (FSO) and Radio Frequency Identification (RFID) technologies. Knowledge of modulation schemes and types. Awareness of Intelligence Community as well as a familiarity with various agency specific policies. |
| **Minimum Education:** Five years of radio frequency (RF) work experience with a Bachelor's Degree or higher in Electrical Engineering or similar field; or at least ten years of equivalent RF work experience. Desired experience in advanced radio wave propagation theory, digital communication systems and bit-stream analysis. Familiarity with new and emerging mobile information technologies. SIGINT or Signal Analyst experience. Familiarity with cryptography and the best security practices for computer networks and mobile computers. Must possess a current clearance at the required contract level. |

| 53. SR. RF ENGINEER [DIGITAL] |
|---|
| **Minimum/General Experience:** Team Lead for RF Countermeasures section. Oversees and directs team responsible for the installation and lifecycle maintenance of RF systems at facilities. Team builds and configures RF systems and test equipment to ensure functionality. Ensures interoperability of highly technical equipment through the management of hardware and software configuration changes. |
| **Functional Responsibility:** Provides technical support for all phases of RF systems, which includes pre-installation, installation, and post installation. Coordinates all reporting, including pre- and post-trip reports and Engineering Security Services Reports (ESSRs). Focuses primarily on RF emanations. Responsible for evaluating new technologies, documenting capabilities, and highlighting possible limitations, and making appropriate recommendations. Trains agency personnel on the identification, analysis, and recognition of signals of interest. Conducts research on emergent technologies. Generates RF environment baselines. Documents selected vulnerabilities via laboratory testing. Assists in drafting and review of technical security policies and guidelines involving state of the art information technologies and their implementation in agency's resources. Responsible for gathering information on new technologies and any previous associated research found on those technologies, identifying emanations that were found but not previously recognized, and for implementing and maintaining a database of signal parameters for easy future recognition. Works with other Agency organizations to determine and understand the vulnerabilities associated with, but not limited to, GSM, GPRS, CDMA, IEEE 802.15, IEEE 802.11a/b/g/n/ac (Wi-Fi), Free Space Optical (FSO) and Radio Frequency Identification (RFID) technologies. Coordinates travel, ECC, and other travel documents. Assists in identifying and developing equipment upgrades and platform replacements. Performs surveys for new installations at existing facilities. Develops and administers user training for multiple existing and new systems. |
| **Minimum Education:** Six years of radio frequency (RF) work experience and an undergraduate degree or higher in Electrical Engineering or a similar field, or at least ten years of equivalent RF work experience. TEMPEST Level II certification is recommended. One year of management experience. Must possess a current clearance at the required contract level. |

| 54. INTELLIGENCE ANALYST |
|---|
| **Minimum/General Experience:** Provide intelligence analysis in support of a security project. Will work in coordination with multi-jurisdictional investigations. The office is a centralized data warehouse, generating intelligence products to provide detailed information and in-depth analysis to law enforcement agencies in support of investigations. |
| **Functional Responsibility:** Provides specialized intelligence and threat analysis and production support in areas of counterterrorism, cybersecurity, counterdrug, travel and science. Accesses and performs research using designated automated intelligence databases for identifying information of interest to the customer, downloading the identified information to an appropriate medium, and editing the information into format(s) to be specified by the customer. Maintain working relationships to coordinate with agents and analysts from multiple federal law enforcement agencies. Provide intelligence and threat analysis of the information that is tailored to the customer's requirements. Develop documents, summaries, reports, and presentations. Present briefings to key personnel. A major portion of this work involves research, interpreting investigation information and report writing. Perform special assignments or projects as directed. |
| **Minimum Education:** Three years of general experience in analysis with federal, state, or local government agency, law enforcement agency, or private industry Undergraduate degree desired. Two years of experience writing Intelligence reports and obtaining data from various sources and compiling the data into reports Proficient in general Microsoft Word processing software. Must have demonstrated excellent written and oral communications skills, and the ability to interact with individuals at all levels. Certifications in Intelligence programs. Must possess a current clearance at the required contract level. |

## ORDERING INFORMATION

For additional information and to receive a formal quotation please contact:

Cathy Ebner
Director, Contracts
Advanced Resource Technologies, Inc. (ARTI)
1555 King Street, Suite 200
Alexandria, VA 22314
703-682-4764
cathy.ebner@team-arti.com