The Contractor will be awarded under the cooperative purchasing program and disaster recovery for the awarded SIN: 54151HACS

Special Item Number 54151HACS: Highly Adaptive Cybersecurity Services (HACS)
FSC Classes/Product Codes: FSC/PSC Class D310 IT And Telecom- Cyber Security And Data Backup

Global Networks, Inc
6460 Dobbin Road, Suite A
Columbia, MD 21045
Phone: 301-741-4315
https://www.gn-inc.com/
Contract Administrator: Andre Shelton
E-Mail: ashelton@gn-inc.com

Contract Number: 47QTCA20D0070

SBA Certified Small Disadvantaged Business, Woman-Owned Small Business

Price List current through Modification PS-0003, effective August 21, 2020

Period Covered by Contract: March 6, 2020 through March 5, 2025

For more information on ordering from Federal Supply Schedules click on the FSS Schedules button at: http://fss.gsa.gov/. On-line access to contract ordering information, terms and conditions, up-to-date pricing, and the option to create an electronic delivery order is available through GSA Advantage!, a menu-driven database system. The INTERNET address for GSA Advantage! is http://www.gsaadvantage.gov
CUSTOMER INFORMATION

1a. Table of awarded special item numbers with appropriate cross-reference to item descriptions and awarded prices.

   *Special Item Number 54151HACS*

1b. Identification of the lowest priced model number and lowest unit price for that model for each special item number awarded in the contract. This price is the Government price based on a unit of one, exclusive of any quantity/dollar volume, prompt payment, or any other concession affecting price. Those contracts that have unit prices based on the geographic location of the customer, should show the range of the lowest price, and cite the areas to which the prices apply.

   *See Approved GSA Pricing*

1c. If the Contractor is proposing hourly rates, a description of all corresponding commercial job titles, experience, functional responsibility and education for those types of employees or subcontractors who will perform services shall be provided.

   *See subsequent pages below*

2. Maximum order.

   $500,000

3. Minimum order.

   $100

4. Geographic coverage.

   *The Geographic Scope of Contract will be domestic delivery (50 States, DC and US Territories).*

5. Point of production.

   *Same as contractor*

6. Discount from list prices or statement of net price.

   *Prices shown are NET Prices; Basic Discounts have been deducted.*

7. Quantity discounts.

   +1%, for task orders over $500,000

8. Prompt payment terms.

   *0% - net 30 days from receipt of invoice or date of acceptance, whichever is later. Information for Ordering Offices: Prompt payment terms cannot be negotiated out of the contractual agreement in exchange for other concessions.*

9a. The Government purchase Card will be accepted for payment on orders below the micro-purchase threshold.

9b. The Government purchase Card will be accepted for payment on orders above the micro-purchase threshold.

10. Foreign items.

   *Not Applicable*
11a. Time of delivery.
*SPECIAL ITEM NUMBER*  
*DELIVERY TIME (Days ARO)*

<table>
<thead>
<tr>
<th>Item Code</th>
<th>Delivery Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>54151HACS</td>
<td>As Negotiated</td>
</tr>
</tbody>
</table>

11b. Expedited Delivery. The Contractor will insert the sentence “Items available for expedited delivery are noted in this price list.” under this heading. The Contractor may use a symbol of its choosing to highlight items in its price lists that have expedited delivery.
*As negotiated on the task order level.*

11c. Overnight and 2-day delivery. The Contractor will indicate whether overnight and 2-day delivery are available. Also, the Contractor will indicate that the schedule customer may contact the Contractor for rates for overnight and 2-day delivery.
*As negotiated on the task order level.*

11d. Urgent Requirements. The Contractor will note in its price list the “Urgent Requirements” clause of its contract and advise agencies that they can also contact the Contractor’s representative to effect a faster delivery.
*As negotiated on the task order level.*

12. F.O.B. point.
*Destination*

13a. Ordering address.
*Same as contractor*

13b. Ordering procedures: For supplies and services, the ordering procedures, information on Blanket Purchase Agreements (BPA’s) are found in Federal Acquisition Regulation (FAR) 8.405-3.

14. Payment address.
*Same as contractor*

15. Warranty provision.
*Not Applicable*

16. Export packing charges, if applicable.
*Not Applicable*

17. Terms and conditions of Government purchase card acceptance (any thresholds above the micro-purchase level).
*None*

18. Terms and conditions of rental, maintenance, and repair are *not applicable.*

19. Terms and conditions of installation are *not applicable.*

20. Terms and conditions of repair parts are *not applicable.*

20a. Terms and conditions for any other services.
*Not applicable*
21. List of service and distribution points: not applicable.

22. List of participating dealers is not applicable.

23. Preventive maintenance is not applicable.

24a. Special attributes such as environmental attributes (e.g., recycled content, energy efficiency, and/or reduced pollutants): Not applicable.

24b. If applicable, indicate that Section 508 compliance information is available on Electronic and Information Technology (EIT) supplies and services and show where full details can be found (e.g., contractor’s website or other location.) The EIT standards can be found at: www.Section508.gov/. https://www.gn-inc.com/

25. Data Universal Number System (DUNS) number: 802975305

26. Notification regarding registration in SAM.gov database: Registration is Current and Valid (Cage Code: 4ZWG4)
Terms and Conditions for all IT Contractors

1) Organizational Conflicts Of Interest
   a) Definitions.
      i) "Contractor" means the person, firm, unincorporated association, joint venture, partnership, or corporation that is a party to this contract.
      ii) "Contractor and its affiliates" and "Contractor or its affiliates" refers to the Contractor, its chief executives, directors, officers, subsidiaries, affiliates, subcontractors at any tier, and consultants and any joint venture involving the Contractor, any entity into or with which the Contractor subsequently merges or affiliates, or any other successor or assignee of the Contractor.
      iii) An "Organizational conflict of interest" exists when the nature of the work to be performed under a proposed ordering activity contract, without some restriction on ordering activities by the Contractor and its affiliates, may either (i) result in an unfair competitive advantage to the Contractor or its affiliates or (ii) impair the Contractor's or its affiliates' objectivity in performing contract work.
   b) To avoid an organizational or financial conflict of interest and to avoid prejudicing the best interests of the ordering activity, ordering activities may place restrictions on the Contractors, its affiliates, chief executives, directors, subsidiaries and subcontractors at any tier when placing orders against schedule contracts. Such restrictions shall be consistent with FAR 9.505 and shall be designed to avoid, neutralize, or mitigate organizational conflicts of interest that might otherwise exist in situations related to individual orders placed against the schedule contract. Examples of situations, which may require restrictions, are provided at FAR 9.508

2) Services Performed
   a) All services performed by the Contractor under the terms of this contract shall be as an independent Contractor, and not as an agent or employee of the ordering activity.
   b) The Contractor shall commence performance of services on the date agreed to by the Contractor and the ordering activity.
   c) The Contractor agrees to render services only during normal working hours, unless otherwise agreed to by the Contractor and the ordering activity.

3) Travel.
   a) Any contractor travel required in the performance of services must comply with the Pub. L.99-234 and FAR Part 31.205-46, as applicable, in effect on the date(s) the travel is performed. Established Federal Government per diem rates will apply to all Contractor travel.

4) Warranty
   a) Unless otherwise specified in this contract, the Contractor's standard commercial warranty as stated in the contract's commercial pricelist will apply to this contract.
   b) The Contractor's commercial guarantee/warranty shall be included in the Commercial Supplier Agreement to include Enterprise User License Agreements or Terms of Service (TOS) agreements, if applicable.
   c) Except as otherwise provided by an express or implied warranty, the Contractor will not be liable to the ordering activity for consequential damages resulting from any defect or deficiencies in accepted items.
Terms and Conditions for SIN 54151HACS Highly Adaptive Cybersecurity Services (HACS)

1. Only IT Professional Highly Adaptive Cybersecurity Services (HACS) shall be offered under this special item number. The following are the approved subcategories:
   • High Value Asset (HVA) Assessments;
   • Risk and Vulnerability Assessments (RVA),
   • Cyber Hunt,
   • Incident Response, and
   • Penetration Testing

2. Resumes shall be provided to the GSA contracting officer or the ordering activity upon request.

3. Services offered SIN 54151HACS shall be in accordance with the following laws and standards when applicable to the specific task orders, including but not limited to:
   o Federal Acquisition Regulation (FAR) Part 52.204-21
   o OMB Memorandum M-17-12 - Preparing for and Responding to a Breach of Personally Identifiable Information (PII)
   o OMB Memorandum M-19-03 - Strengthening the Cybersecurity of Federal Agencies by enhancing the High Value Asset Program
   o 2017 Report to the President on Federal IT Modernization
   o The Cybersecurity National Action Plan (CNAP)
   o NIST SP 800-14 - Generally Accepted Principles and Practices for Securing Information Technology Systems
   o NIST SP 800-27A - Engineering Principles for Information Technology Security (A Baseline for Achieving Security)
   o NIST SP 800-30 - Guide for Conducting Risk Assessments
   o NIST SP 800-55 - Guide to Information Technology Security Services
   o NIST SP 800-44 - Guidelines on Securing Public Web Servers
   o NIST SP 800-48 - Guide to Securing Legacy IEEE 802.11 Wireless Networks
   o NIST SP 800-53 – Security and Privacy Controls for Federal Information Systems and Organizations
   o NIST SP 800-61 - Computer Security Incident Handling Guide
   o NIST SP 800-64 - Security Considerations in the System Development Life Cycle
   o NIST SP 800-82 - Guide to Industrial Control Systems (ICS) Security
   o NIST SP 800-86 - Guide to Integrating Forensic Techniques into Incident Response
   o NIST SP 800-115 - Technical Guide to Information Security Testing and Assessment
   o NIST SP 800-128 - Guide for Security-Focused Configuration Management of Information Systems
   o NIST SP 800-137 - Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations
   o NIST SP 800-153 - Guidelines for Securing Wireless Local Area Networks (WLANs)
   o NIST SP 800-160 - Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems
   o NIST SP 800-171 - Protecting Controlled Unclassified Information in non-federal Information Systems and Organizations.

4. The below is a list of IT Professional Service HACS/Labor Categories being offered:
   Please see page 9 for a list of services offered.
## GSA HOURLY RATES

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>54151HACS</td>
<td>Security Operations Specialist</td>
<td>$123.22</td>
<td>$126.30</td>
<td>$129.46</td>
<td>$132.69</td>
<td>$136.01</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Senior Engineer</td>
<td>$101.83</td>
<td>$104.38</td>
<td>$106.99</td>
<td>$109.66</td>
<td>$112.40</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Engineer</td>
<td>$86.34</td>
<td>$88.50</td>
<td>$90.71</td>
<td>$92.98</td>
<td>$95.30</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Associate Engineer</td>
<td>$71.74</td>
<td>$73.53</td>
<td>$75.37</td>
<td>$77.25</td>
<td>$79.18</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Project Manager</td>
<td>$160.43</td>
<td>$164.44</td>
<td>$168.56</td>
<td>$172.77</td>
<td>$177.09</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Engineer II</td>
<td>$111.86</td>
<td>$114.66</td>
<td>$117.53</td>
<td>$120.46</td>
<td>$123.48</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Engineer III</td>
<td>$134.87</td>
<td>$138.24</td>
<td>$141.70</td>
<td>$145.24</td>
<td>$148.87</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Engineer IV</td>
<td>$161.85</td>
<td>$165.89</td>
<td>$170.04</td>
<td>$174.29</td>
<td>$178.65</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Subject Matter Expert I</td>
<td>$140.26</td>
<td>$143.77</td>
<td>$147.36</td>
<td>$151.05</td>
<td>$154.82</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Subject Matter Expert II</td>
<td>$160.43</td>
<td>$164.44</td>
<td>$168.56</td>
<td>$172.77</td>
<td>$177.09</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Subject Matter Expert III</td>
<td>$242.76</td>
<td>$248.83</td>
<td>$255.05</td>
<td>$261.43</td>
<td>$267.97</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Information Assurance Engineer</td>
<td>$168.95</td>
<td>$173.17</td>
<td>$177.50</td>
<td>$181.94</td>
<td>$186.48</td>
</tr>
</tbody>
</table>
LABOR CATEGORY DESCRIPTIONS

Security Operations Specialist
Experience: 5 years minimum
Education Minimum: Bachelor’s Degree
Certification: CISSP, CISM, or PMP
Responsibilities: Conducts quality control in clients’ system management tools. Primary point of contact for the customer on project/program related details. Ensures quality and timeliness of client deliverables. Supports positive client/team relationships. Develops methodologies and provides recommendations for continuous improvements in Information Technology (IT), Penetration Testing, Incident Response, Cyber Hunt, and Risk and Vulnerability Assessment (RYA) Support Services in compliance with FISMA, DIACAP, DCID, NIST 800 SP, FIPS, ISO, and other statutory and client requirements. Meets with clients and staff to coordinate efforts, resolve conflicts, and provide guidance to meet project requirements. Evaluates proposed solutions to determine technical and functional feasibility and adequacy, and cost for implementation and operation. Provides in-depth knowledge and insight, technical experience and subject-matter expertise (SME) to help solve complex problems. Ensures tasks are adequately planned and implemented. Manages contractors and subcontractors work policies, purposes, goals, standards, contractor schedules, discrepancies, and disputes.

Senior Engineer
Experience: 3 years minimum
Education Minimum: Bachelor’s Degree
Certification: CISSP, CISM, CISA, or equivalent
Responsibilities: Provides clients in-depth knowledge and insight, guidance and support on management for internal and external systems related to information assurance, security engineering, telecommunications engineering, security control assessors, penetration testing, security training, network security, incident response, contingency planning, risk management, policy, guidelines, procedures, data loss prevention, change management tasks. Tracks task status, interfaces with clients, conducts analysis and evaluation of multiple systems, tasks and assignments using automated support tools. Monitors systems through the development life-cycle. Conducts and monitors scanning, testing, interviews, and document development. Collaborates with clients to ensure compliance with FISMA, NIST SPs, OMB Circular A-130, ISO DIACAP, DCID standards, and other required policy, regulations, procedures and guidelines. Conducts quality control checks of the client system assessment tool. Manages vulnerabilities from identification (assessment) to remediation (Plan of Action and Milestones (POA&M)) phase. Completes daily, weekly, monthly, quarterly, and annual reports and presentations to clients. Develops security training for client and tracks training. Monitors blacklist and whitelist to provide recommendations for COTS. Evaluates proposed automated solutions to determine technical and functional feasibility and adequacy, and cost for implementation and operation. Assists with system design, quality assurance, testing and customer training. Maintains records of security monitoring and incident response activities, utilizing case management and ticketing technologies. Monitors and analyzes Security Information and Event Management (SIEM) to identify security issues for remediation. Provides client recommendations based on thorough analysis of threat assessment, vulnerability analysis, risk assessment, information gathered, and evaluation of packets and logs.
Engineer

Experience: 1 year minimum

Education Minimum: Bachelor’s Degree

Certification: Security+, CAP, or equivalent

Responsibilities: Provides client support on internal and external systems in compliance with FISMA DIAQCAP, NIST 800 SPs, ISO, DCID and required governance. Monitors systems through the development life-cycle. Performs analysis, assessments, tests, and evaluation of existing or proposed processes, applications, systems. Researches, drafts, reviews, edits and provides input to operating policy and procedures. Recommends and assists clients with remediation effort. Creates and submits data for client deliverables. Collaborates with system stakeholders on completion of system artifacts and POA&Ms. Plan of Action and Milestones (POAM), manage and track completion dates for POAM items, assemble remediation packages for POAM items and perform remediation of findings involving security program compliance. Conducts scanning, compliance cross-checking, continuous monitoring, penetrating testing, security control assessments, patching, mitigation, creates security authorization reports, conducts interviews, tests software, and generates the formal report to deliver to the client. Completes daily, weekly, and monthly reports and presentations to clients. Updates security training for client and tracks training. Manages and tracks access/ account control process including collecting, distributing, tracking and storing access request forms, perform annual user revalidation documentation updates. Monitors blacklist and whitelist to provide recommendations for COTS. Evaluates proposed automated solutions to determine technical and functional feasibility and adequacy, and cost for implementation and operation. Assists with system design, quality assurance, testing and customer training. Maintains records of security monitoring and incident response activities, utilizing case management and ticketing technologies. Monitors and analyzes SIEM and updates report for submission to client. Provides client recommendations based on thorough analysis of threat assessment, vulnerability analysis, risk assessment, information gathered, and evaluation of packets and logs. Performs hunting activities and live response data collection and analysis to search the network for indicators of compromise and hosts during investigation. Helps determine the extent of the compromise, attributes of any malware and possible data exfiltrated.

Associate Engineer

Experience: 1 year minimum

Education: Associate Degree

Certification: Not required

Responsibilities: Provides client support on internal and external systems in compliance with FISMA DIAQCAP, NIST 800 SPs, ISO, DCID and required governance. Monitors systems through the development life-cycle. Assists with the performance of analysis, assessments, tests, and evaluation of existing or proposed processes, applications, systems. Researches, drafts, reviews, edits and provides input to operating policy and procedures. Assists in providing client recommends and remediation effort. Collaborates with system stakeholders on completion of system artifacts, POA&M completion dates, assembly of remediation packages, and perform remediation of findings involving security program compliance. Conducts scanning, compliance cross-checking, continuous monitoring, penetrating testing, security control assessments, patching, mitigation, creates security authorization reports, conducts interviews, tests software, and generates the formal report to deliver to the client. Completes data for inclusion in the daily, weekly, and monthly reports and presentations to clients. Updates security training for clients and tracks training. Track access/account control process including collecting, distributing, tracking and storing access request forms, perform annual user revalidation documentation updates. Monitors blacklist and whitelist to provide recommendations for COTS. Assists with system design, quality assurance, testing and customer training. Maintains records of security monitoring and incident response activities, utilizing case management and ticketing technologies. Monitors and analyzes SIEM
and updates report for submission to client. Provides client recommendations based on thorough analysis
of threat assessment, vulnerability analysis, risk assessment, information gathered, and evaluation of
packets and logs. Performs hunting activities and live response data collection and analysis to search the
network for indicators of compromise and hosts during investigation. Helps determine the extent of the
compromise, attributes of any malware and possible data exfiltrated. Gathers, analyzes, edits, and prepares
technical information for submission to the client. Conducts research and ensures the use of proper
technical terminology and documentation standards. Translates technical information into readable
documents. Assists in the preparation of presentation graphics and supports the development of contract
deliverables and reports.

**Project Manager**

**Experience:** 5 years minimum  
**Education Minimum:** Bachelor’s Degree  
**Certification:** None  
**Responsibilities:** The Project Manager has the primary responsibility to plan, track, and manage projects
to which they are assigned to success. He/she will identify key stakeholders and help define the project
scope, objectives and expectations. The Project Manager manages projects according to the clients-approved project frameworks, including both Agile and traditional project management approaches. He/she must be able to take an active senior leadership role in the team and create an environment that fosters the prescribed agile methods and processes. Finally the Project Manager must be able to identify issues proactively, resolve conflicts, escalate if necessary, and work across the organization to execute the project.

**Engineer II**

**Experience:** 5 years minimum  
**Education Minimum:** Bachelor’s Degree  
**Certification:** None  
**Responsibilities:** Responsible for supporting hardware configurations, installing software, managing
network systems, and training staff on correct operating procedures. Extensive experience maintaining
large-scale computer systems. Must have excellent troubleshooting skills and have the capability to
support senior engineering personnel in testing control apparatus using IT tools. May direct field
operations and support in systems integrations.

**Engineer III**

**Experience:** 7 years minimum  
**Education Minimum:** Bachelor’s Degree  
**Certification:** None  
**Responsibilities:** Works with clients to ensure that project goals are aligned. Supports quality assurance
and troubleshooting during the lifecycle of the project. Responsible for designing hardware configurations,
installing software, managing network systems, and training staff on correct operating procedures. Designs
and integrates systems utilizing research and development. Must have extensive experience maintaining
large-scale computer systems, have excellent troubleshooting skills and the capability to direct engineering
personnel in testing control apparatus using IT tools. May direct field operations and support in systems
integrations.
Engineer IV
Experience: 15 years minimum
Education Minimum: Bachelor’s Degree
Certification: None
Responsibilities: Manages the full lifecycle of projects, ensuring that they fall within budget and on schedule. Works with clients to ensure that project goals are aligned. Supports quality assurance and troubleshooting during the lifecycle of the project. Responsible for writing proposals, funding and approving project budgets and represent the organization while presenting at conferences about their specific work. Researches, develops, designs, and testing processes, products, and systems for commercial, industrial, medical, military, and scientific applications, applying principles and techniques of systems engineering: Designs electronic components and integrated systems, utilizing ferroelectric, nonlinear, dielectric, phosphorescent, photoconductive, and thermoelectric properties of materials, and directs engineering personnel in fabrication of test control apparatus and equipment. May direct field operations and maintenance of IT Systems.

Subject Matter Expert I
Experience: 5 years minimum
Education Minimum: Bachelor’s Degree
Certification: None
Responsibilities: Responsible for serving as facilitator for defining/ameliorating the policies and procedures of an organization, process or program. Utilizes their specialization and subject matter knowhow to assist the business analysts and Project Managers in developing a secure environment and defining the security requirements and best practices. The Subject Matter Expert (SME) functions as the organizational ambassador for his knowledge area and applies his/her expertise to support an organization’s vision.

Subject Matter Expert II
Experience: 10 years minimum
Education Minimum: Bachelor’s Degree
Certification: None
Responsibilities: The SME II is responsible for leading a workstream of change management and communications experts to develop a change management strategy and communications plan. The SME assesses change readiness, leadership alignment, and organizational impact. Articulates a change vision and strategy and recommends training strategies. The SME conducts stakeholder analysis and communications to obtain awareness, understanding, buy-in, and support. Defines project workflows, manages resources, prioritizing responsibilities and tasks in order to deliver quality and timely results. Proactively engages with clients to identify challenges, recommend solutions and manage expectations. Designs appropriate analysis for diagnostics and implementation, analyzing and interpreting ambiguous and complex information and relationships. Prepares final drafts of major deliverables ensuring quality control. Anticipates client needs, recognizes and acts on opportunities to enhance client services and expand the scope of engagement.
Subject Matter Expert III  
**Experience:** 15 years minimum  
**Education Minimum:** Bachelor’s Degree  
**Certification:** None  
**Responsibilities:** The SME III is the definitive source responsible for managing and assessing compliance with the IS Policy to include the Disaster Recovery Policy for client organizations. Responsible for ensuring that the organization networks and information is secure at all times by constantly monitoring intrusion detection, data encryption, and taking quick and effective corrective measures in the event of a breach. Provides technical knowledge and analysis of information assurance including applications, operating systems, Internet and Intranet, physical security, networks, risk assessment, critical infrastructure continuity and contingency planning, emergency preparedness, security awareness and training. Provides analysis of existing system's vulnerabilities to possible intrusions, resource manipulation, resource denial and destruction of resources. Provides technical support and analysis to document organizational information protection framework and supports policy and procedures preparation and implementation. 

Information Assurance Engineer  
**Experience:** 5 years minimum  
**Education Minimum:** Bachelor’s Degree  
**Certification:** None  
**Responsibilities:** The Information Assurance Engineer is responsible for assessing compliance with the IS Policy including the Disaster Recovery Policy for client organizations. Responsible for ensuring that the organization networks and information is secure at all times by constantly monitoring intrusion detection, data encryption, and taking quick and effective corrective measures in the event of a breach. Provides technical knowledge and analysis of information assurance, to include applications, operating systems, Internet and Intranet, physical security, networks, risk assessment, critical infrastructure continuity and contingency planning, emergency preparedness, security awareness and training. Provides analysis of existing system's vulnerabilities to possible intrusions, resource manipulation, resource denial and destruction of resources. Provides technical support and analysis to document organizational information protection framework and supports policy and procedures preparation as well as implementation. 

Monitor firewall logs. Analyzes the client system security, conducts gap analysis, determines enterprise information security standards, and develops and implements information security standards and procedures. Ensures that all information systems are functional and secure.
### SUBSTITUTION CHART

<table>
<thead>
<tr>
<th>Experience</th>
<th>Equals</th>
<th>Degree</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 years</td>
<td></td>
<td>Associates Degree</td>
</tr>
<tr>
<td>4 years</td>
<td></td>
<td>Bachelor’s Degrees</td>
</tr>
<tr>
<td>6 years</td>
<td></td>
<td>Master’s Degree</td>
</tr>
<tr>
<td>8 years</td>
<td></td>
<td>Ph.D</td>
</tr>
<tr>
<td>Associates</td>
<td></td>
<td>2 years of additional relevant experience</td>
</tr>
<tr>
<td>Bachelor’s</td>
<td></td>
<td>4 years of additional relevant experience</td>
</tr>
<tr>
<td>Master’s</td>
<td></td>
<td>6 years of additional relevant experience</td>
</tr>
<tr>
<td>Ph.D</td>
<td></td>
<td>8 years of additional relevant experience</td>
</tr>
</tbody>
</table>

*Substitution Methodology: Due to the availability or limitation of education, occasionally substitution of experience as referenced above for a professional labor type with additional years of experience will be provided to the Federal Agency when responding to their IT requirements and it is solely the acquiring agency’s determination, if the substitution is considered acceptable prior to an award.*