# *Federal Government*

# *Market Research*

# *FY 2026*

*Prepared by Offeror:*

**DELNOVAK**
**260 Peachtree St Nw Ste 2200**
**Atlanta, GA 30303**
**CAGE: 65KF1 UEI: G8NRKTDRGED3**
**P: (678) 910-4412**
**E: emmanuel@delnovak.com**
**URL: http://www.delnovak.com**

**CMMC LEVEL 1 & 2 CERTIFIED**

***This proposal includes data that shall not be disclosed outside the Government agency or commercial organization and shall not be duplicated, used, or disclosed in whole or in part for any purpose other than to evaluate this request. If, however, a contract is awarded to this offeror because of or in connection with the submission of this data, the Government or commercial organization shall have the right to duplicate, use, or disclose the data to the extent provided in the resulting contract. This restriction does not limit the right to use information contained in this data if it is obtained from another source without restriction. The data subject to this restriction are contained on all pages.***

## TABLE OF CONTENTS

| | |
|---|---|
| **Introduction / Request for set-aside** | **2** |
| **Company Information** | **3** |
| **Past Performance** | **3** |
| **Capability Statement** | **17** |

# Introduction / Request for set-aside

Introduction / Request for set-aside
DELNOVAK
260 Peachtree St Nw Ste 2200
Atlanta, GA 30303
CAGE: 65KF1 UEI: G8NRKTDRGED3
P: (678) 910-4412
E: emmanuel@delnovak.com
URL: http://www.delnovak.com

**Subject:** DELNOVAK Response to Federal Government Market Research Package – 2026.

DELNOVAK is pleased to present our Market Research Package for FY 2026, we respectfully request that our response be included in the Government's market research or 8(a) award for this project.

At DelNovak, we are driven by a commitment to innovation and excellence in technology and engineering. With a team of skilled engineers and technology experts, we specialize in creating advanced, efficient, and reliable systems and structures tailored to meet the unique needs of our clients.

DelNovak is highly experienced in enabling government agencies and corporate enterprises to reduce operational and business risks while ensuring full regulatory compliance.

Our Mission is to develop cutting-edge solutions that empower businesses and industries to thrive in an ever-evolving digital world.

Beyond business, we are dedicated to social responsibility, with a focus on humanitarian efforts – particularly through our involvement with Rotary International, Shriners Children's and Scottish Rite Hospital for Children.

We offer the capability of procuring services that are high quality, demonstrating best value to the government, and procured in a condensed timeframe, as we are eligible under the SBA 8(a) program, and are **CMMC Level 1 & 2 certified.** We ask that you consider making this small business set aside. As a Small Business Administration (SBA) 8(a) and HUBZone certified, we encourage your office to consider procuring these services through the SBA 8(a) program or as a sole source award, which offers speed, efficiency, and flexibility.

Emmanuel Ogidigben
President & CEO

# Company Information

| | |
|---|---|
| **Company Name:** | DelNovak |
| **Company Address:** | 260 Peachtree St Nw Ste 2200<br>Atlanta, GA 30303 |
| **Point of Contact** | Emmanuel Ogidigben<br>emmanuel@delnovak.com |
| **Website** | http://www.delnovak.com |
| **CAGE Code** | 65KF1 |
| **UEI** | G8NRKTDRGED3 |
| **NAICS:** | 541330, 541511, 541512, 541513, 541519, 541611, 541614, 541618, 541690, 541990, 561110, 561210, 561320, 561920, 561990, 611420, 611430, 236220 |
| **Business Classification/Status** | Small Business, SBA 8(a), HUBZone, Small Disadvantaged Business |
| **Facility Clearance Level** | N/A |

# Past Performance

**Reference 1: Enterprise Cybersecurity and Program Management**

| | |
|---|---|
| **Contract Name** | Enterprise Cybersecurity and Program Management<br>Metropolitan Atlanta Rapid Transit Authority (MARTA) |
| **Contracting Agency** | Gantec Corporation |
| **Contract Number** | 201810027 |
| **Award Date** | 04/2019 |
| **Contract Type** | Firm Fixed Price (FFP) |
| **Contract Total Dollar Value** | $2,600,000 |
| **Period of Performance** | 04/2019 - Present |
| **Prime or Subcontractor** | Subcontractor |
| **Major Subcontractors** | *N/A* |
| **Place of Performance** | Atlanta Georgia |
| **Procuring Contracting Officer POC** | Venkat Ravilla<br>CEO<br>vr@gantecusa.com |

| | |
|---|---|
| | 847 372 7802 |

**Summary**

DelNovak is contracted to assist on a mission critical problem; an agency-wide development and implementation of a Cybersecurity Program based on the NIST Cybersecurity and Risk Management Frameworks for the transit agency in alignment with the National Cybersecurity and Critical Infrastructure Protection Act, Department of Homeland Security (DHS) and Federal Transit Authority (TSA) directives, including Payment Card Industry Data Security Standard (PCI-DSS) requirements. Support scope includes enterprise, train control and police department networks.

Support services include; risk and vulnerability assessment. third-party risk assessment. PCI-DSS annual compliance audit support. Penetration testing and Threat Intelligence support working with the Department of Homeland Security and other government agencies.

On this engagement, DelNovak works directly with the CISO, CIO, and AGM of Internal Audit and their designates to develop cybersecurity program strategies, controls, policies, standards and procedures for the Enterprise Network and critical systems such as Supervisory Control and Data Acquisition (SCADA), Automated Train Control Systems, Automated Fare Collection Systems, and Human Resources Systems.

Risk management strategies employed include strategic-level decisions and considerations for how senior leaders and executives are to manage risk to organizational operations and assets, individuals, other organizations, and the nation. We develop, document, and implement an enterprise-wide risk management strategy and processes including a comprehensive cybersecurity program, risk and vulnerability program, and continuous monitoring program to protect Cardholder data and critical infrastructure systems.

Our activities include providing cyber security consultative and advisory support to improve all Authority networks, Assisting in developing and managing the Third-Party Vendor Risk Management program and performing cyber-security assessments on all vendors engaged with the Authority, Performing risk and vulnerability assessments for business processes and current network and application configurations that may pose a risk to the Authority, building Vulnerability and Patch Management programs, and producing metrics for Key Performance Indicators (KPI's) of the security program in totality.

DelNovak is presently supporting the CIO in developing and executing enterprise strategy for Microsoft Azure and Purview adoption. Assisting the CIO with planning, configuration, and deployment of Microsoft Azure and Purview services to enhance cloud governance and data security and compliance.

DelNovak employed the following regulations/standards/laws:

- National Cybersecurity and Critical Infrastructure Protection Act of 2014
- Homeland Security Act of 2002 (HSA)
- Federal Information Processing Standards (FIPS)
- Federal Information Security Modernization Act (FISMA)
- OMB Circular A-130
- Privacy Act of 1974
- PCI DSS v. 3.2/4.0
- Trusted Internet Connection (TIC)

**Relevance**

- Achieved a consensus enterprise-wide cybersecurity program charter and Information Security Program (ISP) framework approved by agency executive leadership and the board
- DelNovak support has resulted in Federal grants funding to enhance critical infrastructure project initiatives across the transit agency
- Achieved consecutive 4 years Payment Card Industry Data Security Standard annual audit compliance
- Achieved TSA Enhancing Cybersecurity Inspection audit with a pass score
- Achieved TSA 2023 TSA BASE Assessment compliance

**Quality of Performance/ Satisfaction**

The customer did not use Customer Satisfaction Surveys. However, DelNovak was singled out by Senior MARTA Officials for exceptional performance since the start of the contract

**Timeliness of Service/Meeting Schedules**

DelNovak met all requirements on or ahead of schedule. Although MARTA made several schedule changes, we were able to meet all requirements.

**Regulatory**

DelNovak complied with all Regulatory Guidance to include 42 USC 5195c: Critical Infrastructure Protection, Critical Infrastructure Information Act of 2002 (CII Act), CISA Transit & Rail Cyber Guidelines, TSA Security Directives 1580/82-2022-01 &-02 , NIST Cybersecurity Framework (CSF), Payment Card Industry Data Security Standard (PCI DSS).

**Cost Control**

DelNovak has maintained exceptional cost control on this contract. Although MARTA initiated changes to the schedule, we were able to meet all changes with no increase to cost. We expect to continue this through the life of the contract.

**Business Relations**

| |
|---|
| DelNovak established exceptional business relations with Gantec and MARTA. We integrated our workforce with the customer to ensure we presented a seamless approach to accomplishing all tasks in the most professional manner.. |
| **Management Oversight** |
| DelNovak's senior management is heavily involved with this project. We have established a span of control using Leads and on-site Supervisor to ensure all employees and deliverables were the most professional products. This has enabled DelNovak to submit all deliverables on time and we have achieved a first submission acceptance from the customer. |

## Reference 2: HIPAA Risk Assessment and Compliance Support

| | |
|---|---|
| **Contract Name** | HIPAA Risk Assessment and Compliance Support |
| **Contracting Agency** | Department of the Interior - Peace Corps |
| **Contract Number** | 47QTCA18D008Q |
| **Award Date** | 04/2021 |
| **Contract Type** | Firm Fixed Price (FFP) |
| **Contract Total Dollar Value** | $349,551 |
| **Period of Performance** | 4/20/2021 - 3/4/2022 |
| **Prime or Subcontractor** | Prime |
| **Major Subcontractors** | N/A |
| **Place of Performance** | Atlanta GA |
| **Procuring Contracting Officer POC** | Name: Crystal Betts<br>Title: Program Manager<br>Email: cbetts@peacecorps.gov<br>Phone: 202-692-1036 |
| **Summary** | |
| The Peace Corps is considered a covered entity by the Health Insurance Portability and Accountability Act (HIPAA). The task order is to provide US Peace Corps - a HIPAA Security Risk Assessment of existing policies and procedures to identify vulnerabilities as well as gaps related to compliance requirements.<br><br>The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal mandate requiring all healthcare providers to protect the security and privacy of all patients and staff | |

members PHI information. These Privacy, Security and Enforcement Rules include standards for protection of confidentiality, integrity and availability of protected health information.

DelNovak provided the Peace Corps with a HIPAA Security Risk Assessment to ensure that it is compliant with all aspects of the HIPAA law and to make appropriate ongoing recommendations regarding policies and procedures pertaining to HIPAA. This risk assessment included a Gap analysis and evaluation of Peace Corps processes and systems.

DelNovak performed a risk analysis of existing policies and procedures to identify vulnerabilities as well as gaps related to compliance requirements. DelNovak performed a Gap analysis and evaluation of the Peace Corps processes and systems to identify areas where it may not meet the current compliance requirements - security, privacy, and functionality requirements. The Gap Analysis addressed specific criteria outlined in the applicable regulations and specifically addressed Peace Corps systems with regard to the relevant criteria.

**In performing this task order, DelNovak:**

1. Reviewed IT systems to ensure they meet all current mandatory HIPAA and HITECH privacy requirements including authorized and restricted use and accessibility to records, storage and protection of records, and proper procedures for the disposal of electronic records.

2. Reviewed IT systems to ensure they meet all current mandatory HIPAA and HITECH security requirements applicable to electronic health records and electronic protected health information, including authorized and restricted accessibility, and storage and protection of electronic health records.

3. Provided Peace Corps with a HIPAA/HITECH compliance report that outlined how the systems meet or do not meet HIPAA and HITECH requirements.

4. Performed a Privacy Threshold Analysis

5. Provided a Privacy Impact Assessment

6. Evaluated adherence to Peace Corps' Manual Section 899, Breach Notification Response Plan

7. Performed GAP analysis to determine requirements for compliance with Federal Information Processing Standards (FIPS), and National Institute of Standards and Technology (NIST) Special Publications

- FIPS 140-2 Security Requirements for Cryptographic Modules
- FIPS 197 Advanced Encryption Standard
- NIST SP 800-122, Guide to Protecting the Confidentiality of Personally

- Identifiable Information (PII)
- NIST SP 800-111, Guide to Storage Encryption Technologies for End User
- Devices
- NIST SP 800-88, Guidelines for Media Sanitization
- NIST SP 800-52, Guidelines for the Selection and Use of Transport Layer
- Security (TLS) – Implementations
- NIST SP 800-77, Guide to IPSec VPNs
- NIST SP 800-113, Guide to SSL VPNs or others which are FIPS 140-2
- validated
- NIST SP 800-66, Resource Guide for Implementing the Health Insurance
- Portability and Accountability Act (HIPAA) Security Rule
- NIST SP 800-88, Guidelines for Medical Sanitization

8. Reviewed Peace Corps business processes to evaluate compliance to the following federal standards:

- OMB Memorandum M-06-16, Protection of Sensitive Information, June 2006
- OMB Memorandum M-07-16, Safeguarding Against and Responding to the
- Breach of Personally Identifiable Information, May 2007
- FIPS-199 Standards for Security Categorization of Federal Information and
- Information Systems
- FIPS-200 Minimum Security Requirements for Federal Information and
- Information Systems
- NIST SP 800-18 Rev. 1, Guide for Developing Security Plans for Federal
- Information Systems
- NIST SP 800-30, Risk Management Guide for Information Technology
- Systems
- NIST SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems
- NIST SP 800-37 Rev. 1, Guide for Applying the Risk Management
- Framework to Federal Information System
- NIST SP 800-53 Rev. 4, Recommended Security Controls for Federal
- Information Systems and Organizations
- NIST SP 800-64 Rev. 2, Security Considerations in the System Development Life Cycle
- NIST SP 800-123, Guide to General Server Security
- NIST SP 800-128, Guide for Security-Focused Configuration Management of Information Systems Applicable sections of the Peace Corps Manual, to include MS 542
- Information and Information Technology Governance and Compliance; Rules of Behavior for General Users

9. Reviewed training documentation to ensure mandates are being met by all necessary staff.
10. Assessed physical safeguards in OHS workspace for protected information.
11. Assessed corrective action steps when privacy breach incidents occur.

| |
|---|
| **Relevance** |
| DelNovak provided a comprehensive Risk Assessment Report that was the basis and outline for the development of a Plan of Action and Milestones (POA&M) for the Peace Corps to achieve regulatory compliance and risk remediation.<br><br>The Peace Corps requires a recommended action plan, in IT Professional Services and/or labor categories for database planning and design; systems analysis, integration, and design; programming, conversion and implementation support; network services, and data records. |
| **Quality of Performance/ Satisfaction** |
| *N/A* |
| **Regulatory** |
| DelNovak complied with all Regulatory Guidance to include, Health Insurance Portability and Accountability Act (HIPAA), Health Information Technology for Economic and Clinical Health Act (HITECH), Federal Information Security Modernization Act (FISMA). |
| **Timeliness of Service/Meeting Schedules** |
| *N/A* |
| **Cost Control** |
| *N/A* |
| **Business Relations** |
| *N/A* |
| **Management Oversight** |
| *N/A* |

## Reference 3: Sec-Ops and FedRAMP ATO Support

| | |
|---|---|
| **Contract Name** | Sec-Ops and FedRAMP ATO Support |
| **Contracting Agency** | Medrics Corp |
| Contract Number | N/A |
| **Award Date** | 10/2023 |
| **Contract Type** | Time & Materials and Labor Hours |
| **Contract Total Dollar Value** | $420,500 |
| **Period of Performance** | 10/2023 - Present |
| **Prime or Subcontractor** | Prime |
| **Major Subcontractors** | *N/A* |
| **Place of Performance** | Atlanta GA |
| **Procuring Contracting Officer POC** | Name: Altug Ozdamar<br>Title: CEO<br>Email: altug.ozdamar@medrics.net<br>Phone: 786 589 0356 |

**Summary**

DelNovak provides comprehensive Security Operations (Sec-Ops) and FedRAMP Authority to Operate (ATO) Support services to Medrics, a health technology company that manages sensitive client and patient information. Our engagement ensures Medrics maintains strong cybersecurity governance, meets FedRAMP compliance requirements, and remains resilient against evolving cyber threats.

A core responsibility of our work is to provide security operations support and continuous monitoring through our **Managed Security Services (MSP)** technical Partner, assist in reviewing and updating Medrics' **System Security Plan (SSP**) and all related **FedRAMP ATO** artifacts. This living document serves as the foundation for Medrics' security program, detailing how FedRAMP security controls are implemented, maintained, and monitored. DelNovak ensures the SSP and its supporting documents remain accurate, current, and fully aligned with federal requirements.

We also **assist with deploying security agents and tools** across Medrics' infrastructure. This includes endpoint detection and response agents, vulnerability management tools, and system monitoring solutions designed to provide continuous visibility into Medrics'

security environment. These tools form the technical backbone of Medrics' ability to detect and respond to threats.

As part of our compliance leadership, DelNovak provides **FedRAMP Authority to Operate (ATO) support and consulting services**. We guide Medrics through the complex ATO process, from preparing evidence and addressing auditor inquiries to advising on corrective actions. This ensures Medrics can demonstrate readiness to meet federal client expectations and maintain its authorization to operate in the cloud.

DelNovak continually **develops and updates Medrics' security artifacts**, including policies, procedures, and control implementation documents. This proactive approach keeps Medrics' security documentation not only FedRAMP-compliant but also practical and usable for staff.

We conduct **Gap Analyses** to evaluate the sufficiency of Medrics' security controls. Each assessment benchmarks Medrics' environment against FedRAMP requirements, highlighting strengths and identifying areas that require remediation. The findings inform a prioritized remediation roadmap, ensuring continuous improvement and risk reduction.

Recognizing the importance of readiness, DelNovak also **evaluates, reviews, and revises Medrics' Incident Response Plan (IRP), processes, and procedures**. We ensure the plan sufficiently addresses FedRAMP requirements, clearly defines roles and responsibilities, and provides actionable steps for detection, containment, eradication, and recovery.

Beyond technical and compliance support, DelNovak serves as Medrics' **Information Security Officer (ISO)**. In this role, we represent Medrics in client meetings, acting as a trusted advisor and ensuring that security considerations are embedded into every client-facing engagement and decision.

Finally, DelNovak provides **flexible IT and cybersecurity support** for any additional needs identified by Medrics. This flexibility ensures that Medrics always has access to expert support, whether for emerging threats, new compliance mandates, or evolving client requirements.

**Relevance**

Through DelNovak's support, Medrics has maintained an audit-ready FedRAMP ATO compliance posture, improved its incident response readiness, enhanced security documentation, and strengthened client trust. By acting as both technical implementer and

| |
|---|
| strategic advisor, DelNovak ensures Medrics operates with a robust, forward-looking cybersecurity program. |
| **Quality of Performance/ Satisfaction** |
| *N/A* |
| **Regulatory** |
| DelNovak complied with all Regulatory Guidance to include, Federal Risk and Authorization Management Program (FedRAMP), United States CLOUD Act, Health Insurance Portability and Accountability Act (HIPAA), Health Information Technology for Economic and Clinical Health Act (HITECH), |
| **Timeliness of Service/Meeting Schedules** |
| *N/A* |
| **Cost Control** |
| *N/A* |
| **Business Relations** |
| *N/A* |
| **Management Oversight** |
| *N/A* |

**Reference 4: Authority to Operate (ATO) Support**

| | |
|---|---|
| **Contract Name** | Authority to Operate (ATO) Support<br>Department of Defense, US Navy |
| **Contracting Agency** | Leidos |

| | |
|---|---|
| **Contract Number** | P010272610 |
| **Award Date** | 06/2022 |
| **Contract Type** | Firm Fixed Price (FFP) |
| **Contract Total Dollar Value** | $129,472.72 |
| **Period of Performance** | 6/2022 |
| **Prime or Subcontractor** | Subcontractor |
| **Major Subcontractors** | N/A |
| **Place of Performance** | San Diego CA |
| Procuring Contracting Officer POC | Name: Devon Rosemeier<br>Title: Sr. Subcontracts Administrator<br>Email: Devon.N.Rosemeier@leidos.com<br>Phone: 571-526-6544 |

**Summary**

DelNovak provided Risk Management Framework Assessment & Authorization to Operate (ATO) support, reviewed implemented security controls and provided input for a Cybersecurity Accreditation package in accordance with the Risk Management Framework (RMF). Prioritized artifacts to be developed and development of artifacts / Augment existing policies/SOP to meet RMF requirements. The artifact requirement was driven by a gap analysis and mapping of the common control identifiers (CCIs) within eMASS.

Documents reviewed:

a. 32 CFR Part 117- National Industrial Security Program Operating Manual (NISPOM)
b. DoDI 3020.41, Contractor Personnel Authorized to Accompany the U.S. Armed Forces
c. DoDI 8510.01, Risk Management Framework for DoD Information Technology (IT)
d. DoDI 8500.01 Cybersecurity
e. United States Navy Risk Management Framework Process Guide Version

**Relevance**

DelNovak efforts led to the actualization of an Authorization to Operate (ATO) for the information system, and ensured the information system meets specific security standards and has an acceptable level of risk to operate on the DOD network.

**Quality of Performance/ Satisfaction**

| |
|---|
| *N/A* |
| **Regulatory** |
| DelNovak complied with all Regulatory Guidance to include, 32 CFR Part 117- National Industrial Security Program Operating Manual (NISPOM), DoDI 8510.01, Risk Management Framework for DoD Information Technology (IT), DoDI 8500.01 Cybersecurity, United States Navy Risk Management Framework Process Guide Version 3.3, Federal Information Security Modernization Act (FISMA). |
| **Timeliness of Service/Meeting Schedules** |
| *N/A* |
| **Cost Control** |
| *N/A* |
| **Business Relations** |
| *N/A* |
| **Management Oversight** |
| *N/A* |

## Reference 5: Web and Mobile Application Development Support Services

| | |
|---|---|
| **Contract Name** | Web and Mobile Application Development Support Services<br>Department of Labor - OPA-DEC |
| **Contracting Agency** | TriTech Enterprise Systems Inc |
| **Contract Number** | *N/A* |
| **Award Date** | 2012 |

| | |
|---|---|
| **Contract Type** | Firm Fixed Price (FFP) |
| **Contract Total Dollar Value** | 1,689,000 |
| **Period of Performance** | 2012 - 2016 |
| **Prime or Subcontractor** | Subcontractor |
| **Major Subcontractors** | N/A |
| **Place of Performance** | Washington DC |
| **Procuring Contracting Officer POC** | Name: Latonia Lewis,<br>Title: Program Manager<br>Email:llewis@tritechenteprise.com<br>Phone:301-346-3865 |

**Summary**

DelNovak Supported all services in accordance with the Departmental Systems Development Life Cycle (SDLC) requirements.

Provided Technical Support Services includes:

- Web applications (both off the shelf and onsite created) and website development
- Support mobile applications (both created inside and outside DEC) for a variety of platforms in support of DEC's development network.
- Service Desk management and support
- Enterprise Active Directory Administration support
- Enterprise Storage Administration Services support
- Enterprise Backup and Recovery Administration support
- Data Archiving and Tape Library services support
- Enterprise Network Administration services for OPA-DEC
- Multiplatform Enterprise System Administration (Windows, UNIX) services
- Enterprise Systems Management services
- Web and Database Application Administration services
- Multiplatform database management system (DBMS) (e.g., MS SQL Server, MySQL) Design and Administration services
- Web content management services including research, editing, proofreading, creating and maintaining graphics, and designing web page layouts, as requested
- Internet and intranet website content editing and publishing (HTML/CSS), including DOL newsletter and e-magazine publications

Provided IT governance and security services, including security assessment and authorization requirements (formerly referred to as certification and accreditation) including development and implementation of related security documentation.

Supported capital planning and enterprise architecture requirements including, but not limited to, Exhibit 53/300 and IT Dashboard submissions, configuration, change, and release management activities. Supported website security, including web application firewalls, incident response, security compliance and testing, information asset protection, and additional security services, as required.

Responded to all Office of Management and Budget (OMB) and Departmental requirements within requested timeframes. Maintained memorandums of understanding and service level agreements (SLAs).

Provided testing and quality assurance (QA) services. Ensuring usability, Section 508/accessibility, and quality assurance for all DOL websites. Provided monthly usage statistics and activity reports on DOL websites as requested using DEC's web metrics solution.

**Relevance**

The comprehensive Web and Mobile Application Development Support Services enabled DOL-OPA DEC to execute its mission more efficiently by improving access to critical tools and information, streamlining processes, and ensuring secure, compliant operations.

**Quality of Performance/ Satisfaction**

*N/A*

**Regulatory**

DelNovak complied with all Regulatory Guidance to include Office of Management and Budget (OMB), Federal Information Security Modernization Act (FISMA), Section 508 of the Rehabilitation Act and Section 255 of the Communications Act.

**Timeliness of Service/Meeting Schedules**

*N/A*

**Cost Control**

*N/A*

**Business Relations**

| |
|---|
| *.N/A* |
| **Management Oversight** |
| *N/A* |

# Capability Statement

## CAPABILITY STATEMENT

*Transforming government operating environments through innovative solutions.*

### WHO WE ARE

DelNovak, LLC is a cybersecurity and technology transformational services company with over twelve (12) years of experience supporting public and private sector clients with high performing Cyber and IT services and solutions. DelNovak supports the mission of its clients.

8(a) CERTIFIED | HUBZONE CERTIFIED | GSA

**CAGE CODE: 65KF1 | UEI: G8NRKTDRGED3**

### Summary of CyberSecurity Expertise and Qualifications

| Expertise | DelNovak Capability and Experience | |
|---|---|---|
| NIST Risk Management and CyberSecurity Frameworks establishment and management | YES | Full range of capabilities including develop, document, and implement an enterprise-wide risk management strategy and processes |
| Security Risk Assessment | YES | Full range of capabilities (assessment, compliance, GRC, HIPAA, Privacy etc) |
| Security Control Assessment and Training | YES | Full range of capabilities |
| Cloud Security | YES | Full range of capabilities |
| Authorization to Operate (ATO) | YES | Full range of capabilities |
| HIPAA/Privacy Compliance | YES | Full range of capabilities |
| Continuous Monitoring | YES | Full range of capabilities |
| Governance Risk and Compliance | YES | Full range of capabilities |

### Summary of Cloud Expertise and Qualifications

| Expertise | DelNovak Capability and Experience | |
|---|---|---|
| SAFe Agile | YES | Range of capabilities (Lean, DevOps, Culture, Alignment, Management etc) |
| Azure Cloud | YES | Migration, Integration, Containerization, Security best-practices, secure configuration policy enforcement, continuous monitoring, leadership, and management |
| AWS Cloud | YES | Migration, Integration, Containerization, Security best-practices, secure configurations, policy enforcement, continuous monitoring, leadership, and management |
| DevOps | YES | Management, automation, development, deployment, integration, monitoring, testing, secureCode, product line management, and orchestration |
| Product Management | YES | IT Infrastructure, End user operations, CyberSecurity |
| Project Management | YES | Full range of capabilities |

### COMPANY INFORMATION

**Technical Certifications:**

- CISSP, CISM, CRISC, PMP, ITIL, DBA, MCITP, Azure, AWS, Red Hat, Microsoft, Cisco, Oracle, CMMC Level-1 UID: S100013784, CMMC Level-2 UID: S200033191

**Contracting Vehicles:**

- GSA 47QTCA20D00AJ
- 54151HACS - Highly Adaptive Cybersecurity Services (HACS)
- 54151S - IT Professional Services
- NASA SEWP (Partner)
- GSA 8(a) STARS - Partner
- Reseller of DELL and Ingram Micro

**Clients:**

- Dept of Navy, Dept of Veterans Affairs,
- Dept of Labor, Dept of Interior etc.

**Business Certifications:**

- SBA 8(a)
- HUBZone
- Small Disadvantaged Business

**SBA Business Opportunity Specialist:**
**Jatavius T. Williams**
**Cell:** (202) 941-8071
**Office:** (404) 850-2958
georgiaofferletters@sba.gov

**NAICS Codes:**

- **541511 - Custom Computer Programming**
- **541512 - Computer Systems Design**
- **541519 - Other Computer Related Services**

***Accepts Credit Cards***

**Technical, Professional, and Administrative *Staffing* domestically and internationally.**

260 Peachtree Street NW, Suite 2200 Atlanta, GA 30303 (202) 505-2782
www.delnovak.com

## PAST PERFORMANCE

- **Department of Interior (Peace Corps)**
  Conducted HIPAA Security Risk Assessment, Performed Gap Analysis of physical, technical and admin safeguards; Reviewed over 100 policies. Developed remediation plan, performed Privacy Threshold Analysis and Privacy Impact Assessment, Provided a comprehensive Security Risk Assessment Report with actionable recommendations.

- **State of Texas Comptroller of Public Accounts**
  Conducted NIST 800-53 Security Controls and IRS 1075 Gap Analysis and provided remediation recommendation to senior leadership. Conducted General Support System (GSS) certification assessment using NIST assessment guidelines, provided remediation recommendations and assisted client in developing POAMs.

- **DelNovak has used these Standards and Guidelines (Sample)**
  - ✓ National Institute of Standards and Technology (NIST) Special Publication 800 series.
  - ✓ Center for Internet Security (CIS) 18.
  - ✓ Homeland Security Act DHS (HSA).
  - ✓ Federal Information Processing Standards (FIPS).
  - ✓ Federal Information Security Modernization Act (FISMA).
  - ✓ OMB Circulars.
  - ✓ Department of Defense 8500, 8510, DoDI 3020.
  - ✓ Presidential and Executive Orders.
  - ✓ HIPAA and HiTECH Act.
  - ✓ PCI DSS Self-Assessment Questionnaires.
  - ✓ Risk and Gap Analysis Proprietary Automated

- **Department of the NAVY**
  Subcontractor to Large Prime on a Department of Defense contract Risk Management Framework DelNovak reviewed 52 control families and provided input for a Cybersecurity Accreditation package in accordance with the Risk Management Framework (RMF). The artifact requirement was driven by a gap analysis and mapping of the common control identifiers (CCIs) within eMASS.

- **Subcontractor to Large Prime on a Department of Veterans Affairs contract**
  **Title:** Enterprise IT Services Support Risk and vulnerability assessment, security architecture review, privacy impact assessment, security relevance review, cloud hosted systems security control assessment, system security assessment and authorization, and Authority to Operate (ATO). Designed processes that assisted in managing and tracking ATO project activities across system enclaves with metrics that improved ATO/ATOC achievement rate by over 90%. FedRAMP security assessment and authorization programs that resulted in 4 major cloud hosted systems security certification and accreditation.

- Metropolitan Atlanta Rapid Transit Authority Enterprise Cyber Security Program Development Risk and Vulnerability Assessment. Third-Party Risk Assessment. PCI-DSS Annual Compliance Assessment and Reporting. Penetration Testing and Threat Intelligence Support working with Department of Homeland Security and other government agencies. Resulted in government funding for critical infrastructure protection.

## LEADERSHIP

**Emmanuel Ogidigben, CISSP**
emmanuel@delnovak.com

**Ayo Alaran, MBA, PMP**
ayo@delnovak.com