



General Services Administration

Federal Supply Service
Authorized Federal Supply Schedule Price List

GSA Schedule 84

TOTAL SOLUTIONS FOR LAW ENFORCEMENT, SECURITY, FACILITY MANAGEMENT SYSTEMS, FIRE, RESCUE, SPECIAL PURPOSE CLOTHING, MARINE CRAFT AND EMERGENCY/DISASTER RESPONSE

SIN 246-52, PROFESSIONAL SECURITY SERVICES



Identification Technology Partners, Inc. (IDTP)
12208 Pueblo Road
North Potomac, MD 20878-2064
Office: 301-990-9404
Fax: 301-990-9405
www.idtp.com

Contract Number: **GS-07F-5866R**

Contract Period: **June 1, 2010 – May 31, 2015**

IDTP is a small business

Point of Contact:

Stephen M. Hunt
shunt@idtp.com
Office: 703-430-2037
Fax: 703-430-3077

Products and ordering information in this Authorized FSS Information Technology Schedule Pricelist are also available on the GSA Advantage! System. Agencies can browse GSA Advantage! by accessing the Federal Supply Service's home page via the Internet at <http://www.fss.gsa.gov/>

Table of Contents

<i>Section 1 – IDTP</i>	3
Qualifications	3
Technical Standards	5
<i>Section 2. Customer Information</i>	6
<i>Section 3. SIN 246-52 Position Descriptions</i>	7
Senior Principal / Subject Matter Expert III:	7
Senior Consultant / Subject Matter Expert II:	7
Consultant:	7
Principal:	8
Subject Matter Expert I:	8
Senior Analyst:	8

Section 1 – IDTP

Qualifications

Identification Technology Partners, Inc. (IDTP) is the leading engineering and consulting firm specialized in the critical elements of secure identity systems, identity management, and forensic identification systems; including their design, development, operation and deployment. IDTP provides independent “subject matter expertise”, broad program support services, and commercial market-centric research and reporting services. Our clients include various agencies of the federal government, Fortune 100 companies, and other commercial businesses.

IDTP is providing trusted, world-class technical support to some of the largest, most advanced identification and credentialing programs of their kind. We have achieved an unrivaled reputation for integrity and performance, and maintain a determined dedication to professional advancement and client support. IDTP has been instrumental in assisting government agencies to develop appropriate and effective program specifications, CONOPS, system architectures and performance testing as a solid foundation for advanced Identity Credentialing and Access Management (ICAM) programs within the enterprise. We are also engaged in providing technical design and operational performance expertise specific to advanced biometrics systems (i.e., AFIS and other modalities) seeking to optimize their effectiveness in integrated systems for forensic and national security solutions.

IDTP provides unbiased, independent expertise in areas that include:

- Identity credentialing programs (e.g. smart cards, identity and access management, PKI, policy)
- Forensic biometrics identification systems (e.g. AFIS and related technologies)
- Testing evaluation and validation of system performance and compliance
- Domestic and international technical industry standards and best practices
- Applied solutions for the development, integration, operation and deployment of identity and access management technologies
- Industry analysis and research in support of commercial market development

IDTP’s capabilities span the full range of services and knowledge necessary to support large-scale, multi-faceted credentialing and identification programs. These capabilities include the following:

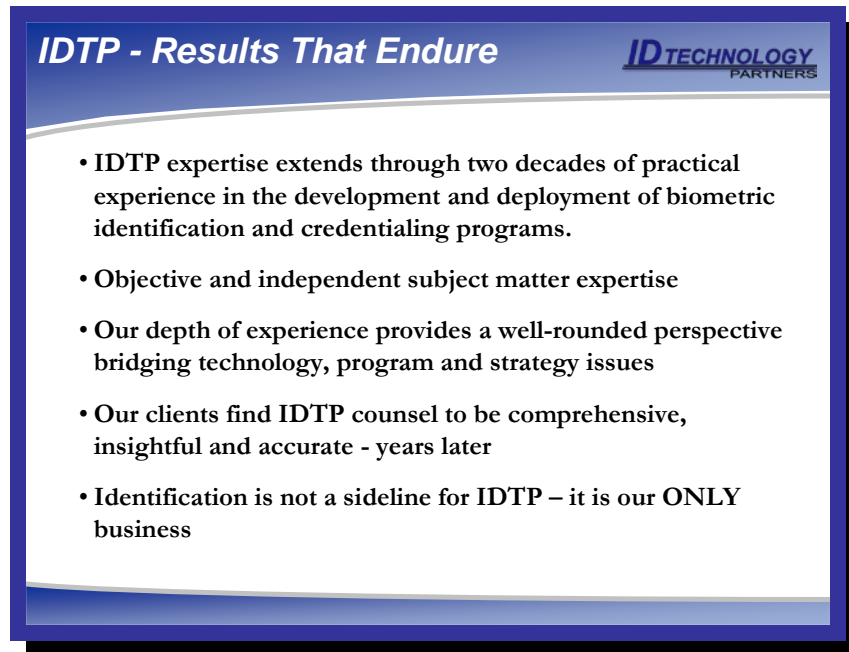
Technical Engineering and Testing Services that provide a full range of consulting, engineering, design, performance testing, test protocol development and system and infrastructure design services based on experience, and knowledge of industry standards and best practices. IDTP specializes in system testing and optimization, comparative performance testing and performance analysis. IDTP services also support related security, identification and authentication requirements.

Program Support Services that provide support to new or in-progress client programs to assist with program management, requirements and specifications development, strategic planning, risk

management, implementation, oversight, business transformation and process change, planning, education and stakeholder communications.

Standards Development Services that provide clients with valuable insight and direction regarding technical industry standards and their impact on program development efforts. We are able to provide representation in standards bodies and working groups of interest to our clients.

Policy Services that provide clients with foundational policy development support based on knowledge and experience including privacy policy, legal and regulatory compliance, security and protection policy. These policy elements are viewed as critical to the success and pace of our client's program implementations.



The slide features a blue header with the title "IDTP - Results That Endure" on the left and the "ID TECHNOLOGY PARTNERS" logo on the right. The main content area is white with a blue border and contains a bulleted list of five points. The slide is set against a dark blue background.

- IDTP expertise extends through two decades of practical experience in the development and deployment of biometric identification and credentialing programs.
- Objective and independent subject matter expertise
- Our depth of experience provides a well-rounded perspective bridging technology, program and strategy issues
- Our clients find IDTP counsel to be comprehensive, insightful and accurate - years later
- Identification is not a sideline for IDTP – it is our **ONLY** business

IDTP has the career-veteran biometric and credentialing experts recognized for their real-world project experience, and extensive involvement in developing standards, compliance testing tools and industry best practices IDTP is a team of highly accomplished professionals, many of whom have been entrusted to develop and support some of the world's largest and most complex biometrics identification systems and identity credentialing programs. IDTP's singular abilities are proven through exemplary performance in original, large-scale, high-visibility projects. Our award-winning technical "subject matter expertise" and program management performance ensures success in the development of effective identification solutions, and the competent fulfillment of program goals.

IDTP maintains a **Conference and Technology Center (C&TC)** which supports technology and system testing, and provides our clients and the industry with an accessible, full-featured conference facility to host client meetings and technical mini-conferences.

Technical Standards

IDTP has been an active participant and contributor to biometrics and smart card technology standards committees and working groups. IDTP holds voting memberships in several domestic and international standards bodies. IDTP individuals have held various supporting positions over many years that include committee and working group chairmanships, project editors and technical writing roles

Our partners and senior associates have been involved with the development and application of technology standards since the mid 1980's. IDTP has made recognized contributions to the national standards process via awards from ANSI / INCITS. IDTP serves as a "standards incubator" to INCITS / M1, the American National Standards Institute (ANSI) standards group for biometrics. IDTP participates in a number of standards initiatives, including:

- BioAPI Consortium
- Common Biometric Exchange Formats Framework (CBEFF)
- Biometric Consortium Working Group
- ANSI/INCITS B10
- INCITS / M1 and related task groups
- ISO/IEC JTC 1 / SC 37 International Biometric Technical Standards Sub-committee
- Data Format for the Interchange of Fingerprint, Facial, & Scar Mark and Tattoo (SMT) Information (ANSI/NIST-ITL-1-2007)
- M1 - Border Management Application Profile
- RTCA Special Committee 207 Airport Security Access Control Standard (DO-230)

Further, IDTP provides key personnel support for:

- M1 – Application Profile for the Identification of Transportation Workers (tech. co-editor)
- M1 - Biometric Data Interchange Formats – (technical editor for the finger image and finger minutiae standards)
 - Acting Chair - Task Group on Biometric Data
 - Chair – Task Group on Biometric Technical Interfaces and Profiles
- SC 37 – Common Biometric Exchange Formats Framework (technical editor parts 1,2,3)
- SC 37 - Biometric Data Interchange Formats (technical editor for 19794-2 Finger Minutiae and 19794-4 Finger image standards)
- Government Smart Card- Interagency Advisory Board (GSC-IAB) Federal Information Processing Standard (FIPS) 201 & Special Publication (SP) 800-73, SP 800-76 and SP 800-78 initiatives.
- Former technical editor of the ANSI/NIST-ITL Data Format Interchange Standards

Section 2. Customer Information

1. a. SIN 246-52; Professional Security Services – See Section 3
b. Government price based on a unit of one; exclusive of any quantity/dollar volume or prompt payment discount. – See Section 4.
2. Maximum order: \$200,000
3. Minimum order; \$100
4. Geographic coverage: Domestic, 50 states, Washington D.C., Puerto Rico, US Territories
5. Points of Production: Not Applicable
6. Discount from list prices: Prices shown are Net prices; basic discounts have been deducted
7. Quantity Discounts: None
8. Prompt payment terms: 2% 20 days – Net 30
9. a. Government purchase cards are accepted for payment at or below the micro-purchase threshold
b. Government purchase cards are accepted for payment above the micro-purchase threshold
10. Foreign items: None
11. a. Time of Delivery: 30 days ARO or per Statement of Work
b. Expedited Delivery: Per Statement of Work
c. Overnight & Two day delivery: None
d. Urgent Requirements: Agencies can contact Contractor's representative to affect a faster delivery. Customers are encouraged to contact the contractor for the purpose of requesting accelerated delivery.
12. FOB Point: Not Applicable
13. Ordering Address: ID Technology Partners, 12208 Pueblo Road, North Potomac MD 20878-2064.
14. Payment Address: Same as Ordering Address
15. Warranty Provisions: Per Statement of Work
16. Export Packing Charges: Not Applicable
17. Terms and Conditions of Government Purchase Card Acceptance: Any thresholds above the micro-purchase level
18. Terms and Conditions of Rental, Maintenance and Repair: Not Applicable
19. Terms and Conditions of Installation: Not Applicable
20. Terms and Conditions of repair parts, indicating date of parts, price lists and any discounts from list prices: Not Applicable
 - a. Terms and Conditions for any other services: Not Applicable
21. Lost of Service and Distribution points: Not Applicable
22. List of Participating Dealers; Not Applicable
23. Preventative Maintenance: Not Applicable
24. a. Special Attributes such as Environmental Attributes: Not Applicable
b. Section 508 Compliance for EIT: Not Applicable
25. DUNS Number: 101520364
26. Notification regarding registration in Central Contractor Registration (CCR) Database: Registration valid

Section 3. SIN 246-52 Position Descriptions

Senior Principal / Subject Matter Expert III:

Experience: Has a minimum of 20 years experience in the corporate/business environment with at least five years in a senior management position responsible for day-to-day operations of a major business operating unit, or equivalent experience in a corporate senior staff role. Possesses the ability to work with clients at the senior manager level to assess and evaluate the total impact of changes to business and/or operating policy, processes, business rules, products, technology and their integration into overall business plans to meet organizational objectives.

Functional Responsibility: The Senior Principal/SME III plans, directs, and coordinates all phases of multiple client projects, and/or leads projects. The Senior Principal/SME III is a member of a senior management team that assesses a client's business and security (physical & logical access) technology organization to in order to determine and meet business or mission objectives. A Senior Principal/SME III develops strategic and tactical business/mission objectives, plans and the supporting infrastructure. This individual develops any necessary reports, documentation, solicitations, or other support materials to support client short and long term objectives.

Education: Bachelor's Degree and/or 20 years in progressive middle and/or senior management positions.

Senior Consultant / Subject Matter Expert II:

Experience: A nationally recognized expert evidenced by past performance, publications, or patents, and fifteen years of progressive experience in the design, development and implementation of security systems. The specialty may relate to a variety of development, operational or support functions that require special expertise, due to degree of complexity, impact on mission, or novelty of approach.

Functional Responsibility: The Senior Consultant/SME II is responsible for advising clients on the proper approach to a unique functional problem regarding a security system, or the design and development of a major new physical or logical access security system, or total redesign of an existing security system.

Education: A Master's degree and/or 15 years of experience in a field appropriate to the area of consultation is required.

Consultant:

Experience: Recognized expert in the field as evidenced by past performance, publications, or patents, and ten years of progressive experience in the application and development of systems in the area of security. The specialty may relate to a variety of development, operational or support functions that require special expertise, because of the degree of complexity, impact on mission, or novelty of approach.

Functional Responsibility: The Consultant is responsible for advising clients on the proper approach to a unique functional problem regarding a security system, or the design and development of a major new physical or logical access security system, or total redesign of an existing system.

Education: A Bachelor's degree and 10 years of experience in a field appropriate to the area of consultation is required.

Principal:

Experience: Has 10 to 15 years experience in a business environment with demonstrated ability to effectively manage a broad spectrum of management activities to include, but not limited to operations, planning, requirements analysis, process design and development, procurement, logistics, financial analysis, strategic and tactical planning, business case development, risk analysis, and other business and/or information technology activity. Has the ability to understand common and distinct business and/or information technology elements and how they can be enabled to meet the business objectives of the client.

Functional Responsibility: The Principal has demonstrated expertise in security technology, and/or physical access and logical access business practices. Demonstrates thought leadership and fluency in issue analyses in the business and/or security technology field. The Principal assesses the scope and complexity of a client's issues and leads the development and execution of strategic programs. He or She serves as a functional or industry specialist within the areas of strategic planning, security process analysis, benchmarking, organizational alignment, and other operational areas.

Education: Bachelor's Degree or equivalent of 12 to 15 years experience in increasingly responsible positions.

Subject Matter Expert I:

Experience: The Subject Matter Expert I have 5 to 12 years experience in a specific area of expertise related to security technology, automated identification, biometrics, image processing, operations, standardization, failure analysis, encryption, PKI, and Integrated Circuit Chip (ICC) definition and application.

Functional Responsibility: The Subject Matter Expert I provides expert advice and guidance to clients based on their expertise and evaluation of assigned problem areas. Prepare written and oral presentations.

Education: A Bachelor's degree in engineering, technical or management discipline. Ten or more years of specific related experience can substitute for a degree.

Senior Analyst:

Experience: The Senior Analyst has 5 to 12 years experience in the development, analysis, and review of business and/or security technology processes or systems. He or She works with minimal supervision and often functions in a supervisor capacity overseeing the day-to-day work of others.

Functional Responsibility: Assists in development of analysis of client organizational and operational issues to include, but not limited to planning, requirements, design and development, procurement, logistics, financial analysis, strategic and tactical planning, business case development, risk analysis, and other business activity.

Education: Bachelor's Degree or equivalent of 6 years experience in increasingly responsible positions.