



CHAPTER 8 TABLE OF CONTENTS

CHAPTER 8. SPECIAL ITEM 132-62: AUTHENTICATION PRODUCTS AND SERVICES.....	1
TERMS AND CONDITIONS	1
8.1. ORDER.....	2
8.2. PERFORMANCE OF SERVICES.....	2
8.3. STOP-WORK ORDER (FAR 52.242-15) (AUG 1989).....	3
8.4. INSPECTION OF SERVICES.....	3
8.5. RESPONSIBILITIES OF THE ORDERING ACTIVITY.....	3
8.6. INDEPENDENT CONTRACTOR	4
8.7. ORGANIZATIONAL CONFLICTS OF INTEREST.....	4
8.8. INVOICES	4
8.9. PAYMENTS	4
8.10. RESUMES	5
8.11. INCIDENTAL SUPPORT COSTS	5
8.12. APPROVAL OF SUBCONTRACTS	5
ADDITIONAL IBM TERMS	5
8.13 REQUIRED CONSENTS	5
8.14 PERSONNEL	5
8.15 ACCEPTANCE.....	6
8.16 MATERIALS OWNERSHIP AND LICENSE.....	6
8.17 WARRANTY FOR IBM SERVICES	6
LABOR CATEGORIES AND DESCRIPTIONS	8
LABOR RATES	16

CHAPTER 8. SPECIAL ITEM 132-62: AUTHENTICATION PRODUCTS AND SERVICES

TERMS AND CONDITIONS

Note: These terms are in addition to those described in Chapter 1, General Information.

During the contract period, International Business Machines Corporation (IBM) and the Government agree that the following terms and conditions will apply to any order for IBM IT Professional Services that is placed by the Government under this Special Item. The term "Government" shall mean all Federal agencies (as defined in Paragraph (b) of 40 USC 472) the Senate, the House of Representatives, the Architect of the Capitol, and the Government of the District of Columbia, all of which are hereinafter referred to as the Government. The materials and services under this Special Item will be available to the Government within the United States, the District of Columbia and Puerto Rico. Such sales will be made to the Government within the United States, the District of Columbia and Puerto Rico. On a case-by-case basis IBM will deliver products and perform Services to overseas U.S. Government locations which are in support of national defense operations (including U.S. Embassies), and to locations which support the national interest of the United States.

General Background

Authentication Products and Services provide for authentication of individuals for purposes of physical and logical access control, electronic signature, performance of E-business transactions and delivery of Government services. Authentication Products and Services consist of hardware, software components and supporting services that provide for identity assurance.

Homeland Security Presidential Directive 12 (HSPD-12), "Policy for a Common Identification Standard for Federal Employees and Contractors" establishes the requirement for a mandatory Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractor employees assigned to Government contracts in order to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy. Further, the Directive requires the Department of Commerce to promulgate a Federal standard for secure and reliable forms of identification within six months of the date of the Directive. As a result, the National Institute of Standards and Technology (NIST) released Federal Information Processing Standard (FIPS) 201: Personal Identity Verification of Federal Employees and Contractors on February 25, 2005. FIPS 201 requires that the digital certificates incorporated into the Personal Identity Verification (PIV) identity credentials comply with the X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework. In addition, FIPS 201 requires that Federal identity badges referred to as PIV credentials, issued to Federal employees and contractors comply with the Standard and associated NIST Special Publications 800-73, 800-76, 800-78, and 800-79.

Special Item Number

IBM offers SIN 132-62 which includes:

Established for products and services for agencies to implement the requirements of HSPD-12, FIPS-201 and associated NIST special publications. The HSPD-12 implementation components specified under this SIN are:

- PIV enrollment and registration services,
- PIV systems infrastructure,
- PIV card management and production services,
- PIV card finalization services,
- Physical access control products and services,
- Logical access control products and services,
- PIV system integration services, and
- Approved FIPS 201-Compliant products and services.

8.1. ORDER

- a. Agencies may use written orders, EDI orders, blanket purchase agreements, individual purchase orders, or task orders for ordering authentication products and services under this contract. Blanket Purchase Agreements shall not extend beyond the end of the contract period; all services and delivery shall be made and the contract terms and conditions shall continue in effect until the completion of the order. Orders for tasks which extend beyond the fiscal year for which funds are available shall include FAR 52.232-19 (Deviation – May 2003) Availability of Funds for the Next Fiscal Year. The purchase order shall specify the availability of funds and the period for which funds are available.
- b. All task orders are subject to the terms and conditions of the contract. In the event of conflict between a task order and the contract, the contract will take precedence.
- c. When placing an order, ordering activities may deal directly with the contractor or ordering activities may send the requirement to the Program Management Office to received assisted services for a fee.

8.2. PERFORMANCE OF SERVICES

- a. The Contractor shall commence performance of services on the date agreed to by the Contractor and the ordering activity.
- b. The Contractor agrees to render services only during normal working hours, unless otherwise agreed to by the Contractor and the ordering activity.
- c. The ordering activity should include the criteria for satisfactory completion for each task in the Statement of Work or Delivery Order. Services shall be completed in a good and workmanlike manner.
- d. Any Contractor travel required in the performance of the Services under this SIN 132-62 must comply with the Federal Travel Regulation or Joint Travel Regulations, as applicable, in effect on the date(s) the travel is performed. Established Federal Government per diem rates will apply to all Contractor travel. Contractors cannot use GSA city pair contracts.

8.3. STOP-WORK ORDER (FAR 52.242-15) (AUG 1989)

(a) The Contracting Officer may, at any time, by written order to the Contractor, require the Contractor to stop all, or any part, of the work called for by this contract for a period of 90 days after the order is delivered to the Contractor, and for any further period to which the parties may agree. The order shall be specifically identified as a stop-work order issued under this clause. Upon receipt of the order, the Contractor shall immediately comply with its terms and take all reasonable steps to minimize the incurrence of costs allocable to the work covered by the order during the period of work stoppage. Within a period of 90 days after a stop-work is delivered to the Contractor, or within any extension of that period to which the parties shall have agreed, the Contracting Officer shall either-

(1) Cancel the stop-work order; or

(2) Terminate the work covered by the order as provided in the Default, or the Termination for Convenience of the Government, clause of this contract.

(b) If a stop-work order issued under this clause is canceled or the period of the order or any extension thereof expires, the Contractor shall resume work. The Contracting Officer shall make an equitable adjustment in the delivery schedule or contract price, or both, and the contract shall be modified, in writing, accordingly, if-

(1) The stop-work order results in an increase in the time required for, or in the Contractor's cost properly allocable to, the performance of any part of this contract; and

(2) The Contractor asserts its right to the adjustment within 30 days after the end of the period of work stoppage; provided that, if the Contracting Officer decides the facts justify the action, the Contracting Officer may receive and act upon the claim submitted at any time before final payment under this contract.

(c) If a stop-work order is not canceled and the work covered by the order is terminated for the convenience of the Government, the Contracting Officer shall allow reasonable costs resulting from the stop-work order in arriving at the termination settlement.

(d) If a stop-work order is not canceled and the work covered by the order is terminated for default, the Contracting Officer shall allow, by equitable adjustment or otherwise, reasonable costs resulting from the stop-work order.

8.4. INSPECTION OF SERVICES

The Inspection of Services-Fixed Price (AUG 1996) (Deviation – May 2003) clause at FAR 52.246-4 applies to firm-fixed price orders placed under this contract. The Inspection-Time and Materials and Labor-Hour (JAN 1986) (Deviation – May 2003) clause at FAR 52.246-6 applies to time and materials and labor-hour orders placed under this contract.

8.5. RESPONSIBILITIES OF THE ORDERING ACTIVITY

Subject to security regulations, the ordering activity shall permit Contractor access to all facilities necessary to perform the requisite services.

8.6. INDEPENDENT CONTRACTOR

All services performed by the Contractor under the terms of this contract shall be an independent Contractor, and not as an agent or employee of the ordering activity.

8.7. ORGANIZATIONAL CONFLICTS OF INTEREST

a. Definitions.

“Contractor” means the person, firm, unincorporated association, joint venture, partnership, or corporation that is a party to this contract.

“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.

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.

8.8. INVOICES

The Contractor, upon completion of the work ordered, shall submit invoices for products and/or services. Progress payments may be authorized by the ordering activity on individual orders if appropriate. Progress payments shall be based upon completion of defined milestones or interim products. Invoices shall be submitted monthly for recurring services performed during the preceding month.

8.9. PAYMENTS

For firm-fixed price orders the ordering activity shall pay the Contractor, upon submission of proper invoices or vouchers, the prices stipulated in this contract for service rendered and accepted. Progress payments shall be made only when authorized by the order. For time and materials orders, the Payments under Time and Materials and Labor Hour Contracts at FAR 52.232-7 (DEC 2002), (Alternate II – Feb 2002) (Deviation – May 2003) applies to time and materials orders placed under this contract. For labor hour orders, the Payment under Time and Materials and Labor Hour Contracts at FAR 52.232-7 (DEC 2002), (Alternate II – Feb 2002)

(Deviation – May 2003)) applies to labor hour orders placed under this contract. IBM's rates identified herein shall apply to labor performed by IBM, its Subcontractors, and/or Divisions, subsidiaries, or affiliates of IBM under a common control.

8.10. RESUMES

Resumes shall be provided to the GSA Contracting Officer or the user ordering activity upon request.

8.11. INCIDENTAL SUPPORT COSTS

Incidental support costs are available outside the scope of this contract. The costs will be negotiated separately with the ordering activity in accordance with the guidelines set forth in the FAR.

8.12. APPROVAL OF SUBCONTRACTS

The ordering activity may require that the Contractor receive, from the ordering activity's Contracting Officer, written consent before placing any subcontract for furnishing any of the work called for in a task order.

ADDITIONAL IBM TERMS

8.13 REQUIRED CONSENTS

The Government is responsible for promptly obtaining and providing to IBM all Required Consents necessary for IBM to provide the Services described in a Statement of Work. A Required Consent means any consents or approvals required to give IBM or our subcontractors the right or license to access, use and/or modify (including creating derivative works) the hardware, software, firmware and other products, to enable IBM and our subcontractors to perform the Services set forth in the Statement of Work without infringing the ownership or license rights (including patent and copyright) of the providers or owners of such product. IBM will be relieved of the performance of any obligations that may be affected by your failure to promptly provide any Required Consents to IBM.

8.14 PERSONNEL

Each of us is responsible for the supervision, direction, control, and compensation of our respective. personnel.

IBM reserves the right to determine the assignment of its personnel.

IBM may subcontract a Service, or any part of it, to subcontractors.

8.15 ACCEPTANCE

For services having Completion Criteria identified in the Statement of Work, acceptance occurs when IBM meets the Completion Criteria.

For hourly services, acceptance occurs upon completion of the service hours.

8.16 MATERIALS OWNERSHIP AND LICENSE

IBM will specify materials to be delivered to the Government. They will be identified as being "Type I Materials," "Type II Materials," or otherwise as mutually agreed upon. If not specified, Materials will be considered Type II Materials.

Type I Materials are those, created during the Service performance period, in which the Government has all right, title and interest (including ownership of copyright). IBM will retain one copy of the Materials. IBM is granted 1) an irrevocable, nonexclusive, worldwide, paid-up license to use, execute, reproduce, display, perform, distribute (internally and externally) copies of, and prepare derivative works based on Type I Materials and 2) the right to authorize others to do any of the former. With respect to data or materials of a proprietary nature, IBM will safeguard the data or materials in accordance with the terms of a mutually agreeable Confidential Disclosure Agreement.

Type II Materials are those, created during the Service performance period or otherwise (such as those that preexist the Service), in which IBM or third parties have all right, title and interest (including ownership of copyright). IBM will deliver one copy of the specified Materials to the Government. IBM grants the Government an irrevocable, nonexclusive, worldwide, paid-up license to use, execute, reproduce, display, perform, and distribute, within the Government agency, copies of Type II Materials.

Both IBM and Government agree to reproduce the copyright notice and any other legend of ownership on any copies made under the license granted under this item.

Any idea, concept, know-how, or technique which relates to the subject matter of a service and is developed or provided by either IBM or the Government, or jointly, in the performance of a service may (subject to applicable patents and copyrights) be freely used by either the Government or IBM.

8.17 WARRANTY FOR IBM SERVICES

IBM warrants that it performs each IBM Service using reasonable care and skill and according to its current description (including any completion criteria) contained in an Attachment or Statement of Work.

THIS WARRANTY IS YOUR EXCLUSIVE WARRANTY AND REPLACES ALL OTHER WARRANTIES OR CONDITIONS, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

IBM does not warrant uninterrupted or error-free operation of any deliverable or Service or that IBM will correct all defects. Unless IBM specifies otherwise. It provides Materials and non-



IBM Services WITHOUT WARRANTIES OF ANY KIND. However, non-IBM suppliers may provide their own warranties to you.

LABOR CATEGORIES AND DESCRIPTIONS

SIN 132-62 Labor Category	SIN 132-62 Labor Description
Security Project Executive	Up to 20 years of progressive experience. Acts as a management authority for client engagements. Performs management of overall contract support operations, organizes, directs and coordinates the planning and production of contract support activities. Manages and coordinates resources, satisfying contract terms, and securing customer satisfaction. Monitors progress of project. Provides primary interface with client management personnel regarding strategic issues. (HSPD-12) Certification required: CISA, CISM or CISSP.
Trusted Identity Security and Privacy SME	Up to 15 years of progressive accomplishment as experts in large and complex information technology systems implementation. Under minimal direction, provides support for security related programs, policies and initiatives. Develops, establishes, and applies knowledge of security principles, concepts and industry practices and standards in the analysis of information and projects. Provides a solid understanding of federal information security/assurance policies, standards and regulations. Familiar with the latest relevant security standards, including FIPS 201 and the related NIST special publications, as well as the associated technologies to include credentialing topics such as PKI, biometrics, and smart cards. Utilizes his/her advanced skills and experience in systems development, detailed knowledge of business processes, technical background and security skills to implement business and security solutions. Performs analysis of security related risks, threats and vulnerabilities of systems, networks and applications. Recommends strategies to prevent security exposure and detect intrusions. Provides direction to IBM project teams and interact with clients at the supervisory level. (HSPD-12) Certification required: CISA, CISM, CISSP
Senior Web Architect	Up to 15 years of progressive experience. Leads or supports requirements analysis, design, development or maintenance of technical integrations or infrastructures for internal and external web applications, protocols, SOA implementations and interfaces. Certified as CISSP, CISM or CISA. Supports HSPD-12, Real ID and other credentialing initiatives or smartcard implementations.
Trusted Identity Project Manager	Up to 15 years of progressive experience. Acts as the overall lead - manager and administrator for the contract effort. Manages all phases of projects from inception through

SIN 132-62 Labor Category	SIN 132-62 Labor Description
	<p>completion. Establishes milestones, and monitors adherence to master plans and schedules. Implementing detailed management techniques such as Critical Path Method (CPM) and Earned Value Analysis. Detailed functional analysis and gap/fit analysis of Government-Off-the-Shelf (GOTS) and/or Commercial-Off-the-Shelf (COTS) software packages. Expert in Security Management. Knowledgeable of GSA HSPD 12 authorized products and services, Real ID requirements, and NIST standards. Detailed migration planning and trade-off analysis. Certification requirements: CISA, CISM, CISSP. Directs daily staff and task activities to meet client and corporate work objectives. Works with team members to resolve difficult problems. (HSPD-12)</p>
<p>Trusted Identity Quality Assurance Specialist - Senior</p>	<p>Up to 15 years of progressive experience. Able to execute the QA/QC process by reviewing work products for correctness, and adherence to the design concepts an standards, and reviewing program documentation to ensure adherence to standards and requirements. Coordinate with the project manager to ensure problem resolution and client satisfaction. Knowledgeable of FISMA, NIST and other security standards and regulatory mandates. Review software design, change specifications, and related plans against contractual requirements. (HSPD-12)</p>
<p>Trusted Identity Systems Architect/ Engineer - Lead</p>	<p>Up to 15 years of progressive accomplishment as experts in large and complex information technology systems implementation. Familiar with the latest relevant security standards, including FIPS 201 and the related NIST special publications, as well as the associated technologies to include PKI, biometrics, and smart cards. Ensures proper governance of program architecture. Able to design and develop new IT products based on client requirement and technical drivers. Performs major enhancements to existing IT systems. Serves as a technical expert, addressing problems of systems integration, compatibility, and multiple platforms. Evaluates and recommend appropriate hardware and network infrastructure based on cost, performance, need, quality, security and reliability. Strong understanding of network security including configuring and using firewall and IDS equipment, end-to-end information assurance, correlating security events across events across a WAN, TCP/IP DNS, firewall Technologies, IDS/IPS, anti-virus technologies, secure telecommunications, two-factor authentication, encryption, PKI/Digital certificates, SSL based VPN solutions, web protocols and Identity Management. (HSPD-12)</p>

SIN 132-62 Labor Category	SIN 132-62 Labor Description
Identity Management Privacy Analyst	Up to 12 years of progressive accomplishment as experts in large and complex information technology systems implementation. Creates analyses and develops strategies, policies, architectures, and privacy assessments to meet Federal mandates. Implements privacy practices in the organization, including collaboration with all the necessary functions (e.g. Legal, ADS, and HR etc). Knowledgeable of NIST PIV requirements, HSPD 12 and State privacy laws in support of Real ID. Monitors all ongoing activities related to the development, implementation, maintenance of, and adherence to, the organization's policies and procedures covering the privacy of, and access to, customer personal information in compliance with Federal law. Extend compliance process to all affiliated and non-affiliated third parties as appropriate. (HSPD-12)
Trusted Identity Training Lead – Senior	Up to 10 years of progressive accomplishment as experts in large and complex information technology systems implementation. Up to 10 years of progressive accomplishment as experts in large and complex information technology systems implementation. Leads the effort to design, develop, implement, and conduct training and instructions of technical-based subject matter. Defines training requirements, training objectives and test methods and designs instructionally valid training materials. Develops computer-based training objectives and methodologies. Coordinates with subject matter expert to design training strategy; designs courseware, including structuring training classes, creates lesson text, provides documentation for software training, tests training programs, presents training programs to users. May conducts research into new training, educational and multimedia technologies. (HSPD-12)
Quality Assurance Analyst	Up to 10 years of progressive experience. Provides IV&V, QA/QC, survey and testing services by reviewing trusted identity processes ,technologies or work products for correctness and adherence to NIST standards, design concepts or and reviewing program documentation and requirements. Knowledgeable of FISMA, NIST and other security standards and regulatory mandates. Certified CISSP, CISA or CISM.
Business Operations Specialist - Senior	Up to 8 years of progressive experience. Supports level of project business activity by planning, directing, and coordinating the total operations of the project. Monitors daily operations to ensure contract requirements are met. Keeps abreast of major situations affecting service to customer and ensures all aspect of client satisfaction. (HSPD-12)

SIN 132-62 Labor Category	SIN 132-62 Labor Description
Identity Management IT Systems Engineer	Up to 12 years of progressive experience. Applies logical analyses or test and evaluation on programs within the contractual scope. Analyzes user needs and identifies resources required for each task to determine functional requirements. Assists in designing and development of new systems or modifies existing systems according to client's needs. Assists higher-level analysts in analyzing alternative systems, cost aspects and feasibility factors. Familiar with the latest relevant security standards, including FIPS 201 and the related NIST special publications, as well as the associated technologies to include PKI, biometrics, and smart cards. (HSPD-12)
Security Change Management Consultant - Mid Level	Up to 12 years of progressive experience. Applies organizational change management processes and methodologies to facilitate communication of change messages. Prepares, maintains and inventories associated technical drawings for assigned projects. Researches data, and creates and maintains inventory and other databases for assigned projects. Prepares configuration change requests and verifies tracks and documents configuration changes. (HSPD-12)
Trusted Identity Database Administrator	Up to 10 years of progressive experience .Act as the overall lead and manager of database system management projects. Design software tools and subsystems to support and manage software systems implementation. Manage software development and support using formal specifications, data flow diagrams, other accepted design techniques, and Computer Aided Software Engineering (CASE) tools. Knowledgeable of supporting database packages supporting privacy and security for the protection of and administration of identities. Knowledgeable of entity analytics software packages is desired. Provide technical expertise and guidance in the logical and physical database design, development, transition, operation and maintenance of database management systems. (HSPD-12)
Security Business Process Functional Senior Analyst – Senior	Up to 10 years of progressive experience. Serves as lead BPR functional Subject Matter Expert (SME) in their area of specialty. Applies their broad skills and specialized functional and technical expertise to guide project teams in delivering client solutions or to manage the day-to-day operations of IBM projects. Core job responsibilities to include design and implement new organizational structures, assist client to translate its vision and strategy into core human resource and business process. Lead clients through streamlining, reengineering and transforming business

SIN 132-62 Labor Category	SIN 132-62 Labor Description
	processes. (HSPD-12)
Trusted Identity Senior Computer Specialist/ Programmer	Up to 10 years of progressive experience. Defines business and technical requirement, establish scope, project plans, priorities and manage the efforts in delivering software applications. Design software tools and subsystems to support and manage software systems implementation. Manage software development and support using formal specifications, data flow diagrams, other accepted design techniques, and Computer Aided Software Engineering (CASE) tools. Provides leadership knowledge of computer science principles to perform complex software engineering assignments relative to the modification and/or development of software systems. Manages, formulates and develops systems or subsystems architecture, requirements, and design documents. (HPSD-12)
Web Architect	Up to 8 year of progressive experience. Provides support and design, develop and maintain a technical infrastructure for internal and external web applications. Develops web pages, page components and web application code/components for client. Manages designs, codes, tests, debugs and document programs. Participates in the technical design, development, testing, implementation and maintenance of client's website. (HSPD-12)
Identity Management Systems Security Engineer	Up to 10 years of progressive accomplishment as experts in large and complex information technology systems implementation. Experience to include defining computer security requirements for high-level applications, evaluation of approved security product capabilities, and developing solutions to Multilevel Security (MLS) problems. Analyzes and defines security requirements for MLS issues. Designs, develops, engineers, tests and implements solutions to MLS requirements. Responsible for implementation and development of MLS. Familiar with the latest relevant security standards, including FIPS 201 and the related NIST special publications, as well as the associated technologies to include PKI, biometrics, and smart cards. Participates in planning and installation of new security related hardware and networks. Strong understanding of network security including configuring and using firewall and IDS equipment, end-to-end information assurance, correlating security events across events across a WAN, TCP/IP DNS, firewall Technologies, IDS/IPS, anti-virus technologies, routers, bridges, two-factor authentication, encryption, PKI/Digital certificates, SSL based VPN solutions and Identity

SIN 132-62 Labor Category	SIN 132-62 Labor Description
	Management. (HSPD-12)
Trusted Identity Computer Security Analyst	Up to 8 years of progressive experience. Analyze criteria for access controls, storage, reproduction, transmission, and destruction of data maintained automated systems requiring protection. Performs IT security assessments and evaluations. Plans and conducts security risk analysis, security evaluations, and audits of information processing system Familiar with the latest relevant security standards, including FIPS 201 and the related NIST special publications, as well as the associated technologies to include PKI, biometrics, and smart cards. Determines computer security compliance and effectiveness of information processing systems. Performs security awareness training. Strong understanding of network security including configuring and using firewall and IDS equipment, end-to-end information assurance, correlating security events across events across a WAN, TCP/IP DNS, firewall Technologies, IDS/IPS, anti-virus technologies, routers, bridges, two-factor authentication, encryption, PKI/Digital certificates, SSL based VPN solutions and Identity Management. (HSPD-12)
Trusted Identity Computer Specialist/ Programmer	Up to 7 years of progressive experience. Provides mid-level analytical and problem solving skills when addressing and resolving issues, assessing possible system impacts, and recommending technical solutions. Provides knowledge of computer science principles to perform complex software engineering assignments relative to the modification and/or development of software systems. Performs software algorithm development, design, coding, and documentation work of systems. Familiar with modeling in UML using Rational Rose Real-time, coding in C++ using Rational Rose Real-time, C++ development using Microsoft Visual, GUI development in a Windows environment, and Object Oriented Design. (HSPD-12)
Security Business Process Functional Analyst	Up to 5 years of progressive experience. Provides BPR subject matter expertise to assist in implementing business process solutions. Assists in client's current business process flows. (HSPD-12)
Identity Management IT Software Specialist	Up to 8 years of progressive experience. Provides assistance in addressing software issues during IT engagements. Delivers a set of functional and technical services to assess, plan and implement software process improvement efforts for software development and maintenance to keep abreast with technological progress, economic change, and business needs. Involvement with software and hardware upgrades, planning and roll out of desktop and Laptop PC's.



SIN 132-62 Labor Category	SIN 132-62 Labor Description
	Knowledgeable of Web applications or Tivoli TIM/TAM/FIM. Review existing software programs and assist in making refinements, reducing operating time, and improving current development methods. (HPSD-12)
Trusted Identity Database Analyst	Up to 6 years of progressive accomplishment as experts in large and complex information technology systems implementation. Perform data analysis, database design, development activities, and implementation, as directed, for databases and database conversions. Develop and test logical and physical database designs. Review logical and physical designs of existing databases and perform tuning, in coordination with the DBA to ensure maximum operating efficiency. (HSPD-12)
Trusted Identity IT Hardware Specialist	Up to 6 years of progressive experience. Provides assistance in addressing hardware issues during IT engagements. Ability to work with client, identifies issues, and quickly provides resolution. Assist with the deployment of hardware to client including installation, configuration and testing. Analyzes customer LAN/WAN hardware/software Requirement. Designs LAN/WAN and recommends hardware, software, and communications solutions. Provides recommended solutions for future LAN/WAN growth. Provides solutions for problems incurred during LAN/WAN installations. Provides after-hours service for escalated issues. (HSPD-12)
Trusted Identity Trainer	Up to 6 years of progressive experience. Conducts the research necessary to develop and revise training courses and prepares appropriate training catalogs. Prepares all instructor materials (course outline, background material, and training aids). Prepares all student materials (course manuals, workbooks, handouts, completion certificates, and course critique forms). Train personnel by conducting formal classroom courses, workshops, and seminars. Provides daily supervision and direction to staff. (HSPD-12)
Trusted Identity Database Programmer	Up to 5 years of progressive experience. Performs analysis and programming of databases. Under general direction, designs, implements, and maintains moderately complex databases with respect to operating system, access control methods, validation checks, organization and statistical methods. Maintains database dictionaries, and integrates system through database design. (HSPD-12)
Security Document/Technical Writer	Up to 3 years of progressive experience. Reviews and edits highly complex written and graphic technical materials, including system configuration, documentation, studies, reports and other presentation graphics. Plans, writes, and maintains documentation pertaining to procedures, internal

SIN 132-62 Labor Category	SIN 132-62 Labor Description
	references manuals and knowledge bases. (HSPD-12)
Business Operations Specialist - Junior	Up to 3 years of progressive experience. Supports basic day-to-day functional management activities within the PMO. Maintain responsibility for budgeting, internal coordination, and reporting, estimating and financial analysis for the project. (HSPD-12)
Identity Management Computer Specialist/Data Entry – Junior	Up to 3 years of progressive experience. Applies knowledge of computer science principles to perform software engineering assignments relative to the modification and/or development of software systems. Formulates and develops systems or subsystems architecture, requirements, and design documents. Performs software algorithm development, design, and coding, of systems. Familiar with Tivoli TIM/TAM/FIM or WebSphere and other Web development software packages. (HPSD-12)
Trusted Identity Help Desk Specialist	Up to 2 years of progressive experience. Under direct supervision, provides customer assistance with routine inquiries, and problems such as software, hardware and network operations. Responds to and diagnoses problems through discussions with users. Includes problem recognition, research, isolation, and resolution steps. (HSPD-12)
Trusted Identity IT System Analyst - Junior	Up to 3 years of progressive experience. Assists Sr. IT Systems Analyst in preparing input and test data for the proposed system. Help develop plans for systems from project inception to conclusion. Analyzes the problem and information to be processes. Assists in designing and development of new systems or modifies existing systems according to client's needs. (HSPD-12)



LABOR RATES

Proposed GFY08-GFY12 SIN 132-62 Rates					
Labor Category	GFY08	GFY09	GFY10	GFY11	GFY12
Security Project Executive	\$272	\$278	\$284	\$292	\$300
Trusted Identity Security and Privacy SME	\$242	\$248	\$254	\$261	\$268
Senior Web Architect	\$226	\$231	\$236	\$243	\$249
Trusted Identity Project Manager	\$195	\$199	\$204	\$210	\$216
Trusted Identity Quality Assurance Specialist-Senior	\$195	\$199	\$204	\$210	\$216
Trusted Identity Systems Architect/ Engineer - Lead	\$195	\$199	\$204	\$210	\$216
Identity Management Privacy Analyst	\$180	\$184	\$188	\$193	\$198
Trusted Identity Training Lead – Senior	\$170	\$174	\$178	\$183	\$188
Quality Assurance Analyst	\$159	\$163	\$167	\$172	\$177
Business Operations Specialist - Senior	\$154	\$158	\$162	\$167	\$171
Identity Management IT Systems Engineer	\$154	\$158	\$162	\$167	\$171
Security Change Management Consultant - Mid Level	\$154	\$158	\$162	\$167	\$171
Trusted Identity Database Administrator	\$154	\$158	\$162	\$167	\$171
Security Business Process Functional Senior Analyst – Senior	\$150	\$153	\$157	\$162	\$166
Trusted Identity Senior Computer Specialist/ Programmer	\$150	\$153	\$157	\$162	\$166
Web Architect	\$144	\$147	\$150	\$154	\$158
Identity Management Systems Security Engineer	\$144	\$147	\$150	\$154	\$158
Trusted Identity Computer Security Analyst	\$144	\$147	\$150	\$154	\$158
Trusted Identity Computer Specialist/ Programmer –	\$144	\$147	\$150	\$154	\$158
Security Business Process Functional Analyst	\$134	\$137	\$140	\$144	\$148
Identity Management IT Software Specialist	\$129	\$132	\$135	\$139	\$143
Trusted Identity Database Analyst	\$129	\$132	\$135	\$139	\$143
Trusted Identity IT Hardware Specialist	\$129	\$132	\$135	\$139	\$143
Trusted Identity Trainer	\$126	\$129	\$132	\$136	\$140
Trusted Identity Database Programmer	\$123	\$126	\$129	\$133	\$137
Security Document/Technical Writer	\$118	\$121	\$124	\$128	\$131
Business Operations Specialist - Junior	\$113	\$116	\$119	\$122	\$125
Identity Management Computer Specialist/Data Entry – Junior	\$93	\$95	\$97	\$100	\$103
Trusted Identity Help Desk Specialist	\$93	\$95	\$97	\$100	\$103
Trusted Identity IT System Analyst - Junior	\$93	\$95	\$97	\$100	\$103
	Rates include .75% IFF				



