



STATE OF UTAH COOPERATIVE CONTRACT AMENDMENT

AMENDMENT #: 4

CONTRACT #: AR2484

Starting Date: Unchanged

Expiration Date: Unchanged

TO BE ATTACHED AND MADE PART OF the specified contract by and between the State of Utah Division of Purchasing and ECS Federal LLC (Referred to as CONTRACTOR).

BOTH PARTIES AGREE TO AMEND THE CONTRACT AS FOLLOWS:

As a result of the Cloud Solutions "refresh" under solicitation # SK18008, Contractor's master agreement is amended to incorporate Platform as a Service (PaaS) into the Agreement's awarded scope.

- Attached Exhibit 2 to Master Agreement: Platform-as-a-Service is incorporated as an exhibit into Attachment A.
- Attached Attachment B Scope of Services Awarded to Contractor is incorporated into the current Attachment B.
- Attached Attachment C Pricing Discounts and Pricing Schedule is incorporated into the current Attachment C.

Effective Date of Amendment: 4/29/2019

All other terms and conditions of the contract, including those previously modified, shall remain in full force and effect.

IN WITNESS WHEREOF, the parties sign and cause this contract to be executed.

CONTRACTOR

John Norell
Digitally signed by John Norell
DN: cn=John Norell, o=ECS Federal, LLC,
ou=Contracts Department,
email=john.norell@ecs.federal.com, c=US
Date: 2019.05.10 13:48:09 -0400

05/10/2019

Contractor's Signature

Date

STATE OF UTAH

Christopher Hughes
Christopher Hughes (May 13, 2019)

May 13, 2019

Director, State of Utah Division of Purchasing

Date

John Norell

Contractor's Name (Print)

Senior Contracts Manager

Title (Print)

For Division of Purchasing Internal Use

Purchasing Agent	Phone #	E-mail Address	Contract #
Solomon Kingston	801-538-3228	skingston@utah.gov	AR2476

Exhibit 2 to the Master Agreement: Platform-as-a-Service

1. Data Ownership: The Purchasing Entity will own all right, title and interest in its data that is related to the Services provided by this Master Agreement. The Contractor shall not access Purchasing Entity user accounts or Purchasing Entity data, except (1) in the course of data center operations, (2) in response to service or technical issues, (3) as required by the express terms of this Master Agreement, Participating Addendum, SLA, and/or other contract documents, or (4) at the Purchasing Entity's written request.

Contractor shall not collect, access, or use user-specific Purchasing Entity Data except as strictly necessary to provide Service to the Purchasing Entity. No information regarding a Purchasing Entity's use of the Service may be disclosed, provided, rented or sold to any third party for any reason unless required by law or regulation or by an order of a court of competent jurisdiction. This obligation shall survive and extend beyond the term of this Master Agreement.

2. Data Protection: Protection of personal privacy and data shall be an integral part of the business activities of the Contractor to ensure there is no inappropriate or unauthorized use of Purchasing Entity information at any time. To this end, the Contractor shall safeguard the confidentiality, integrity and availability of Purchasing Entity information and comply with the following conditions:

- a. The Contractor shall implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of Personal Data and Non-Public Data. Such security measures shall be in accordance with recognized industry practice and not less stringent than the measures the Contractor applies to its own Personal Data and Non-Public Data of similar kind.
- b. All data obtained by the Contractor in the performance of the Master Agreement shall become and remain the property of the Purchasing Entity.
- c. All Personal Data shall be encrypted at rest and in transit with controlled access. Unless otherwise stipulated, the Contractor is responsible for encryption of the Personal Data. Any stipulation of responsibilities will identify specific roles and responsibilities and shall be included in the service level agreement (SLA), or otherwise made a part of the Master Agreement.
- d. Unless otherwise stipulated, the Contractor shall encrypt all Non-Public Data at rest and in transit. The Purchasing Entity shall identify data it deems as Non-Public Data to the Contractor. The level of protection and encryption for all Non-Public Data shall be identified in the SLA.
- e. At no time shall any data or processes — that either belong to or are intended for the use of a Purchasing Entity or its officers, agents or employees — be copied, disclosed or retained by the Contractor or any party related to the Contractor for subsequent use in any transaction that does not include the Purchasing Entity.
- f. The Contractor shall not use any information collected in connection with the Services issued from this Master Agreement for any purpose other than fulfilling the Services.

3. Data Location: The Contractor shall provide its services to the Purchasing Entity and its end users solely from data centers in the U.S. Storage of Purchasing Entity data at rest shall be located solely in data centers in the U.S. The Contractor shall not allow its personnel or contractors to store Purchasing Entity data on portable devices, including personal computers, except for devices that are used and kept only at its U.S. data centers. The Contractor shall permit its personnel and contractors to access Purchasing Entity data remotely only as required to provide technical support. The Contractor may provide technical user support on a 24/7 basis using a Follow the Sun model, unless otherwise prohibited in a Participating Addendum.

4. Security Incident or Data Breach Notification: The Contractor shall inform the Purchasing Entity of any security incident or data breach within the possession and control of the Contractor and related to the service provided under the Master Agreement, Participating Addendum, or SLA. Such notice shall include, to the best of Contractor's knowledge at that time, the persons affected, their identities, and the Confidential Information and Data disclosed, or shall include if this information is unknown.

a. Incident Response: The Contractor may need to communicate with outside parties regarding a security incident, which may include contacting law enforcement, fielding media inquiries and seeking external expertise as mutually agreed upon, defined by law or contained in the Master Agreement, Participating Addendum, or SLA. Discussing security incidents with the Purchasing Entity should be handled on an urgent as-needed basis, as part of Contractor's communication and mitigation processes as mutually agreed, defined by law or contained in the Master Agreement, Participating Addendum, or SLA.

b. Security Incident Reporting Requirements: Unless otherwise stipulated, the Contractor shall immediately report a security incident related to its service under the Master Agreement, Participating Addendum, or SLA to the appropriate Purchasing Entity.

c. Breach Reporting Requirements: If the Contractor has actual knowledge of a confirmed data breach that affects the security of any Purchasing Entity data that is subject to applicable data breach notification law, the Contractor shall (1) promptly notify the appropriate Purchasing Entity within 24 hours or sooner, unless shorter time is required by applicable law, and (2) take commercially reasonable measures to address the data breach in a timely manner

5. Breach Responsibilities: This section only applies when a Data Breach occurs with respect to Personal Data within the possession or control of the Contractor.

a. The Contractor, unless stipulated otherwise, shall immediately notify the appropriate Purchasing Entity identified contact by telephone in accordance with the agreed upon security plan or security procedures if it reasonably believes there has been a security incident.

b. The Contractor, unless stipulated otherwise, shall promptly notify the appropriate Purchasing Entity identified contact within 24 hours or sooner by telephone, unless shorter time is required by applicable law, if it has confirmed that there is, or reasonably believes that there has been a data breach. The Contractor shall (1) cooperate with the Purchasing Entity as reasonably

requested by the Purchasing Entity to investigate and resolve the data breach, (2) promptly implement necessary remedial measures, if necessary, and (3) document responsive actions taken related to the data breach, including any post-incident review of events and actions taken to make changes in business practices in providing the services, if necessary.

c. Unless otherwise stipulated, if a Data Breach is a direct result of Contractor's breach of its contractual obligation to encrypt Personal Data or otherwise prevent its release, the Contractor shall bear the costs associated with (1) the investigation and resolution of the data breach; (2) notifications to individuals, regulators or others required by federal and state laws or as otherwise agreed to; (3) a credit monitoring service required by state (or federal) law or as otherwise agreed to; (4) a website or a toll-free number and call center for affected individuals required by federal and state laws — all not to exceed the average per record per person cost calculated for data breaches in the United States (currently \$217 per record/person) in the most recent Cost of Data Breach Study: Global Analysis published by the Ponemon Institute at the time of the data breach; and (5) complete all corrective actions as reasonably determined by Contractor based on root cause.

6. Notification of Legal Requests: The Contractor shall contact the Purchasing Entity upon receipt of any electronic discovery, litigation holds, discovery searches and expert testimonies related to the Purchasing Entity's data under the Master Agreement, or which in any way might reasonably require access to the data of the Purchasing Entity. The Contractor shall not respond to subpoenas, service of process and other legal requests related to the Purchasing Entity without first notifying and obtaining the approval of the Purchasing Entity, unless prohibited by law from providing such notice.

7. Termination and Suspension of Service:

a. In the event of an early termination of the Master Agreement, Participating or SLA, Contractor shall allow for the Purchasing Entity to retrieve its digital content and provide for the subsequent secure disposal of the Purchasing Entity's digital content.

b. During any period of service suspension, the Contractor shall not take any action to intentionally erase or otherwise dispose of any of the Purchasing Entity's data.

c. In the event of early termination of any Services or agreement in entirety, the Contractor shall not take any action to intentionally erase any Purchasing Entity's data for a period of 1) 45 days after the effective date of termination, if the termination is for convenience; or 2) 60 days after the effective date of termination, if the termination is for cause. After such day period, the Contractor shall have no obligation to maintain or provide any Purchasing Entity data and shall thereafter, unless legally prohibited, delete all Purchasing Entity data in its systems or otherwise in its possession or under its control. In the event of either termination for cause, the Contractor will impose no fees for access and retrieval of digital content to the Purchasing Entity.

d. The Purchasing Entity shall be entitled to any post termination assistance generally made available with respect to the services, unless a unique data retrieval arrangement has been established as part of an SLA.

e. Upon termination of the Services or the Agreement in its entirety, Contractor shall securely dispose of all Purchasing Entity's data in all of its forms, such as disk, CD/ DVD, backup tape and paper, unless stipulated otherwise by the Purchasing Entity. Data shall be permanently deleted and shall not be recoverable, according to National Institute of Standards and Technology (NIST)-approved methods. Certificates of destruction shall be provided to the Purchasing Entity.

8. Background Checks:

a. Upon the request of the Purchasing Entity, the Contractor shall conduct criminal background checks and not utilize any staff, including subcontractors, to fulfill the obligations of the Master Agreement who have been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise convicted of any felony or misdemeanor offense for which incarceration for up to 1 year is an authorized penalty. The Contractor shall promote and maintain an awareness of the importance of securing the Purchasing Entity's information among the Contractor's employees and agents.

b. The Contractor and the Purchasing Entity recognize that security responsibilities are shared. The Contractor is responsible for providing a secure infrastructure. The Purchasing Entity is responsible for its secure guest operating system, firewalls and other logs captured within the guest operating system. Specific shared responsibilities are identified within the SLA.

c. If any of the stated personnel providing services under a Participating Addendum is not acceptable to the Purchasing Entity in its sole opinion as a result of the background or criminal history investigation, the Purchasing Entity, in its' sole option shall have the right to either (1) request immediate replacement of the person, or (2) immediately terminate the Participating Addendum and any related service agreement.

9. Access to Security Logs and Reports:

a. The Contractor shall provide reports on a schedule specified in the SLA to the Purchasing Entity in a format as specified in the SLA and agreed to by both the Contractor and the Purchasing Entity. Reports will include latency statistics, user access, user access IP address, user access history and security logs for all Purchasing Entity files related to the Master Agreement, Participating Addendum, or SLA.

b. The Contractor and the Purchasing Entity recognize that security responsibilities are shared. The Contractor is responsible for providing a secure infrastructure. The Purchasing Entity is responsible for its secure guest operating system, firewalls and other logs captured within the guest operating system. Specific shared responsibilities are identified within the SLA.

10. Contract Audit: The Contractor shall allow the Purchasing Entity to audit conformance to the Master Agreement terms. The Purchasing Entity may perform this audit or contract with a third party at its discretion and at the Purchasing Entity's expense.

11. Data Center Audit: The Contractor shall perform an independent audit of its data centers at least annually at its expense, and provide an unredacted version of the audit report upon request to a Purchasing Entity. The Contractor may remove its proprietary information from the unredacted version. A Service Organization Control (SOC) 2 audit report or approved equivalent sets the minimum level of a third-party audit.

12. Change Control and Advance Notice: The Contractor shall give a minimum forty eight (48) hour advance notice (or as determined by a Purchasing Entity and included in the SLA) to the Purchasing Entity of any upgrades (e.g., major upgrades, minor upgrades, system changes) that may impact service availability and performance. A major upgrade is a replacement of hardware, software or firmware with a newer or better version in order to bring the system up to date or to improve its characteristics. It usually includes a new version number.

Contractor will make updates and upgrades available to Purchasing Entity at no additional costs when Contractor makes such updates and upgrades generally available to its users.

No update, upgrade or other charge to the Service may decrease the Service's functionality, adversely affect Purchasing Entity's use of or access to the Service, or increase the cost of the Service to the Purchasing Entity.

Contractor will notify the Purchasing Entity at least sixty (60) days in advance prior to any major update or upgrade.

13. Security: As requested by a Purchasing Entity, the Contractor shall disclose its non-proprietary system security plans (SSP) or security processes and technical limitations to the Purchasing Entity such that adequate protection and flexibility can be attained between the Purchasing Entity and the Contractor. For example: virus checking and port sniffing — the Purchasing Entity and the Contractor shall understand each other's roles and responsibilities.

14. Non-disclosure and Separation of Duties: The Contractor shall enforce separation of job duties, require commercially reasonable non-disclosure agreements, and limit staff knowledge of Purchasing Entity data to that which is absolutely necessary to perform job duties.

15. Import and Export of Data: The Purchasing Entity shall have the ability to import or export data in piecemeal or in entirety at its discretion without interference from the Contractor at any time during the term of Contractor's contract with the Purchasing Entity. This includes the ability for the Purchasing Entity to import or export data to/from other Contractors. Contractor shall specify if Purchasing Entity is required to provide its' own tools for this purpose, including the optional purchase of Contractors tools if Contractors applications are not able to provide this functionality directly.

16. Responsibilities and Uptime Guarantee: The Contractor shall be responsible for the acquisition and operation of all hardware, software and network support related to the services being provided. The technical and professional activities required for establishing, managing and maintaining the environments are the responsibilities of the Contractor. The system shall be available 24/7/365 (with agreed-upon maintenance downtime), and provide service to customers as defined in the SLA.

17. Subcontractor Disclosure: Contractor shall identify all of its strategic business partners related to services provided under this Master Agreement, including but not limited to all subcontractors or other entities or individuals who may be a party to a joint venture or similar agreement with the Contractor, and who shall be involved in any application development and/or operations.

18. Business Continuity and Disaster Recovery: The Contractor shall provide a business continuity and disaster recovery plan upon request and ensure that the Purchasing Entity's recovery time objective (RTO) of XXX hours/days is met. (XXX hour/days shall be provided to Contractor by the Purchasing Entity.) Contractor must work with the Purchasing Entity to perform an annual Disaster Recovery test and take action to correct any issues detected during the test in a time frame mutually agreed between the Contractor and the Purchasing Entity.

19. Compliance with Accessibility Standards: The Contractor shall comply with and adhere to Accessibility Standards of Section 508 Amendment to the Rehabilitation Act of 1973 or any other state laws or administrative regulations identified by the Participating Entity..

20. Web Services: The Contractor shall use Web services exclusively to interface with the Purchasing Entity's data in near real time.

21. Encryption of Data at Rest: The Contractor shall ensure hard drive encryption consistent with validated cryptography standards as referenced in FIPS 140-2, Security Requirements for Cryptographic Modules for all Personal Data as identified in the SLA, unless the Contractor presents a justifiable position that is approved by the Purchasing Entity that Personal Data, is required to be stored on a Contractor portable device in order to accomplish work as defined in the scope of work.

22. Subscription Terms: Contractor grants to a Purchasing Entity a license to: (i) access and use the Service for its business purposes; (ii) for PaaS, use underlying software as embodied or used in the Service; and (iii) view, copy, upload and download (where applicable), and use Contractor's documentation.

No Contractor terms, including standard click through license or website terms or use of privacy policy, shall apply to Purchasing Entities unless such terms are included in this Master Agreement.

Attachment B – Scope of Services Awarded to Contractor

1.1 Awarded Service Model(s).

Contractor is awarded the following Service Models:

- Infrastructure as a Service (IaaS)
- Platform as a Service (PaaS)
- Software as a Service (SaaS)

1.2 Risk Categorization.*

Contractor's offered solutions offer the ability to store and secure data under the following risk categories:

Service Model	Low Risk Data	Moderate Risk Data	High Risk Data	Deployment Models Offered
IaaS	x	x	x	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
SaaS	x	x	x	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
PaaS	Amazon Aurora	Amazon Aurora	Amazon Aurora	Private Cloud, Public Cloud, Hybrid Cloud
PaaS	Amazon RedShift	Amazon RedShift	Amazon RedShift	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
PaaS	Amazon Relational Database Service (RDS)	Amazon Relational Database Service (RDS)	Amazon Relational Database Service (RDS)	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
PaaS	Amazon DynamoDB	Amazon DynamoDB	Amazon DynamoDB	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
PaaS	AWS Database Migration Service	AWS Database Migration Service	AWS Database Migration Service	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
PaaS	Amazon Elastic MapReduce (EMR)	Amazon Elastic MapReduce (EMR)	Amazon Elastic MapReduce (EMR)	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
PaaS	Amazon Elastic File System (EFS)	Amazon Elastic File System (EFS)	Amazon Elastic File System (EFS)	Private Cloud, Public Cloud, Hybrid Cloud
PaaS	Amazon Elastic Container Service for Kubernetes	Amazon Elastic Container Service for Kubernetes (Amazon EKS)	Amazon Elastic Container Service for Kubernetes	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud

	(Amazon EKS)		(Amazon EKS)	
PaaS	Amazon Sagemaker	Amazon Sagemaker	Amazon Sagemaker	Private Cloud, Public Cloud, Hybrid Cloud
PaaS	Amazon Elasticsearch	Amazon Elasticsearch	Amazon Elasticsearch	Private Cloud, Community

*Contractor may add additional OEM solutions during the life of the contract.

2.1 Deployment Models.

Contractor may provide cloud based services through the following deployment methods:

- **Private cloud.** The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.
- **Community cloud.** The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.
- **Public cloud.** The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.
- **Hybrid cloud.** The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds)

Attachment C - Pricing Discounts and Schedule

Contractor: ECS Federal LLC

Pricing Notes

1. % discounts are based on minimum discounts off Contractor's commercially published pricelists versus fixed pricing. Nonetheless, Orders will be fixed-price or fixed-rate and not cost reimbursable contracts. Contractor has the ability to update and refresh its respective price catalog, as long as the agreed-upon discounts are fixed.
2. Minimum guaranteed contract discounts do not preclude a Contractor and/or its authorized resellers from providing deeper or additional, incremental discounts at their sole discretion.
3. Purchasing entities shall benefit from any promotional pricing offered by Contractor to similar customers. Promotional pricing shall not be cause for a permanent price change.
4. Contractor's price catalog include the price structures of the cloud service models, value added services (i.e., Maintenance Services, Professional Services, Etc.), and deployment models that it intends to provide including the types of data it is able to hold under each model. Pricing shall all-inclusive of infrastructure and software costs and management of infrastructure, network, OS, and software.

Cloud Service Model: Platform as a Service (PaaS)

Description	Discount
PaaS Minimum Discount % (applies to all OEM's offered within this service model)	2.00%
Average Service Model OEM Discount Off	2.00%

Additional Value Added Services

Item Description	Onsite Hourly Rate		Remote Hourly Rate	
	NVP Price	Catalog Price	NVP Price	Catalog Price
Analyst 1	\$ 116.21	\$118.58	\$ 110.28	\$112.53
Analyst 2	\$ 163.27	\$166.60	\$ 154.94	\$158.10
Analyst 3	\$ 181.52	\$185.22	\$ 172.25	\$175.77
Analyst 4	\$ 210.33	\$214.62	\$ 199.60	\$203.67
Application Support 1	\$ 142.14	\$145.04	\$ 134.89	\$137.64
Application Support 2	\$ 153.66	\$156.80	\$ 145.82	\$148.80
Application Support 3	\$ 160.39	\$163.66	\$ 152.20	\$155.31
Application Support 4	\$ 168.07	\$171.50	\$ 159.50	\$162.75
Consultant 1	\$ 164.23	\$167.58	\$ 155.85	\$159.03
Consultant 2	\$ 184.40	\$188.16	\$ 174.99	\$178.56
Consultant 3	\$ 200.72	\$204.82	\$ 190.48	\$194.37
Customer Support Rep 1	\$ 61.47	\$62.72	\$ 58.33	\$59.52
Customer Support Rep 2	\$ 80.67	\$82.32	\$ 76.56	\$78.12
Customer Support Rep 3	\$ 102.76	\$104.86	\$ 97.52	\$99.51
Deputy Project Manager	\$ 154.62	\$157.78	\$ 146.74	\$149.73
Functional Analyst 1	\$ 106.60	\$108.78	\$ 101.17	\$103.23
Functional Analyst 2	\$ 120.05	\$122.50	\$ 113.93	\$116.25
Functional Analyst 3	\$ 129.65	\$132.30	\$ 123.04	\$125.55
Functional Analyst 4	\$ 138.30	\$141.12	\$ 131.24	\$133.92
Functional Analyst 5	\$ 149.82	\$152.88	\$ 142.18	\$145.08
Information Technology Specialist 1	\$ 58.58	\$59.78	\$ 55.60	\$56.73
Information Technology Specialist 2	\$ 68.19	\$69.58	\$ 64.71	\$66.03
Information Technology Specialist 3	\$ 75.87	\$77.42	\$ 72.00	\$73.47
Information Technology Specialist 4	\$ 81.63	\$83.30	\$ 77.47	\$79.05
Information Technology Support 1	\$ 29.77	\$30.38	\$ 28.25	\$28.83
Information Technology Support 2	\$ 34.57	\$35.28	\$ 32.81	\$33.48
Information Technology Support 3	\$ 41.30	\$42.14	\$ 39.19	\$39.99
Information Technology Support 4	\$ 48.98	\$49.98	\$ 46.48	\$47.43
Program Manager 1	\$ 214.17	\$218.54	\$ 203.24	\$207.39
Program Manager 2	\$ 254.51	\$259.70	\$ 241.52	\$246.45
Project Manager 1	\$ 173.83	\$177.38	\$ 164.96	\$168.33
Project Manager 2	\$ 196.88	\$200.90	\$ 186.84	\$190.65
Project Support Analyst 1	\$ 87.40	\$89.18	\$ 82.94	\$84.63
Project Support Analyst 2	\$ 98.92	\$100.94	\$ 93.87	\$95.79
Security Analyst 1	\$ 90.28	\$92.12	\$ 85.67	\$87.42
Security Analyst 2	\$ 101.80	\$103.88	\$ 96.61	\$98.58
Security Analyst 4	\$ 141.18	\$144.06	\$ 133.98	\$136.71
Senior Consultant 1	\$ 209.37	\$213.64	\$ 198.69	\$202.74
Senior Consultant 2	\$ 225.69	\$230.30	\$ 214.18	\$218.55
Software Integrator 1	\$ 179.59	\$183.26	\$ 170.43	\$173.91
Software Integrator 2	\$ 203.60	\$207.76	\$ 193.22	\$197.16
Software Integrator 3	\$ 224.73	\$229.32	\$ 213.27	\$217.62

Attachment C - Pricing Discounts and Schedule

Contractor: ECS Federal LLC

Software Integrator 4	\$	246.82	\$251.86	\$	234.23	\$239.01
Systems Integrator 1	\$	154.62	\$157.78	\$	146.74	\$149.73
Systems Integrator 2	\$	170.95	\$174.44	\$	162.23	\$165.54
Systems Integrator 3	\$	193.04	\$196.98	\$	183.19	\$186.93
Systems Integrator 4	\$	212.25	\$216.58	\$	201.42	\$205.53
Systems Support 1	\$	115.25	\$117.60	\$	109.37	\$111.60
Systems Support 2	\$	125.81	\$128.38	\$	119.39	\$121.83
Systems Support 3	\$	131.57	\$134.26	\$	124.86	\$127.41
Technical Writer 1	\$	72.99	\$74.48	\$	69.27	\$70.68
Technical Writer 2	\$	92.20	\$94.08	\$	87.49	\$89.28
Technical Writer 3	\$	105.64	\$107.80	\$	100.25	\$102.30
Associate Software Consultant	\$	310.21	\$316.54	\$	294.38	\$300.39
Associate SW Consultant 2	\$	374.56	\$382.20	\$	355.45	\$362.70
Principal Software Consultant	\$	403.37	\$411.60	\$	382.79	\$390.60
Security Consultant 1	\$	305.41	\$311.64	\$	289.83	\$295.74
Security Consultant 2	\$	365.91	\$373.38	\$	347.24	\$354.33
Senior Software Consultant	\$	388.00	\$395.92	\$	388.00	\$395.92
Senior Software Consultant 2	\$	553.19	\$564.48	\$	553.19	\$564.48
Software Consultant	\$	351.51	\$358.68	\$	351.51	\$358.68
Software Consultant 2	\$	458.11	\$467.46	\$	458.11	\$467.46
Software Technician 1	\$	281.40	\$287.14	\$	281.40	\$287.14
Software Technician 2	\$	320.77	\$327.32	\$	320.77	\$327.32
Software Technician 3	\$	389.92	\$397.88	\$	389.92	\$397.88
Software Technician 4	\$	439.86	\$448.84	\$	439.86	\$448.84
Software Technician 5	\$	505.17	\$515.48	\$	505.17	\$515.48
Systems Technician 1	\$	225.69	\$230.30	\$	225.69	\$230.30
Systems Technician 2	\$	255.47	\$260.68	\$	255.47	\$260.68
Technical Expert 1	\$	255.47	\$260.68	\$	255.47	\$260.68
Technical Expert 2	\$	298.68	\$304.78	\$	298.68	\$304.78
Technical Expert 3	\$	337.10	\$343.98	\$	337.10	\$343.98
Training Specialist 1	\$	96.04	\$98.00	\$	91.14	\$93.00
Training Specialist 2	\$	121.01	\$123.48	\$	114.84	\$117.18
Training Specialist 3	\$	144.06	\$147.00	\$	136.71	\$139.50

Deliverable Rates

NVP Price Catalog Price

[Insert additional value added services as necessary]		
[Insert additional value added services as necessary]		