

Washington State Patrol

A Central Computerized Enforcement Service System Message Switch Replacement Project

Request for Proposals

October 16, 2009

TABLE OF CONTENTS

Page

I.	Introduction	2
	A. Scope	2
	B. Contact.....	2
	C. Evaluation Schedule	2
	D. Contract Period	3
II.	Current ACCESS Environment.....	5
	A. Current Model	5
	B. Hardware and Software	7
	C. Network	8
	D. Transactions, Records, and Metrics	10
III.	Target ACCESS Environment and Drivers	13
	A. Future WSP ACCESS Model.....	13
	B. Change Drivers.....	14
	C. Interfaces	15
	D. Key Issues	16
	E. Implementation Strategy	17
	F. Hardware Maintenance and Support Strategy	20
IV.	Standards, Compliance, and Staffing.....	23
	A. Standards and Policies	23
	B. Standards Compliance.....	24
	C. Staffing	27
V.	Proposal Content and Organization	29
	A. Instructions to Vendors	29
	B. Management Response Binder	29
	C. Technical Response Binder.....	43
	D. Cost Response Binder.....	48
VI.	Target ACCESS Environment Requirements.....	51
	A. Functional Specifications.....	51
	B. Technical Specifications	52
	C. Functional and Technical Model Relationships.....	53

TABLE OF CONTENTS
(continued)

	<u>Page</u>
VII. Evaluation Information	55
A. Proposal Evaluation	55
B. Evaluation Criteria	56
VIII. Administrative Rules	59
A. Acquisition Authority.....	59
B. Acceptable Alternative Defined	59
C. Multiple Responses	59
D. Vendor Must Appoint Representative	59
E. Questions and Answers.....	60
F. Mandatory Intent to Respond.....	60
G. Submission of Proposals	60
H. Supplemental Materials.....	61
I. Proprietary Information / Public Disclosure	61
J. Minority and Women-Owned Business Participation	62
K. Acceptance Period.....	62
L. Responsiveness.....	62
M. Award Based On Multiple Factors	63
N. Contract and General Terms and Conditions.....	63
O. Costs to Propose	63
P. No Obligation to Contract.....	63
Q. Funding	63
R. Rejection Of Proposals	63
S. Failure to Comply	63
T. Waivers.....	64
U. Commitment of Funds	64
V. Electronic Payment	64
W. Insurance Coverage	64
X. Response Property of the Agency.....	64
Y. Minor Administrative Irregularities	64
Z. Errors In Response.....	65
AA. RFP Amendments	65
BB. Points of Clarification	65
CC. Right to Cancel	65
DD. No Multiple Award	65
EE. Incorporation of Solicitation Document(s) Into Contract ...	65
FF. Payment for Project Deliverables	66

TABLE OF CONTENTS

(continued)

	<u>Page</u>
GG. No Costs Chargeable	66
HH. Non-Endorsement	66
II. Single Response	66
JJ. Withdrawal of Response.....	66
KK. Announcement of Apparently Successful Vendor	66
LL. Optional Vendor Debriefing	67
MM. Vendor Complaints	67
NN. Protest Procedures.....	67
OO. Covered Services.....	68
PP. Certifications and Assurances	68

Appendix A – ACCESS Message Formats

Appendix B – ACCESS Message Keys

Appendix C – Functional Requirements

Appendix D – Technical Requirements

Appendix E – References Form

Appendix F – Vendor Strength and Stability Form

Appendix G – Proposal Checklist

Appendix H – Cost Forms: Cash Purchase Response

Appendix I – Washington Sample Contract

Appendix J – Certifications and Assurances

Appendix K – Glossary

I. Introduction

I. Introduction

Washington State Patrol (WSP) is pleased to release this Request for Proposals (RFP) to implement the future A Central Computerized Enforcement Service System (ACCESS) message switch. The primary goal of the future ACCESS is to provide flexible, reliable, and accurate message switching and information access within and among law enforcement and criminal justice agencies in Washington State and across the United States.

A. Scope

Through this RFP, WSP seeks to replace the core components of the existing ACCESS message switch. Specific elements sought from prospective bidders include, but are not limited to, the following:

- *Hardware* – Acquisition of core ACCESS Web services, switching/routing, application server, and database equipment.
- *Software* – Acquisition of all necessary software to ensure a fully functional, communicative, and national standards-compliant ACCESS host and related infrastructure. Of particular interest here are the interfaces to the various local, state, and national systems connected to the current system.
- *Services* – Acquisition of all required expert services to ensure successful implementation, migration, conversion, and ongoing management and support of the acquired ACCESS.

More specific requirements are presented in this RFP.

B. Contact

WSP will assign a project manager for the ACCESS Message Switch Replacement Project. A secured Web site has been established that contains all of the reference materials related to this RFP. Reference materials include copies of all standards and policies applicable to this project and interface documentation, as well as forms and templates required in the vendor responses. All reference materials may be found at the following secured Web site:

www.mtgmc.com/projects/WSP-ACCESS-REISSUE/

The password for this site can be obtained by contacting the project manager via e-mail at Steven.Cole@wsp.wa.gov. The project manager will provide a nondisclosure agreement to be completed by the respondent and returned to the ACCESS project manager. Upon receipt of the signed nondisclosure agreement, a password will be issued to the respondent.

C. Evaluation Schedule

The procurement manager will make every effort to adhere to the following schedule:

Ref.	Action	Date
1	RFP Publicly Posted	10/16/2009
2	Vendor Questions Due	10/23/2009
3	Vendor Questions Answered and Addendum Posted by WSP	10/28/2009
4	Vendor Intent to Respond Due	11/6/2009
5	Vendor Proposals Due	11/13/2009
6	Vendor Proposal Scoring	12/4/2009
7	Optional Vendor Demonstrations and Presentations	12/14/2009
8	Identification of Apparent Successful Bidder	1/8/2010
9	Vendor Contract Award	3/1/2010

D. Contract Period

WSP estimates an initial discovery phase duration of 2 months and an implementation duration of 12 months. It is further anticipated that WSP will pursue annual support agreements with the vendor, beyond the length of the coverage of the initial warranty period.

NOTE: The contract for this procurement will not be signed until the funding is secured.

II. Current ACCESS Environment

II. Current ACCESS Environment

This section provides an overview of the current ACCESS operating environment, including a look at each aspect of facilities, hardware, software, databases, and users of the system. ACCESS is operated out of a WSP facility. The data center provides a mission-critical operational environment, including staffing, uninterruptible power supply (UPS), HVAC, and security. *This section is included for informational purposes only and does not specify any requirements for the replacement system except where it describes or alludes to protocols which must be preserved for data source systems and regional service systems.*

A. Current Model

This subsection outlines the current ACCESS model, including a brief historical perspective of ACCESS and a high-level diagram and description of the components of the ACCESS environment.

1. Historical Context

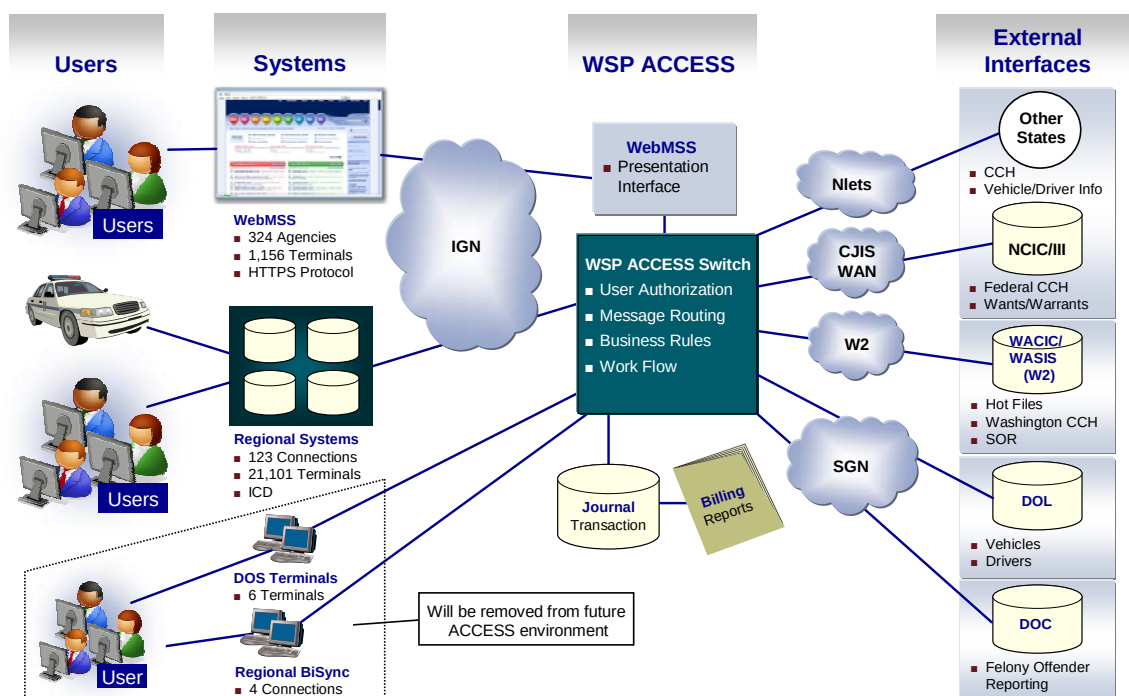
ACCESS is a statewide message switching system. ACCESS was established by WSP in partnership with all subscribing criminal justice agencies throughout the state.

The current ACCESS switch hardware and application were installed in 1997. ACCESS provides a means for the state's criminal justice community to exchange information of critical importance both within the state and across the nation. This information includes all-points bulletins, criminal history, driver and vehicle information, information related to unsolved crimes, wanted and missing persons, and other information necessary in providing service to the public and ensuring their safety. ACCESS provides the means for the exchange of public safety information, but it is not a repository for any of this information.

2. Model Diagram

A depiction of the current ACCESS processing model is presented below.

Current Message Switch Environment



3. Model Elements

The elements of the current ACCESS model are detailed below.

Component	Elements
Users	The following end-user interface devices are employed to access the message switch system: <i>Disk Operating System (DOS) Terminals</i> – Legacy end-user direct-connect interface to ACCESS. This interface will be removed in the future ACCESS environment. <i>WebMSS Interface</i> – Web-based end-user interface to ACCESS. This interface will be replaced in the new ACCESS environment. <i>Regional System User Interface</i> – End-user interface presentation to ACCESS via local agency-owned land- or mobile-based devices. This interface must continue in the new ACCESS environment and cannot be changed.
Systems	Agencies transmit data to the ACCESS switch via a variety of methods, including a Web interface, regional systems, or terminals. <i>WebMSS</i> – WebMSS is the Web-based interface to ACCESS. Users transmit messages to the switch using standard message formatting or through the utilization of masks, which create forms. Agencies that connect to ACCESS via WebMSS do not communicate directly with the switch. A WebMSS server provides the user interface and connects to the switch.

Component	Elements
	• <i>Regional Systems</i> – Agencies may use their own local systems, such as a records management system (RMS), to transmit messages to ACCESS. An Interface Control Document (ICD) is provided to agencies wishing to connect to ACCESS via this method. The ICD provides the formatting standards which must be followed to communicate with ACCESS. The majority of end users connect to ACCESS via these regional systems. These interfaces cannot be changed with the implementation of the new system. • <i>DOS Terminals</i> – The DOS terminals provide a direct connection to the ACCESS switch. The terminals are legacy equipment, with very few users. This method of connection to ACCESS will not be available in the future ACCESS environment. • <i>Regional BiSync</i> – These systems provide a direct connection to the ACCESS switch. The systems have very few users. This method of connection to ACCESS will not be available in the future ACCESS environment.
WSP ACCESS	The ACCESS message switch hardware performs a variety of functions within the ACCESS environment. These functions include: • Processing message headers. • Passing messages to the proper interface(s). • Logging all message transactions and routing the log files to the journal database. • Annual statistical reports are run against the journal logs to produce billing amounts.
External Interfaces	Messages are routed to and from a number of repositories at the state and national levels. The ACCESS switch must adhere to the interface specification for each of these interfaces. These interfaces include: • NCIC/Interstate Identification Index (III). • Nlets – the International Justice & Public Safety Information Sharing Network. • Washington Crime Information Center (WACIC)/Washington State Identification System (WASIS) (W2). • Washington State Department of Licensing (DOL). • Washington State Department of Corrections (DOC).

B. Hardware and Software

This subsection outlines the physical hardware and software products currently deployed in the ACCESS operating environment.

1. Hardware Product Review

The specifics regarding installed hardware infrastructure utilized in the current WSP message switch environment are outlined below.

Ref.	Hardware Product	Year	Application
1	Stratus Continuum 1228: - Two HP PA-RISC 180 MHz processors. - Two 9 GB Ultra 1 SCSI 10,000 RPM hard drives. 4mm DAT SCSI tape drive.	1997	Operating system and ACCESS application software.
2	Stratus Continuum 5200.	2001	Operating system and WebMSS application software.

2. Software Product Review

The table below outlines the specifics regarding the installed software and processing infrastructure for the current WSP message switch environment.

Ref.	Software Product	Application
Operating System and Application		
1	Stratus Virtual Operating System (VOS).	Stratus hardware operating system.
2	Level II, Inc., MAGUS software.	ACCESS message switch software.
3	Microsoft Windows 2000.	WebMSS server operating system software.
4	ACCESS journal (transaction logs).	Journal – logging of all system transactions.
Database		
5	Microsoft SQL Server 2000.	Journal – ACCESS transaction logs.
User Interface		
6	Level II MAGUS Web Interface.	WebMSS user interface to ACCESS.
7	Level II's The Journal (transaction logs).	Remote client interface journal transaction logs.

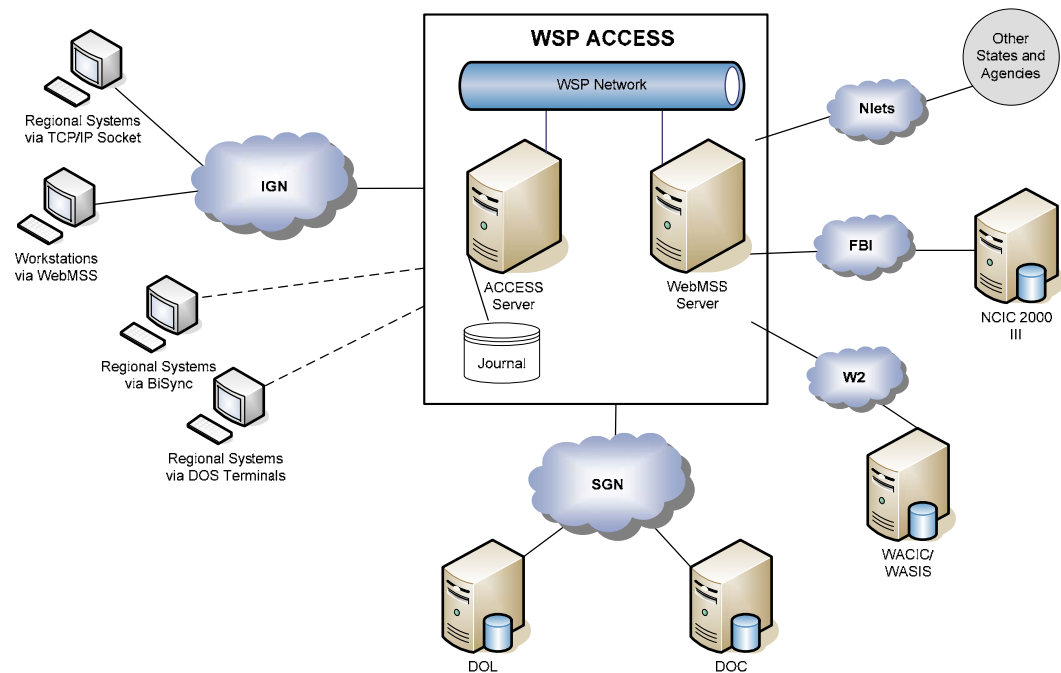
C. Network

This subsection provides an outline of the interfaces and exchanges currently implemented in the ACCESS operating environment.

1. Interface Overview

The diagram below provides a high-level view of the interfaces inherent to the WSP message switch environment.

Message Switch System Interfaces



2. Topology Element Review

The specifics regarding each of the network interface elements utilized in the WSP message switch environment are outlined below.

Ref.	Element Type	Protocol	Quantity	Network
1	Regional Systems	TCP/IP Stream Socket	119 Connections 21,101 Terminals	Inter-governmental Network (IGN)
2	Regional Systems (will be eliminated)	Bisynchronous	4 Connections	Eliminated
3	DOS Terminals (will be eliminated)	Asynchronous	6 Terminals	Eliminated
4	WebMSS Terminals	TCP/IP	324 Agencies 1,156 Terminals	IGN, State Government Network (SGN)
5	W2 Network	TCP/IP	1	WSP

3. Interface Explanations

The external and internal interface/exchange elements utilized in the WSP ACCESS message switch environment are listed in the table below.

Ref.	Interface/Exchange	Explanation	Network
1	LCJA DOS Terminals (will be eliminated)	Law enforcement agencies DOS terminal direct-connect user interface.	Eliminated
2	WebMSS User Interface	Local criminal justice agency (LCJA) user Web interface to message switch.	IGN
3	ACCESS Journal	System journal for system transaction logging	WSP
4	DOC	Department of Corrections for felony offender information.	SGN
5	DOL	Department of Licensing for driver and vehicle information.	SGN
6	W2	Washington Crime Information Center for hot file information and the WASIS for Computerized Criminal History (CCH) and sex offender information.	WSP
7	NCIC/III	The FBI's NCIC files for the national hot files information and III system for interstate criminal history information.	CJIS
8	Nlets	Nlets, providing direct access to other state CCH, driver and vehicle information systems, and interstate messaging.	Nlets

D. Transactions, Records, and Metrics

This subsection examines transactions and records processed in the current ACCESS message switch environment, including the performance, administrative, and database metrics for the current system.

1. Transactions, Messages, and Reports

LCJA personnel and other stakeholders utilize ACCESS via transactions and message forms through their interfaces. APPENDIX A provides a more specific listing of the ACCESS message formats utilized in the current environment. APPENDIX A provides an informative view of the current ACCESS functional level, but does not necessarily represent specific ACCESS requirements. Vendors are encouraged to present alternate solutions to the current functionality.

ACCESS must be available 99.999 percent of the time, including unplanned downtime, hardware/software error, power failure, and failures from other causes. The WSP data center is currently supported by an adequate UPS system.

2. Message Keys

Transactions and messages available in the current ACCESS operating environment are initiated through the use of message keys that correspond to and are in compliance with the NCIC, Nlets, or ACCESS specifications. APPENDIX B provides a listing of the message keys utilized in the current ACCESS operating environment.

3. System Metrics

This subsection examines the performance, database, and administrative metrics that characterize the current ACCESS processing environment.

Performance and Data

There is limited data available regarding the volume of transactions processed by ACCESS. The table below highlights the three primary performance and data metrics for the current ACCESS environment. WSP anticipates a growth of 5 percent per year for these message rates.

Ref.	Transactions	Metric
1	Peak system input message processing.	120,000 messages per hour.
2	ACCESS transactions processed from Washington through Nlets.	1.7 million messages per month.
3	ACCESS journal transaction log (6 years of data).	3.4 GB.

Administrative

The table below details the system administrative metrics related to the operation of the ACCESS environment.

Ref.	Element	Quantity
1	Number of terminal agencies.	604
2	Number of nonterminal agencies.	800
3	Number of possible users.	17,000

III. Target ACCESS Environment and Drivers

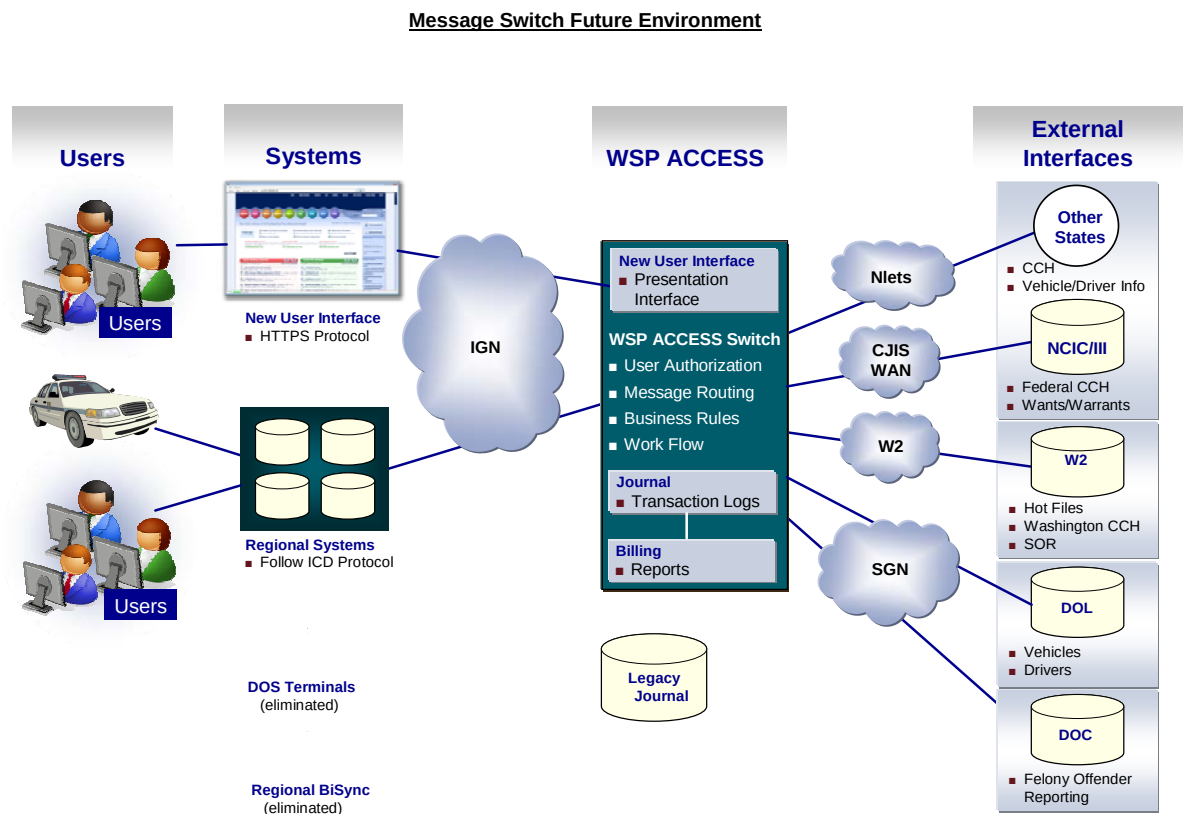
III. Target ACCESS Environment and Drivers

This section outlines the business and technical change drivers at work in order to provide an understanding of the goal of the future ACCESS environment. This section also presents an overview of the target ACCESS environment, including a review of the model elements and issues that will be addressed as a result of this migration.

The overarching goal of the ACCESS Message Switch Replacement Project is to implement a solution that provides critical statewide criminal justice information and a central technology environment with minimal impact on and maximum service to the justice community. In addition, WSP must have control over standard administrative functions, such as adding message keys, collecting data, and others, without vendor intervention.

A. Future WSP ACCESS Model

The diagram below represents a high-level vision for the future ACCESS message switch processing environment.



The significant changes in this target WSP ACCESS environment relative to the current environment include:

- Eliminating the connection for the DOS terminals.

- Eliminating the regional BiSync connections.
- Replacing the current WebMSS interface with a new Web-based user interface.

In their technical responses, vendors should include recommendations in the following areas for the future ACCESS environment:

- Whether to move the user interface application from a separate server to within the ACCESS switch application.
- Whether to move the journal database and logging functions inside the ACCESS switch application.

B. Change Drivers

This subsection presents an overview of the change drivers that have pushed WSP to reconsider its current business and technical model and to look at alternatives for providing ACCESS services.

1. Business Drivers

As part of the discovery process, high-level business goals were identified that support the pursuit of the future ACCESS processing model. These needs, or change drivers, related to the business-rule side of this system operation are listed in the table below.

Ref.	Business Goal	Description
1	Supportability	Procure a solution that can be effectively maintained and administered by WSP staff, such as through adding or modifying message keys.
2	Cost-Effectiveness	Procure a more modular solution with current technologies that can be managed, updated, and replaced without requiring wholesale replacement of the entire system.
3	Risk Management	Manage the overall risks and impact on LCJAs of implementing and operating the new ACCESS environment while improving system functionality.
4	High Availability	Provide higher levels of service with the ability to meet new evolving requirements and user operational needs.
5	Disaster Recovery/ Business Continuity	Develop and manage a program that provides a constant state of business continuity readiness.
6	User Training and Certification	WSP is interested in implementing a browser-based application for NCIC operator certification and recertification. The solution should provide the ability to manage certified users and should provide randomized testing capabilities, multiple levels of access (e.g., user, terminal agency coordinator [TAC], administrator), and certification expiration reports. The system needs to support the current 20,000-plus users and allow for future growth.

The goals listed above were central to crafting the management requirements of the future ACCESS model.

2. Technical Drivers

The following technical goals, or change drivers, were identified by WSP and support the pursuit of a future ACCESS processing model:

Ref.	Technical Goal	Description
1	Enhanced Data Exchanges	Allow for expanded use of emerging technologies and data exchanges by leveraging National Information Exchange Model (NIEM) standards.
2	Standards-Based System	Adhere to state and national standards for data exchange, security, and interfaces.
3	Improved Support and Costs	Leverage best-of-breed components and commercial off-the-shelf (COTS) solutions to improve system supportability, by both WSP and the vendor, and decrease total cost of ownership.
4	Open Architecture	Provide open systems-based architecture that is more reliable, flexible, and maintainable.
5	Enhanced Security	Retain the necessary level of system security to protect users and information from unauthorized access.
6	Enhanced Services	Provide client agencies with complete NCIC 2000 text- and image-based services as well as improved functionality.

The goals listed above were central to crafting the functional and technical requirements of the future ACCESS model.

C. Interfaces

The table below recaps the external and internal interface/exchange elements utilized and required in the future WSP ACCESS message switch environment. These interfaces are described in the MSS Interface document by Level II, now posted on the ACCESS RFP Reference Web site: <http://www.mtgmc.com/projects/WSP-ACCESS-REISSUE/>. DOC, DOL, and W2 are the “database” interface rather than the “regional/CAD” interface.

Ref.	Interface/Exchange Type	External	Internal
1	<i>New User Interface</i> – LCJA Web interface to the message switch.		✓
2	<i>Regional Systems</i> – Agency interface to transmit messages to ACCESS. (These interfaces cannot be changed with the implementation of the new system).	✓	

Ref.	Interface/Exchange Type	External	Internal
3	<i>ACCESS Journal</i> -- System journal. (The existing journal system will be replaced as part of this procurement, and no data conversion will be done.)		✓
4	<i>DOC</i> – Washington State Department of Corrections.	✓	
5	<i>DOL</i> – Washington State Department of Licensing.	✓	
6	<i>W2</i> – WACIC/WASIS.		✓
7	<i>NCIC/III</i> – The FBI's NCIC files and III system.	✓	
8	<i>Nlets</i> – Access to other state CCH, driver, and vehicle information systems.	✓	

Legend:

- *Interface/Exchange Type* – Interface agencies and systems.
- *External* – System/agency interfaces external to the WSP environment.
- *Internal* – System/agency interfaces internal to the WSP environment.

The table above summarizes the various interfaces and exchange points that must be included in the proposed future ACCESS environment. Other key elements of the target message switch model are discussed in the next subsection.

NOTE: Subsection I.B contains information about a secure Web site where copies of all interface specification documentation, standards, and policies can be found and will be made available to vendors upon signing a nondisclosure agreement.

D. Key Issues

This subsection highlights the key high-level issues to be addressed by the future ACCESS environment. Below is an outline of these high-level issues to be resolved with a transition to the future ACCESS solution.

- *Enhanced Data Exchanges* – Coupled with the enhanced applications and communication, an environment that enables the exchange of data between systems and the application in a robust and flexible manner is sought.
- *System Architecture* – The current message switch environment is a traditional, legacy, proprietary hardware/software system, which creates a high degree of dependency on the vendor for support, as well as increased cost and risk.
- *Proprietary Solutions* – The current message switch environment is a proprietary system at a time when open architecture and standards-based data and communication are the norm.
- *Supportability* – The current message switch environment will begin to experience diminishing support after the July 2009 time period.
- *System Administration* – WSP administrative staff must have the ability to make changes such as modifications to message key routing or the presentation level of

the user interface without involving the vendor. Also, staff need the ability to better manage user training and certification.

- *Business Continuity* – The current message switch system relies on a single physical location. If this site were affected by a disaster, the entire system could be disabled for days or even weeks.
- *Local Agency Impact* – The local law enforcement community cannot afford the cost in time and money to move to a new ACCESS solution that requires a number of local changes. Regional system interfaces cannot be changed with the implementation of the new system.
- *Visibility* – ACCESS affects many users and agencies throughout the Washington law enforcement and criminal justice communities, making it important that the vendor has the capacity and experience to instill confidence in these stakeholders.
- *Flexibility of Reporting* – WSP requires a more robust message switch transaction log reporting capability. This includes ease of data access, canned report utilization, and custom report specification across common areas of statistics and billing, among others.

The list above highlights some of the primary issues that WSP has identified as key to the desire to begin the migration to the future ACCESS processing model.

E. Implementation Strategy

This subsection highlights a series of plans that are recommended for successful implementation of the future ACCESS environment and that will serve to minimize risks. WSP requires the bidding vendors to provide responses to each concern outlined in the Implementation Approach and Data/Interface Approach subsections below.

1. Implementation Approach

The following table presents the general elements of implementation that WSP requires the vendors to respond to and address in their proposals:

Ref.	Approach	Elements
1	Data Conversion Approach	WSP does not envision any conversion of data from the existing message switch to the new system with the possible exception of the originating agency identifier (ORI) table. In their cost proposals, vendors should include conversion costs only for the ORI table.

Ref.	Approach	Elements
2	Migration Approach	An approach that allows for parallel operation of the newly installed components with the current operational environment. The migration must occur with minimal impact on the user community. Specific elements to be considered in this migration approach include: • <i>Regional Systems</i> – These interfaces cannot be changed or affected by the implementation of the new system. • <i>Switch Hardware</i> – When to install ACCESS hardware. • <i>Message Routing/Applications</i> – Orderly implementation of routing tables and applications. • <i>User Interface</i> – Replacement of the WebMSS user interface to a new user environment and migration of the regional system interfaces to the new environment. Vendors should describe the options available within their systems. During planning, WSP will work with the vendor to detail actual transition, dependent upon the capabilities of the systems. An on-off scenario with one system taking on the new load right away is as feasible as a connection-by-connection migration.
3	Testing Plan Approach	A comprehensive and orderly process or approach for testing each aspect of the new environment (hardware, messaging, applications, etc.) in a preproduction setting, including: • Factory acceptance testing. • Site installation testing. • Regression testing. • User acceptance testing.
4	Training Approach	An approach for the training of administrators and users of the system, including: • Training guides (electronic and hard copy). • User manuals (electronic and hard copy). • Online help files.
5	Fail-Back Approach	An approach addressing the rapid and orderly return to the prior (current) version or environment if the transition effort for any element of the new environment begins to fail in production, including consideration of: • System restoration and rollback. • Data restoration and rollback.

Ref.	Approach	Elements
6	Hot Files Approach	Hot files exist and reside on the WACIC system. The ACCESS message switch serves as a pass-through between the users and WACIC, routing hot file entries and file maintenance transactions from the user to WACIC with responses back to the user.

The elements outlined above are the high-level activities that will be necessary for successful implementation of the future ACCESS environment.

2. User Interface Approach

Considerations for the user input devices element of the overall ACCESS implementation include:

- *Direct-Connect and WebMSS Interfaces* – Users of the direct-connect and WebMSS interfaces will need to be supported and migrated to the new environment and the new ACCESS user interface, which will replace the WebMSS product.
- *Interface Support* – A strategy will need to be developed for supporting and debugging the current regional system interfaces during implementation of the new switch environment.

The above summarizes the key elements and considerations for the implementation and migration to a new ACCESS environment.

3. Business Continuity Approach

Current business continuity/return-to-service capabilities for ACCESS are limited to off-site replication of data. In the event of disruptions of service at WSP's primary data center, WSP is interested in options for a quick return to service during these hardware-related disruptions.

As such, WSP is interested in a business continuity option(s) minimally predicated on the following elements:

- A solution that is designed as a clustered/load-balanced system during normal ACCESS production. The design of the architecture should address the following parameters:
 - » Production ACCESS operates over all elements of the architecture during normal operation.
 - » Each element of the clustered environment has the capacity to carry 100 percent of the production operating system.

- » Each element of the clustered environment normally carries a proportional amount of the production load in normal operation (e.g., 50 percent or less for two servers, 33 percent or less for three).
- A solution that provides automated or directed return to service in the event of a disruption-of-service scenario.
- A solution that supports the installation of a fully functional remote “hot site” in the future.

WSP does **not** desire to purchase off-site disaster recovery (DR) as a part of this procurement. However, the proposal must provide on-site “hot failover” functionality in the event of a failure in a major component of the system. The proposed system must also be delivered with the built-in ability to synchronize with an off-site DR system that may be deployed at a future date, at no additional development cost at that time. Costs for software licenses and equipment for the off-site DR system will be determined at that time.

All business continuity options should include a consideration of the synchronization of files/data in the vendor proposals.

F. Hardware Maintenance and Support Strategy

WSP intends to require the successful vendor to be responsible for primary support of **all** ACCESS hardware and software provided. The table below illustrates WSP’s expectations.

Area of Support	Vendor Responsibility	WSP Responsibility
Facilities and Environmental Support	• None.	• Provision.
24x7 Hardware, System Software, and Application Support	• Ongoing support. • Problem diagnosis. • Solution provision.	• System monitoring. • Error detection.
On-Site Defective Hardware Component Replacement or Upgrades	• Installation.	• Assistance.
Antivirus, Anti-Malware/Spyware, Cisco Security Agent	• None.	• Installation. • Monitoring. • Detection. • Diagnosis. • Solution.
Vendor Application Patches	• Installation.	• Assistance.
Microsoft and Other Party System Software Upgrades and Patches – Option 1	• Installation. • WSP notification process.	• Approval. • Observation.

Area of Support	Vendor Responsibility	WSP Responsibility
Microsoft and Other Party System Software Upgrades and Patches – Option 2	Approval of patches for applications.	Installation.
Backup and Recovery	Provision.	Observation.
Performance Monitoring	Provision.	Provision.

IV. Standards, Compliance, and Staffing

IV. Standards, Compliance, and Staffing

This section gives insight on the national and state standards and policies applicable to the future ACCESS environment and compliance, as well as a brief look at the WSP staffing levels involved with the current environment from a training perspective.

A. Standards and Policies

This subsection provides an overview of the national and state standards and policies applicable to the future ACCESS environment, as well as an assessment of the compliance status of the current environment.

1. Applicable Standards

The table below lists the standards that are specifically applicable to the implementation and operation of a state message switch in the criminal justice environment.

Ref.	Standard/Policy	Objectives
1	FBI NCIC 2000	• Inquiry response time. • III response time. • Record entry. • Equipment and technology compatibility. • System and service availability.
2	FBI CJIS Security Policy	Minimum security requirements for CJIS data in the following areas: • Access. • Transmission. • Processing. • Storage.
3	Washington State IT Security Standards	Enables a shared, trusted environment for interaction among agencies as well as agency-to-customer transactions.
4	Washington State Standards for Internet Markup Language	Enables: • Web consistency and ease-of-use guidelines. • Nonproprietary tools for universal access.
5	NIEM, Version 2.0, or most current version	A framework for: • Identification of information-sharing requirements. • Development of standards and information exchange packages. • Technical tools to support reuse of exchanged information.

Ref.	Standard/Policy	Objectives
		• Training, assistance, and support for enterprise-wide information exchange. • Criminal justice information exchange.
6	Washington State Department of Information Services (DIS) Network Standards	Establishes: • The SGN for application interaction with state agency users. • The IGN for application interaction with local agencies within the state.
7	Washington State DIS Identity Management User Authentication Standards	• Establishes the use of the state's Enterprise Active Directory (EAD), SecureAccess Washington, and Transact Washington. • Directs all executive branch agencies and agencies headed by elected officials to set plans for migrating agency Active Directory files to the EAD. • Establishes SecureAccess Washington and Transact Washington as the authentication mechanism for users external to state government. • Enables SecureAccess Washington to extend functionality to allow federated identity management for other government entities, including legislative, judicial, higher education, local, and federal agencies.
8	Washington State Information Services Board (ISB) Enterprise Architecture Standards and Guidelines	Enables: • Agency-to-agency data sharing. • System interfaces. • Data integration.

The standards and policies detailed above are those that are directly applicable to the operation of the state message switch system in Washington State.

B. Standards Compliance

The table below outlines the implementation status and goals for the future ACCESS operating environment in the area of standards and policies.

Ref.	Standard/Policy	Implementation	
		Current	Future
1	FBI NCIC 2000	✓	✓
2	FBI CJIS Security Policy	Partial	✓

Ref.	Standard/Policy	Implementation	
		Current	Future
3	Washington State IT Security Standards	✓	✓
4	Washington State Standards for Internet Markup Language	✓	✓
5	NIEM 2.0	X	✓
6	Washington State DIS Network Standards	✓	✓
7	Washington State DIS Identity Management User Authentication Standards	Partial	✓
8	Washington State ISB Enterprise Architecture Standards and Guidelines	Partial	✓

Legend

✓ = Operational compliance.

Partial = Substantially in compliance.

X = Not implemented.

Explanations for less-than-full compliance with the standards or policies are provided below.

- *CJIS Security Policy* – ACCESS is not fully compliant regarding password management and advanced authentication.
- *NIEM 2.0* – Due to the legacy nature of the ACCESS platform, the current environment is unable to implement NIEM.
- *Washington State DIS Identity Management User Authentication Standards* – SecureAccess Washington and Transact Washington are not being used due to the legacy nature of the ACCESS platform.

NOTE: NIEM 2.0 is an information exchange model, not a required standard. WSP will require the ability to implement the standards above in the future ACCESS message switch.

The following are the specific citations for each standard or policy noted above:

- FBI NCIC 2000 Operating Manual, Section 5, December 1999.
- FBI Criminal Justice Information Services Security Policy (V4.4), June 2007.
- Washington State IT Security Standards, Policy 401-S3, January 10, 2008, <http://isb.wa.gov/policies/security.aspx>.
- Washington State Standards for Internet Markup Language, Policy 801-S2, August 12, 2005, <http://isb.wa.gov/policies/references.aspx>.
- NIEM (V2.0), July 31, 2007.

- Washington State DIS Network Standards, Version 4.0, September 14, 2006, http://dis.wa.gov/enterprise/enterprisearch/Network_standards.doc.
- Washington State DIS Identity Management User Authentication Standards, Version 2.0, July 10, 2008, http://isb.wa.gov/policies/portfolio/ea/User_Authentication_Standards_v2.0_ISB.pdf.

In addition, vendors need to *be aware of the fact (and understand) that* the enterprise architecture and user authentication to the new solution may need to be able to accommodate the following standards and developing approaches related to system architecture, Web access gateway, and authentication in the state of Washington. WSP is also interested in understanding the costs for compliance with only these State of Washington standards and policies:

- Washington State ISB Enterprise Architecture Standards and Guidelines: <http://isb.wa.gov/policies/eaprogram.aspx>.
- Washington State Enterprise Architecture Program Network Standards: http://dis.wa.gov/enterprise/enterprisearch/Network_standards.doc.
- Washington State security and authentication (for users external to the state government):
 - » Security policy – <http://isb.wa.gov/policies/portfolio/400P.doc>.
 - » Security standards – <http://isb.wa.gov/policies/portfolio/401S.doc>.
- Washington State DIS SecureAccess Washington: http://techmall.dis.wa.gov/services/secure_access_wa.aspx.

NOTE: User authentication through a Web path (e.g., <https://>) must accommodate the following approaches and systems:

- SecureAccess Washington (SAW).
- ACCESS system solution.
- SAW and DIS EAD.

Further, the following security and user authentication issues must be accommodated in this implementation:

- CJIS Security Policy compliance.
- Account for and identity maintenance by user agency (identity management must be self-service and cannot be based on call to WSP).
- Timeliness of the administration of accounts.

NOTE: Subsection I.B contains information about a secure Web site where copies of all of these standards and policies can be found.

It should also be noted that the standards and policies above are current as of this publication. It is anticipated that these documents will continue to be updated to reflect emerging requirements, and this RFP will be modified as necessary to remain current.

1. Active Directory

The Washington State DIS Identity Management User Authentication Standards do not require that this application use the EAD but do require that WSP set up migration plans. Applications are required to employ Active Directory as the authentication mechanism for users. The future ACCESS message switch should allow for this migration.

2. Advanced Authentication

WSP's goal is to be fully compliant with all applicable systems security requirements at the state and federal levels. However, the exact impacts of these requirements as they apply to WSP are not yet clear. These requirements will be addressed during the discovery phase. WSP does **not** desire to purchase advanced authentication as a part of this procurement. Offerors should not include costs attributed to this functionality when submitting their cost proposals. Based on the outcome of the discovery phase, WSP may elect to revisit advanced authentication pricing.

C. Staffing

The table below provides a high-level listing of the administrative and IT staffing levels involved in the current ACCESS message switch environment. Included in this listing are the WSP staffing levels for each category.

Ref.	Staff Description	Quantity
1	Business Operations	6
2	Systems Administration	3
3	Technology Support	6
4	Database Administrators (DBAs)	3
5	Customer Services Support	17

The staffing levels indicated above provide guidance as to the requisite training needs for the administrative and support members responsible for the ACCESS operations. It is anticipated that staff members will require training on the replacement ACCESS.

V. Proposal Content and Organization

V. Proposal Content and Organization

This section outlines the specific proposal content and format sought by WSP for the ACCESS Message Switch Replacement Project.

A. Instructions to Vendors

WSP requires vendor responses in three distinct binders:

- Management Response Binder
- Technical Response Binder
- Cost Response Binder

Instructions for these three response sections are outlined below.

All proposals should be printed on standard 8½ × 11 paper (larger paper is permissible for charts, spreadsheets, etc.) and placed in a three-ring binder with tabs delineating each section of the response. Elaborate submissions in the form of brochures or other presentations beyond what is necessary to present a complete and effective proposal are not desired. The response should be complete and comprehensive with a corresponding emphasis on being concise and clear and following all instructions contained in the Management, Technical, and Cost Response sections.

B. Management Response Binder

Vendors must follow the outline below for the Management Response section of the overall proposal. A more detailed explanation of the information sought by WSP in each subsection is also provided. For the purposes of this response, each vendor is asked to provide an approach to the various planning areas listed below.

- Transmittal Letter
- Table of Contents
- Executive Summary
- Prior Experience
- Vendor References
- Vendor Strength and Stability
- Exceptions to Requirements of the RFP
- Contract Requirements
- Escrow Agreement Approach
- Statements of Work (SOWs) Required
- Conflict of Interest

- Project Management Approach
- Risk Management Approach
- Proposed Project Staff
- Data Conversion Approach
- Business Continuity Approach
- Implementation Approach
- Migration Approach
- Fail-Back Approach
- Test Plan Approach
- Training Approach
- System Documentation Approach
- Maintenance and Support Approach
- Optional Components Approach
- Project Oversight Acknowledgement
- SOW Acknowledgement
- Proposal Checklist

1. Transmittal Letter

Each proposal must be accompanied by a transmittal letter that provides the following information:

- Identify the submitting organization, including:
 - » Full name, federal tax identification number, address, and telephone number.
 - » Date established.
 - » Background of firm.
 - » Ownership (public company, partnership, subsidiary, etc.).
 - » If incorporated, state of incorporation.
 - » Number of full-time employees on January 1 for the past 3 years or for the duration that the vendor's firm has been in business, whichever is lower.
- Identify the name, title, telephone and fax numbers, and e-mail address of the person authorized to contractually obligate the organization.
- Identify the name, title, telephone and fax numbers, and e-mail address of the person authorized to negotiate the contract on behalf of the organization.
- Identify the name, title, telephone and fax numbers, and e-mail address of the person to be contacted for clarification.
- Acknowledge receipt of any and all amendments to this RFP.

- Provide a statement indicating whether proprietary information has been included in the proposal and ensure that each occurrence has been clearly marked at the top or bottom of each applicable page.
- Provide a statement that the proposed solution will meet the specifications set forth in this RFP and/or a list of exceptions to the specifications in the RFP. (It is important to note that WSP reserves the right to reject any proposal containing such exceptions or to require modifications before acceptance.) Any errata or exceptions must be stated on a separate page labeled "Errata and/or Exceptions," with references to the corresponding terms or provisions of this solicitation.
- Provide a statement that the proposal shall remain valid for a minimum period of 180 days after the proposal opening date.

2. Table of Contents

A table of contents should be included as a part of the overall proposal with cross-references between each RFP requirement and the specific page of the response to the requirement.

3. Executive Summary

The executive summary shall condense and highlight the contents of the Management Response and Technical Response sections in such a way as to provide WSP management and the evaluation groups with a broad understanding of the entire proposal.

4. Prior Experience

Vendors must clearly define their experience with projects providing message switch solutions for comparable enterprises. WSP is concerned about the overall company strength and viability to support WSP with this solution. WSP views this procurement as a long-term technology investment and seeks to ensure that vendors can accomplish the ACCESS Message Switch Replacement Project.

Briefly describe the vendor's prior provision of message switch solutions. The vendor must have successfully completed, and provide examples of, at least two message switch solution implementations of comparable complexity to that needed by WSP. These examples and references must include demonstrable experience with:

- Interfacing with federal law enforcement systems. The referenced message switch solutions implemented must have included multiple integration points to federal-level public safety systems, including:
 - » Nlets.
 - » NCIC.

- Interfacing with other applications (e.g., WASIS, WACIC, DOL) in the client environment not provided by the proposing vendor. The vendor must list the application name and provider of the system, including:
 - » Regional justice systems or local law enforcement systems.
 - » Other law enforcement repositories (e.g., CCH, hot files, and driver/vehicle records).

In addition, vendors must indicate prime contractor and subcontractor roles (if any) in the experience provided.

5. Vendor References

Vendors must provide **three** references by using the References Form (APPENDIX E).

Please be advised that the WSP Evaluation Committee will call the vendor references to confirm information. Vendors must have satisfactorily completed the qualifying project, as verified by the references, in order to receive evaluation points for this requirement. WSP also reserves the right to check other references beyond the three provided by the vendor in the proposal.

6. Vendor Strength and Stability

Vendors must complete the Vendor Strength and Stability Form (APPENDIX F). If the proposal involves multiple vendors, be sure to include relevant information for each vendor. Please provide a clear and concise response to each question.

7. Exceptions to Requirements of the RFP

Vendors must list and explain any exceptions they have with the requirements of the RFP. Responses need to be clear and concise.

8. Contract Requirements

The Washington sample contract, based on the Model Information Technology Contract Terms and Conditions adopted by the ISB, has been included as APPENDIX I.

To be responsive, vendors must indicate a willingness to enter into a contract substantially similar to WSP's proposed contract by signing the Certifications and Assurances, included as APPENDIX J. Any specific areas of dispute with the attached terms and conditions must be identified in the proposal and may, at the sole discretion of WSP, be grounds for disqualification from further consideration in the award of a contract.

Under no circumstances is a vendor to submit its own standard contract terms and conditions as a response to this solicitation. Instead, vendors must review and identify the language in APPENDIX I that they find problematic, state the issue(s), and propose the

language or contract modification they are requesting. All of a vendor's exceptions to the contract terms and conditions in APPENDIX I must be submitted within the proposal, attached to APPENDIX J, Certifications and Assurances. WSP expects the final contract signed by the Apparent Successful Vendor (ASV) to be substantially the same as the contract located in APPENDIX I.

The foregoing should not be interpreted to prohibit either party from proposing additional contract terms and conditions during negotiation of the final contract.

The ASV is expected to execute the contract within 30 business days of its receipt of the final contract. If the selected vendor fails to sign the contract within the allotted time frame, WSP may elect to cancel the award and instead award the contract to the next-ranked vendor or cancel or reissue this solicitation (subsection VIII.DD, Right to Cancel). A vendor's submission of a proposal to this solicitation constitutes acceptance of these contract requirements.

9. Escrow Agreement Approach

WSP intends to enter into an escrow agreement as soon as possible after the effective date of the contract, but no more than 60 days after the effective date. Vendors must discuss their approaches to entering into an escrow agreement with WSP.

10. SOWs Required

WSP intends to award a contract from which specific SOWs will be issued. The SOWs serve to specifically identify and schedule tasks included in the contractor's proposal; the vendor's cost proposal must include costs for any work proposed by the vendor from the discovery phase through implementation to post-implementation maintenance.

The first SOW will address a discovery phase in which the apparent successful vendor will examine a number of application, architectural, and security requirements associated with the project and make recommendations for the final future ACCESS environment. Subsequent SOWs will be developed to continue the project through implementation and final acceptance. There is no guarantee, however, that future SOWs will be issued beyond the initial discovery phase. Vendors should develop project plans, schedules, and costs to reflect this approach.

11. Conflict of Interest

The following are the conditions relevant to conflict of interest matters:

- By signing the proposal, vendors certify that no assistance in preparing the response was received from any current or former employee of WSP whose duties relate(d) to this RFP (unless such assistance was provided by the state employee in his/her

official public capacity) and that neither such employee nor any member of his/her immediate family has any financial interest in the outcome of this RFP.

- The proposal must state whether the vendor or any employee of the vendor is related by blood or marriage to a WSP employee or resides with a WSP employee. If there are such relationships, list the names and relationships of said parties. Include the position and responsibilities in the vendor's organization of such vendor employees. The proposal must state the employees' titles and start dates.

12. Project Management Approach

Vendors must provide their approach to project management related to this project that includes elements of project management, status reporting, quality assurance (QA), and scheduling. The specific guidelines for the vendor's project manager are included in subsection V.B.12, Proposed Project Staff. Specific elements to be addressed in the approach should include:

Project Management

Vendors must provide an overview of how they will successfully manage the complex aspects of budget, scope, and schedule management. In addition, vendors need to describe the project management methodology to be utilized, including a description of any supporting software. This discussion will include information about overall project management techniques, issue management approaches, weekly status reporting, meeting facilitation, and staffing. WSP prefers the use of Microsoft Project 2003 as the project scheduling software.

Status Reporting

Vendors should describe the process of providing project status updates to WSP. The vendor project manager will report to the WSP project manager weekly by e-mail and a minimum of once a month in person to update WSP on completed tasks, review the progress of uncompleted tasks, clarify requirements, and discuss other issues related to the ACCESS replacement project. The vendor project manager will report project status to the project Executive Steering Committee as necessary.

Quality Assurance

Vendors must describe the QA process to be utilized for the project tasks, schedule, deliverables, and testing in order to ensure that work related to the production of acceptable deliverables is on track and expectations are met or exceeded. The QA process is expected to be proactive so as to ensure not only that the schedule is met but also that product and service quality is maintained.

Project Schedule

Vendors must describe the process of developing the schedule, including the identification of all major phases, tasks, and subtasks. For each identified task or subtask, vendors should include the following information:

- Resource assignments (e.g., vendor staff, local agency staff).
- Milestones.
- Time frames.
 - » Assume 10 business days for WSP review on each iteration of a deliverable.
- Deliverables.

Phase Duration

WSP is interested in implementing this project as expeditiously as possible. WSP prefers a project schedule that is realistic and reflects the shortest reasonable time frame based on the offeror's experience with projects of similar size and complexity and its capacity to successfully deliver proposed outcomes. Vendors should develop their project schedules with the following assumptions:

- *Discovery Phase Duration* – Maximum of 2 months.
- *Final System Acceptance* – 12 months following discovery phase completion.

If your company cannot adhere to these timing preferences, please provide a schedule that reflects the most expeditious and reasonable time frame possible. For your final schedule, describe your delivery approach, your assumptions and needs, and any additional risks or work requirements that will be important for WSP to understand in working with you to ensure successful delivery.

13. Risk Management Approach

Vendors must provide their approach to risk management that minimally identifies all risks associated with implementing ACCESS, the methods proposed to mitigate each risk, the probability that each risk will occur (i.e., high, medium, low), and the impact each risk can have on the project (i.e., high, medium, low). Each environment option proposed (i.e., service-oriented versus traditional) has different risks associated with it, and these risks must be included in the risk management plan.

14. Proposed Project Staff

The proposed vendor project staff will include the account manager, project manager, training personnel, and all other key staff to be assigned to the ACCESS Message Switch Replacement Project. Vendors must provide an outline of all proposed individuals, including

their major areas of responsibility during the project and the percentage of time that each will be dedicated to the project.

Specific guidelines for the vendor's project manager include the following:

- Must be able to demonstrate a history of *successful* projects of similar size, nature, and complexity.
- Must have a bachelor's degree or equivalent work experience.
- Must be able to demonstrate a minimum of 5 years' project management experience.

Though not required, Project Management Professional (PMP) certification from the Project Management Institute, Inc. (PMI) would be a value-added qualification.

Resumes of all key proposed personnel are required and must include the following, at a minimum:

- Experience with the vendor.
- Experience with projects related to public safety, especially message switch solutions.
- Experience with projects similar in size, scope, and complexity to this project.
- System design and development experience.
- System implementation and support experience.
- System integration experience.

Vendors shall indicate any industry-acknowledged certifications (e.g., Capability Maturity Model Integration [CMMI], PMP, International Organization for Standardization [ISO]) that their organizations or key proposed personnel have attained or are actively pursuing.

The description of experience must include specific responsibilities of vendor personnel and the number of years of their experience.

Each project referenced in a resume should include the customer name, customer reference (including current telephone number), and time period of the project, as well as a very brief project description. Limit references to the last 5 years.

It is important to note that WSP reserves the right to approve or reject any changes to the vendor's project manager or other key personnel after the contract award. WSP also reserves the right to require key personnel changes, with reasonable notice to the vendor, following contract award if WSP determines that such changes are in the best interest of the project.

15. Data Conversion Approach

WSP does **not** envision any conversion of data from the existing message switch to the new system, with the **possible** exception of the ORI table.

16. Business Continuity Approach

Vendors must provide a brief overview of their proposed business continuity approaches in light of the business continuity considerations outlined in subsection III.E., A detailed response to the business continuity approach requirements outlined in subsection III.E should also be provided with the overall solution approach within the Technical Response section. Pricing for the proposed business continuity solution should be included in the Cost Response section as an optional component.

WSP does **not** desire to purchase off-site DR as a part of this procurement. However, the proposal must support on-site hot failover functionality in the event of a failure in a major component of the system. The proposed system must also be delivered with the built-in ability to synchronize with an off-site DR system that may be deployed at a future date, at no additional development cost at that time. Costs for software licenses and equipment for the off-site DR system will be determined at that time.

17. Implementation Approach

Vendors must provide their approaches to implementation of the proposed ACCESS solution, outlining the steps from the time of contract signing through complete acceptance and go-live of the future ACCESS infrastructure in the production environment. Specific attention should be given to the requirements outlined in subsection III.E.

18. Migration Approach

Vendors must provide their approaches to the migration of WSP from the current (legacy) message switch to the new message switch application. Specific attention should be given to the requirements outlined in subsection III.E., Vendors should include a discussion of possible migration alternatives, including prior experience with these alternatives. This plan will include considerations for the logistics of cutover of the following installations:

- WSP central site.
- User/interface sites.

This approach will need to address the seamless migration of regional system interfaces to the new environment. Finally, this plan must clearly include the logistics of coordinating the training of users of the new environment and the cutover to the new system.

19. Fail-Back Approach

Each vendor must provide its approach (based on prior experience) to the rapid and orderly return to the prior (current) version or environment if the transition effort for any element of the new environment (during cutover and for the period up to final acceptance) begins to fail in production, including plans for:

- System restoration and rollback.
- Data restoration and rollback.

Specific attention should also be given to the requirements outlined in subsection III.E.

20. Test Plan Approach

Vendors must provide their approaches to testing and test plans for the new ACCESS switch and its components. Elements of this approach must include:

- *Test Procedures* – Define the test procedures overall and for each of the specific test areas below, including verification of compliance with requirements.
- *Inspection* – Ensure the availability and quality of delivered equipment, certifications, documentation, and so forth.
- *Functional Testing* – Demonstrate each of the discrete functional capabilities of the system.
- *Operational Testing* – Demonstrate the full operability of all integrated components in an operational environment and to validate associated user and maintenance documentation.
- *Benchmark Testing* – Demonstrate that the system meets or exceeds performance requirements, including throughput and response time and identification accuracy.
- *Final Acceptance Testing* – Demonstrate that system components are completely readied for production implementation.
- *Test Reporting and Remediation* – After each phase of testing, compile and deliver a test report that includes the following:
 - » Completed and signed checklists documenting the successful performance of each inspection or test.
 - » A list of issues identified, corrected, and retested.

21. Training Approach

Vendors must provide their approaches to user and system administrator training programs, as well as periodic refreshers. This approach should consider elements of skills inventory and training plan needs outlined as follows:

Skills Inventory

An overview of the current WSP professional staff, by grouping, that will need to be addressed in the training approach, is presented in a table in subsection IV.C.

Training Plan

The proposed training approach must include:

- An overview of the training program, including objectives, roles and responsibilities, and facility requirements.
- Course descriptions and curriculum outlines for each training course.
- A plan for student testing and evaluation, including:
 - » Train-the-trainer program for the ACCESS operations staff and system administrators.
 - » Directed and detailed software and application training for developer and support staff.
 - » Directed and detailed hardware training for system operations staff. This training may be a matter of familiarization and clarification about where operating switches are, the meaning of messages, status light meanings, and so forth. Training on the Microsoft Windows operating system will not be necessary.
 - » Directed and detailed DBA training.
- A suggested training schedule and timeline.
- A discussion of training in relation to system installation and system go-live.

22. System Documentation Approach

Vendors must describe their overall approaches to providing WSP with a comprehensive set of user, system, and management documentation. WSP seeks both online, or otherwise electronic, documentation and hard copy documentation volumes. The online user documentation must describe the functionality and navigation of the ACCESS application. Operations descriptions must include a list and description of all error conditions, as well as the associated error message displayed and the action required of the operator for each error condition.

In addition, WSP expects that online documentation must be maintained and updated throughout the life of the system to reflect hardware/software version updates and modifications. WSP administrative personnel should also be able to edit documentation. A description of how this is to be accomplished should be included in the proposal.

Finally, each location with the ACCESS application must be provided with complete online user documentation that is resident on the workstation or can be accessed via WSP's internal networks.

23. Maintenance and Support Approach

Vendors must provide their approaches to maintenance and operations support that include a discussion of the following:

- Preventive maintenance.
- Remedial maintenance.
- Help desk support.
- On-site support.
- Updating and maintenance of the application product.

See subsection III.F for WSP's expectations regarding hardware maintenance and support.

Below is a support and maintenance matrix for any problems encountered by WSP with the new solution which provides the minimal parameters and timelines that need to be met.

ACCESS Support Requirements Matrix			
Ref.	Resource	Response	Availability
1	Remote/Dial-In Technical Support Response (Break/Fix)	Within 15 minutes of first call.	24/7
2	On-Site Technical Support Response	Within 4 hours of first call.	24/7
3	Help Desk/Administrative Assistance	Within 2 hours of first call.	Standard Business Day

The maintenance and operations support approach must address the following minimal elements:

- An overview of the maintenance and operations support program, including objectives, roles and responsibilities, and facility requirements.
- A suggested preventive maintenance schedule for each system component.
- A set of service level agreements outlining the requirements and plan for providing response and remediation (including on-site support) of problems for each system component.
- An approach to processing enhancement or change requests. Vendors should refer to Section 57, Updating and Maintaining the Application Product, of the sample contract in APPENDIX I.

- A proposal for on-site and/or remote ongoing maintenance support required by WSP, including:
 - » An explanation of how the vendor can support the application using remote access and on-site presence. The vendor should explain the appropriate means to accomplish the support and maintenance for application, system software (operating system, database, etc.), and hardware. The description should address such issues as what the controls are, what products are used, and what techniques are used. Further, it should describe any additional features of the approach.
 - » A problem escalation procedure, including the escalation metrics.
 - » Help desk plans and procedures, including support during non-business hours.
 - » A procedure for warranty repair/replacement of defective components.
 - » A comprehensive list of maintenance spares and consumable items.

24. Optional Components Approach

The Optional Components Approach subsection shall include a comprehensive written description of the vendor's project approach toward optional components (not requirements) and functionality. Vendors should identify any and all hardware, software, service, and ongoing operational requirements, beyond their baseline proposal, to fully implement optional functionalities. This should be accompanied by a description of how the functions will operate from user and administrator perspectives in relation to the baseline ACCESS solution proposed. In addition, all costs, including maintenance, associated with selecting and adding these optional components to the system with initial implementation or at a later date should be provided. WSP is particularly interested in understanding the following optional components:

- Ongoing user training and certification approach.
- Transfer of system licensing and code ownership to WSP.
- Business continuity approach.
- Compliance with State of Washington standards and policies.

Vendors should understand that procurement is a unique opportunity for WSP to further enhance its ACCESS operations. As such, WSP may be in a position to expand the scope of the procurement during contract negotiations to include some or all optional functionality if financially feasible.

NOTES:

- Vendors are required to provide responses to all optional components outlined above; the choice regarding whether to select an option and which option to select remains with WSP.
- Vendors should also indicate, for each of the optional components, what elements of the above components are already included in their proposed ACCESS solutions.

25. Project Oversight Acknowledgement

By submitting a proposal in response to this RFP, vendors agree to and acknowledge the approach wherein participation in the QA oversight process is required and acknowledge and ensure that any required QA participation is covered within the cost proposal.

26. SOW Acknowledgement

Vendors will provide a statement of agreement and acknowledgement that WSP intends to award a contract from which specific SOWs will be issued and that there is no guarantee that future SOWs will be issued beyond the initial discovery phase.

Each SOW will be developed collaboratively by WSP with the successful bidding vendor in preparation for contract signing. Each SOW will establish the work to be performed and deliverables to be produced with acceptance criteria for each deliverable, a timeline and period of performance, and a compensation and payment plan. Each SOW will be constructed based on the requirements of this RFP and the proposal. The order of precedence in any dispute on the ACCESS Message Switch Replacement Project will be as follows:

- Contract.
- SOW.
- RFP.
- Proposal.

NOTE: The successful vendor's proposal in response to the ACCESS RFP will be incorporated into the contract.

27. Proposal Checklist

Vendors must complete and attach the Proposal Checklist (APPENDIX G).

C. Technical Response Binder

Vendors must follow the outline below for the Technical Response section of the overall proposal. A more detailed explanation of the information sought by WSP in each subsection is also provided.

- Functional Specifications Response
- Technical Specifications Response
- Standards, Policies, and User Authentication Compliance Approach
- Overall Solution Approach
- Value-Added Services

1. Functional Specifications Response

This subsection of the Technical Response section shall provide a comprehensive and written description of the vendor's approach to all functional specifications. Inserting the functional specifications tables (APPENDIX C), vendors must first respond directly to each specification entry by placing an "X" in the applicable column in each row. Descriptions of each column heading are provided in the table below.

Immediately following the completed functional specifications tables, vendors are to provide detailed explanations for their responses to each requirement ID, according to the format outlined in the table below.

Requirement ID	Definition	Explanation
Current Capability or Configurable Item		
List <i>each requirement ID</i> , so marked, in the same order as in the specifications tables.	Specification will be met by the proposed future ACCESS solution that is installed, operational, and can be demonstrated to WSP. <i>The cost of specifications receiving this response must be included in the cost of the base package.</i>	For each requirement ID listed, vendors must provide a <i>detailed explanation</i> of how the specification is met at initial installation.
Custom Development		
List <i>each requirement ID</i> , so marked, in the same order as in the specifications tables.	Specification will be met by package software currently under development, in beta test, or not yet released. <i>The cost of specifications receiving this response must be included in the cost of the base package, and the specifications must be delivered with the baseline solution at installation.</i>	For each requirement ID listed, vendors must provide a <i>detailed explanation</i> of how the specification will be customized, implemented, and maintained. Vendors may also note whether the associated custom development will be provided as part of the base package without additional cost.

Requirement ID	Definition	Explanation
Future Release		
List <i>each requirement ID</i> , so marked, in the same order as in the specifications tables.	Specification will be met by a future release of the product, within 1 year of baseline solution installation. <i>The cost of specifications receiving this response must be included in the cost of the base package.</i>	For each requirement ID listed, vendors must provide a <i>detailed explanation</i> of when and how the specification will be met within 1 year of installation.
Not Available		
List <i>each requirement ID</i> , so marked, in the same order as in the specifications tables.	Specification cannot be provided either as part of the baseline solution or future enhancement.	For each requirement ID listed, vendors must provide a <i>detailed explanation</i> of why they chose not to provide the specification.

NOTES:

- A response is required for each requirement ID entry in APPENDICES C and D (place an “X” in the applicable column). Failure to respond to each entry will be grounds for elimination.
- Failure to provide a detailed explanation for each requirement ID will also be grounds for elimination.
- All costs associated with each response must be included in the Cost Forms: Cash Purchase Response (APPENDIX H).
- WSP seeks vendor solutions that meet all specifications with no or minimal customization required.

2. Technical Specifications Response

This subsection of the Technical Response section shall provide a comprehensive and written description of the vendor’s approach to all technical specifications. Inserting the technical specifications tables (APPENDIX D), vendors must first respond directly to each specification entry by placing an “X” in the applicable column in each row. Descriptions of each column heading are provided in the table below.

Immediately following the completed technical specifications tables, vendors are to provide detailed explanations for their responses to each requirement ID, according to the format outlined in the table below.

Requirement ID	Definition	Explanation
Current Capability or Configurable Item		
List each <i>requirement ID</i> , so marked, in the same order as in the specifications tables.	Specification will be met by the proposed future ACCESS solution that is installed, operational, and can be demonstrated to WSP. <i>The cost of specifications receiving this response must be included in the cost of the base package.</i>	For each requirement ID listed, vendors must provide a <i>detailed explanation</i> of how the specification is met at initial installation.
Custom Development		
List each <i>requirement ID</i> , so marked, in the same order as in the specifications tables.	Specification will be met by package software currently under development, in beta test, or not yet released. <i>The cost of specifications receiving this response must be included in the cost of the base package, and the specifications must be delivered with the baseline solution at installation.</i>	For each requirement ID listed, vendors must provide a <i>detailed explanation</i> of how the specification will be customized, implemented, and maintained. Vendors may also note whether the associated custom development will be provided as part of the base package without additional cost.
Future Release		
List each <i>requirement ID</i> , so marked, in the same order as in the specifications tables.	Specification will be met by a future release of the product, within 1 year of baseline solution installation. <i>The cost of specifications receiving this response must be included in the cost of the base package.</i>	For each requirement ID listed, vendors must provide a <i>detailed explanation</i> of when and how the specification will be met within 1 year of installation.
Not Available		
List each <i>requirement ID</i> , so marked, in the same order as in the specifications tables.	Specification cannot be provided either as part of the baseline solution or future enhancement.	For each requirement ID listed, vendors must provide a <i>detailed explanation</i> of why they chose not to provide the specification.

NOTES:

- A response is required for each requirement ID entry in APPENDICES C and D (place an "X" in the applicable column). Failure to respond to each entry will be grounds for elimination.
- Failure to provide a detailed explanation for each requirement ID will also be grounds for elimination.
- All costs associated with each response must be included in the Cost Forms: Cash Purchase Response (APPENDIX H).

- WSP seeks vendor solutions that meet all specifications with no or minimal customization required.

3. Standards, Policies, and User Authentication Compliance Approach

This subsection of the Technical Response section shall provide an explanation of how the vendor's solution will comply with the standards, policies (including Washington State policies), and user authentication requirements previously detailed in subsections IV.A and IV.B.

Using the table format below in their response, vendors should indicate (with an "X") both that they have reviewed the standard or policy and their solution's compliance status. Additionally, vendors are to provide a written explanation of their approach to each of the standards and policies enumerated below. Finally, vendors shall provide the cost for bringing their proposed solution into compliance with the State of Washington standards and policies as an *optional cost* on the cost forms in APPENDIX H.

Ref.	Standard/Policy	Reviewed	Currently Compliant	Capable of Compliance
1	FBI NCIC 2000.			
2	FBI CJIS Security Policy.			
3	Washington State IT Security Standards.			
4	Washington State Standards for Internet Markup Language.			
5	NIEM 2.0.			
6	Washington State DIS Network Standards.			
7	Washington State DIS Identity Management User Authentication Standards.			
8	Washington State ISB Enterprise Architecture Standards and Guidelines.			
9	Washington State Enterprise Architecture Program Network Standards.			
10	Washington State security and authentication (for users external to the state government): • Security policy. • Security standards.			
11	Washington State DIS SecureAccess Washington.			

Each vendor's approach and response must address each of the standards, policies, and security and user authentication issues enumerated in detail throughout subsections IV.A and IV.B.

4. Overall Solution Approach

The Overall Solution Approach subsection of the Technical Response section shall provide a comprehensive written description of the vendor's solution, project approach, and business continuity strategy. This should include a discussion of the vendor's understanding of the WSP vision, how the solution will specifically address this vision, and a definition of all services to be provided. Specific emphasis must be placed on:

- A description of the proposed solution and a discussion of how this solution addresses the goals and requirements of the target ACCESS environment.
- A description of the proposed business continuity solution and capability and a discussion of how this solution addresses the goals and requirements of the target ACCESS environment. The operational production availability of the proposed solution should be at least 99.999 percent on a 24/7 basis.
- A description of the standard techniques utilized to enable scalability, security, and integrity.
- How the vendor will accomplish the required interfaces.
- Recommendations regarding whether to move the user interface and system journal database and logging functions from a separate server to within the message switch.
- A description of the extent to which the proposed solution adheres to national standards.
- A description of how user authentication and password resets could be accomplished in an Active Directory scenario. If the vendor has a different user database or directory scenario as a normal part of its product, it should be described as well. In the Cost Response section, the active directory scenario should be shown as a separate alternative or optional cost.
- Identification of any known/anticipated implementation and operational risks in the near and long terms.

Any proposal that does not adhere to these requirements may be deemed nonresponsive and rejected on that basis.

Vendors may attach other materials that they feel may improve the quality of their responses. However, these materials should be included as items in a separate appendix.

5. Value-Added Services

Vendors are encouraged to provide descriptions of any additional value-added services that are not already referenced by specifications included within this RFP. Any value-added services may be included in the base package costs or presented as optional components when there are associated additional costs. This subsection of the Technical Response section shall provide a comprehensive and written description of the vendor's approach to all value-added services that may be provided.

WSP is particularly interested in the option of implementing a browser-based application for NCIC operator certification and recertification. The solution should provide the ability to manage certified users and provide randomized testing capabilities, multiple levels of access (e.g., user, TAC, administrator), and certification expiration reports. The system needs to support the current 20,000-plus users and allow for future growth.

Each proposed value-added service is to be listed with a detailed explanation. At the onset, the details should note whether the given value-added service is included in the base package costs. If not, the service is to be associated with additional costs and, as a result, is to be included as an optional component on the Cost Forms: Cash Purchase Response (APPENDIX H).

D. Cost Response Binder

WSP is interested in understanding all costs associated with the Management Response and Technical Response sections of proposals for the ACCESS Message Switch Replacement Project. WSP reserves the right to utilize the state's enterprise software licensing or hardware contracts for the procurement of the new ACCESS solution.

WSP requires a deliverables-based milestone payment plan, with the largest percentage (not less than 20 percent of the total value of the contract) of the disbursement being made upon final testing and acceptance. No single deliverable cost prior to the final deliverable should be greater than 10 percent of the total value of the contract. The final deliverable, which constitutes and will be part of final acceptance of the entire system, must be included and must be priced at least 20 percent of the total contract.

The available state funding is limited to \$1,500,000 for the initial investment in the following components:

- Application software.
- System software.
- System hardware.
- Implementation.

See Sections A, B, C, and D of Cost Forms: Cash Purchase Response (APPENDIX H). Offerors shall bid a fixed price for these components. Bids exceeding this limit will be rejected as nonresponsive.

Enterprise licenses listed in cost proposals must apply to all users of ACCESS. ACCESS users include agencies both in and out of the state of Washington, including:

- Local agencies (city and county).
- State agencies.
- Federal agencies.
- Regional consortia.

Vendors are required to submit a completed copy of Cost Forms: Cash Purchase Response (APPENDIX H) for their proposed solutions.

* * * * *

NOTES:

- The vendor's solution must be deliverable-based, and each deliverable must receive a final acceptance.
- All Cost Response sections delivered will be considered to include a not-to-exceed price for delivering all required services in order to ensure complete and successful implementation and ongoing operation of the proposed solution.
- Although WSP cannot guarantee that future SOWs will be issued beyond the initial discovery phase, vendors must include all implementation costs for the entire project from discovery through final acceptance to post-acceptance maintenance support.
- The vendor's solution proposal should also address the issues and costs of transfer of system licensing and code ownership to Washington State. In this case, the ACCESS application vendor will supply all source code in English.
- WSP should be provided with the option to procure only select elements of a total proposal at the costs quoted for those specific elements.
- The state of Washington belongs to the Western States Contracting Alliance (WSCA). If the vendor proposes hardware that is available via the WSCA contract, the WSCA contract price is less than the vendor price, and the vendor will support the hardware, then WSP will purchase the hardware through WSCA.

VI. Target ACCESS Environment Requirements

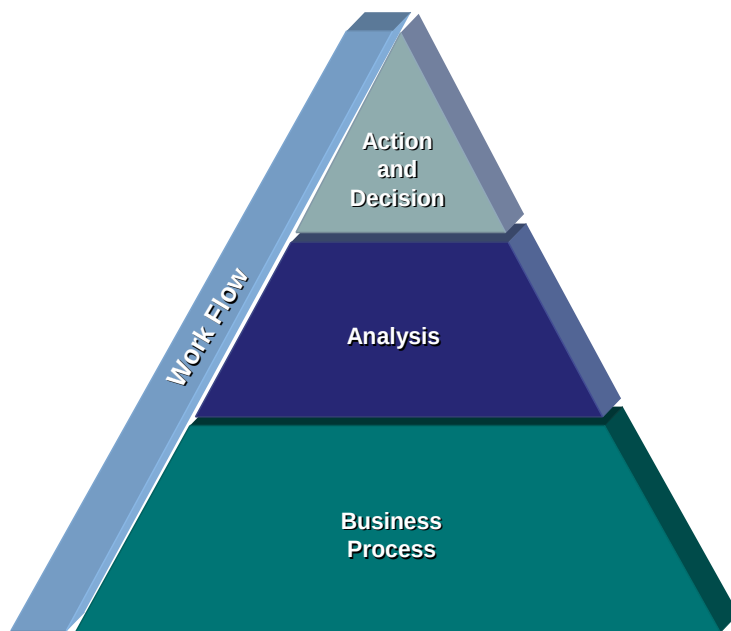
VI. Target ACCESS Environment Requirements

This section presents the framework for the functional and technical specifications (APPENDICES C and D). Methodologies for both functional and technical specifications are described below, followed by a brief explanation of the interrelationships of the two models.

A. Functional Specifications

Functional specifications for the future ACCESS solution are categorized into predictable elements comprising business process, analysis, action and decision, and work flow. The figure below depicts the structure of the functional specifications model.

Functional Specifications Pyramid



From the bottom moving upward, the layers of the functional specifications pyramid are explained below.

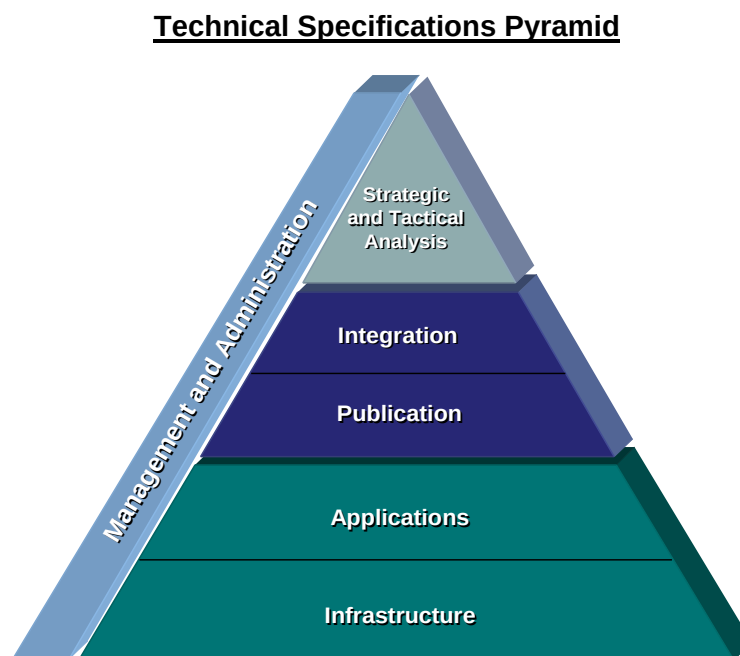
- *Business Process* – Denotes the core functional business components of the future ACCESS environment. This includes the modules necessary to meet business needs such as data query and messaging.
- *Analysis* – Outlines the components required of the future ACCESS solution relative to the use of the data captured for subsequent analytical decision making. Specifications in this layer include various types of online and hard copy reporting specifications.
- *Action and Decision* – Outlines the components required to allow users of the future ACCESS solution to render business decisions based on the analytical information presented. These decisions will have a downstream effect on other system users.

For example, an operator may wish to request confirmation of a warrant from the originating agency.

- *Work Flow* – Denotes specifications related to the routing, verification, and storage of information in the future ACCESS environment.

B. Technical Specifications

This subsection describes the structures associated with the technical specifications for the future ACCESS environment. Technical specifications for ACCESS solutions can be categorized into predictable elements – infrastructure, applications, publication, integration, strategic and tactical analysis, and management and administration. The figure below depicts the structure of the technical specifications model.



From the bottom up, the layers of the technical specifications pyramid are explained below.

- *Infrastructure* – Denotes the components that provide technology solutions delivering secure and reliable systems. This layer includes primarily hardware and networking components.
- *Applications* – Captures the components required of the software system solutions that ensure operability in the target environment. This layer includes software platform, storage, and data model specifications.
- *Publication* – Outlines the components required to ensure user access to information captured by the desired solution. These include indexing global search engines, report-writing services, data transformation services, and subscription and notification systems.

- *Integration* – Denotes the components related to the exchange of information between the future ACCESS and related public safety systems. Specifications here are relevant to the interfaces that move information between systems at a predetermined time (i.e., batch and/or real-time interfaces).
- *Strategic and Tactical Analysis* – Strategic and tactical analysis is achieved with a system that successfully addresses the functional layers above. These components provide complex relational information to criminal justice users from existing information systems. They include summary data sets that can be used to build comprehensive data warehouses designed to drive business decisions between organizations.
- *Management and Administration* – Represents the components associated with the management and administration of the systems. These include the components necessary to ensure successful operation in the desired technical environment, as well as applicable standards and vendor support.

C. Functional and Technical Model Relationships

The purpose of the differing functional and technical specifications models is relatively straightforward. It is conceivable that an individual business (functional) requirement can impact the technical architecture of the systems on multiple levels. As an example, from a message switch records management perspective, the functional specifications of entering or removing a wanted person record will have an impact on data structures, integration with the CCH applications, access restrictions, and security elements of the technical specifications model.

VII. Evaluation Information

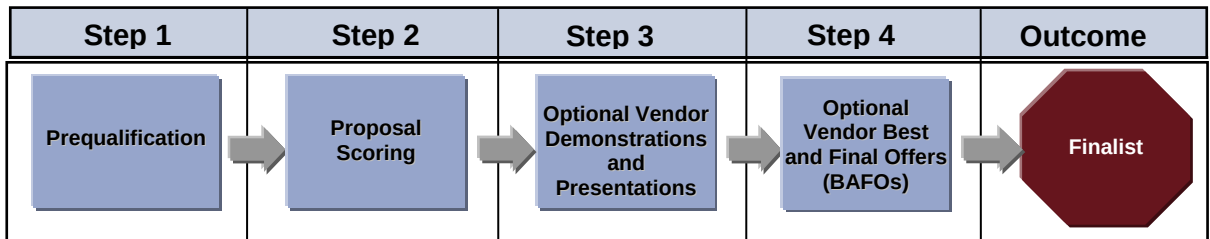
VII. Evaluation Information

This section outlines additional information regarding the evaluation process to be used for this RFP.

A. Proposal Evaluation

This subsection provides an overview of the process that will be used to evaluate proposals.

It is important to note that the basis for vendor selection is not proposal scoring alone but rather a larger sequence of events, as outlined below.



Step 1 – Prequalification

This step entails ensuring that vendors meet the baseline requirements of the bid process. If vendors fail to meet these or other defined minimum requirements, they may be subject to disqualification at the discretion of the WSP Evaluation Committee.

Step 2 – Proposal Scoring

This step includes a detailed review and numerical scoring of specific proposal content by the assigned subcommittees.

Step 3 – Optional Vendor Demonstrations and Presentations

Based on the results of Step 2, all vendor proposals with qualifying scores may be invited to participate in vendor demonstrations and presentations regarding their proposed solution. This step will involve allowing vendors to demonstrate and present their products based on a standard set of scripts that will be provided in advance and to clarify any proposal material that is unclear to the WSP Evaluation Committee.

The vendor demonstrations/presentations will be scored on a pass/fail basis for the purpose of determining qualification for proceeding to the next step.

Step 4 – Optional Vendor BAFOs

As a result of Step 3, specific vendors may be requested to submit BAFOs regarding their proposed solutions. The BAFO requests will be based on a set of questions or issues provided by the WSP Evaluation Committee in writing for the vendors to address. Then

vendors will be asked to provide structured responses to the questions or issues and, if appropriate, re-quote (as necessary) the cost response of their final proposals and submit them for consideration by the WSP Evaluation Committee. Upon receipt of the vendor response to the BAFO request, each proposal will be re-scored only in those areas of the BAFO request and on the basis of the BAFO response.

WSP reserves the right to make an award without further discussion of the proposal submitted (i.e., WSP may request a BAFO when it is in the interests of the state and solely at WSP's option). Therefore, the proposal should be submitted on the most favorable terms that the vendor intends to offer.

* * * * *

At the end of each step above, a report will be drafted in order to allow the WSP Evaluation Committee to review and, if deemed necessary, approve the results.

B. Evaluation Criteria

This subsection identifies the proposal evaluation criteria that will be used in selecting the finalist vendor. Vendor submissions will be evaluated based on a variety of quantitative and qualitative criteria, and the award will be made on a best-value basis according to the following criteria and weights:

Vendor Response	Scoring Category	Weight
Cost	Costs.	30%
Management	- Vendor Experience and References. - Customer Support/Warranty and Maintenance. - Training, Documentation, and System Administration.	30%
Technical	- Satisfaction of Functional and Technical Requirements. - Approach to Management Response.	<u>40%</u>
	Total	100%

The column headings in the table above are defined as follows:

- *Vendor Response* – The vendor response section for each scoring category.
- *Scoring Category* – The defined and specific areas to be addressed by the vendor responses.
- *Weight* – The relative weight for each scoring category.

NOTE: WSP seeks those solutions that minimize or fully eliminate the use of vendor proprietary architectural and data standards. In addition, WSP seeks vendor solutions that

require no or minimal customization and are compatible with the external application processing environment and thus will cause minimal or no impact on end users.

VIII. Administrative Rules

VIII. Administrative Rules

This section of the RFP provides a detailed listing of all of the applicable State of Washington contractual terms and conditions.

A. Acquisition Authority

Chapter 43.105 of the Revised Code of Washington (RCW) as amended establishes the Washington State ISB. While the ISB does not purchase for agencies, it regulates the manner in which state agencies may acquire information technology equipment, software, and services. WSP issues this Request for Proposal (RFP) acting under the delegated authority of the ISB.

Because the Contract resulting from this RFP will be for the design, development, and implementation of a major information technology system that has significant statewide impact and is subject to ISB approval, the Office of Financial Management (OFM) has authority over the Contract resulting from this RFP. Such major system contracts are required to be filed with OFM. Work shall not commence and payment shall not be made pursuant to such Contracts until a minimum of 10 working days after the date of filing, and, if required, until reviewed or approved by OFM. In the event OFM fails to approve the Contract, the Contract shall be null and void.

B. Acceptable Alternative Defined

Vendors may propose an alternative strategy or approach for meeting the objectives of the procurement. The AGENCY, at its sole discretion, will determine if the proposed alternative is consistent with the expected goals, objectives, and outcomes for this procurement and will either accept or reject the proposed approach.

C. Multiple Responses

Vendors may submit multiple responses if they feel alternate offerings will better meet the needs described in this RFP. Any alternative response, other than the alternative hosting responses specifically described, must be a fully complete and separate submission complying with the instructions in this RFP.

D. Vendor Must Appoint Representative

Each Vendor must appoint an individual to officially represent the Vendor for this procurement. Include the following information in the transmittal letter for the Vendor response:

- Name of Vendor Representative.
- Title.
- Name of Company.
- Address.

- Telephone Number.
- E-mail.
- Company Web Site.
- Fax Number.

E. Questions and Answers

Specific questions concerning the RFP should be submitted to the RFP Coordinator in writing (e-mail and fax acceptable) no later than the dates and times listed in the Evaluation Schedule (see Section I.C) so AGENCY representatives may prepare responses. In accordance with the Evaluation Schedule, Vendor questions will be researched and the official responses published as an amendment to this RFP and published to the Department of General Administration Office of State Procurement (GA/OSP) Web site at <http://www.ga.wa.gov/Webs/index.html>. This will ensure accurate, consistent responses to all Vendors. Vendors are responsible for checking the Web site for this information.

F. Mandatory Intent to Respond

Vendors must indicate their intent to respond to the RFP Coordinator by the due date and time designated in the acquisition schedule. Letters of intent may be sent via mail, fax, or e-mail. The burden is on the Vendor to ensure timely delivery. The letter of intent should affirm that the Vendor can provide a proven ACCESS solution and other applicable standards included in the RFP requirements, and that the Vendor has sufficient capacity to meet the requirements defined in the RFP. The letter of intent should provide contact information to ensure correct distribution of notices pertaining to this RFP.

G. Submission of Proposals

Proposals must be submitted in hard copy and electronically. Proposals may not be transmitted via facsimile.

Vendors are required to submit five (5) copies of their proposal. One (1) copy must have original signatures and four (4) copies can have photocopied signatures. The proposal submission must include a copy of the proposal on CD using clearly labeled file names including the vendor name. The proposal, whether mailed or hand delivered, must be received by the AGENCY no later than 4:00 p.m. local time in Olympia, Washington, on the date in the evaluation schedule provided in Section I.C. The proposal is to be sent to:

Washington State Patrol ACCESS – Request for Proposals
Attn: Steven R. Cole, Senior Project Manager
Washington State Patrol
Information Technology Division
403 Cleveland Avenue Southeast, Suite C
Tumwater, Washington 98501-3311

Hand delivered proposals must be submitted to Information Technology Division Reception:

Suite C
403 Cleveland Avenue Southeast
Tumwater, Washington

Vendors mailing proposals should allow normal mail delivery time to ensure timely receipt of their proposals by the RFP Coordinator. Vendors hand delivering proposals should allow time for traffic congestion. Vendors assume the risk for the method of delivery chosen. The AGENCY assumes no responsibility for delays caused by any delivery service.

Late proposals will not be accepted and will be automatically disqualified from further consideration. The proposals must respond to the procurement requirements. Do not respond by referring to material presented elsewhere. The proposal must be complete and must stand on its own merits.

Failure to respond to any portion of the procurement document may result in rejection of the proposal as non-responsive. All proposals and any accompanying documentation become the property of the AGENCY and will not be returned.

H. Supplemental Materials

Vendors may submit supplemental materials such as brochures, articles, specifications, or report samples they believe to be helpful, subject to the following:

- Such materials will not qualify as substitutes for direct answers within the response.
- Such materials may be referenced in, but must not be combined with a required component of the response.
- Such materials are for the benefit of the evaluators, but they will not be required to use them. Therefore, answers to the responses must be complete.

I. Proprietary Information / Public Disclosure

Materials submitted in response to this competitive procurement shall become the property of the AGENCY.

Any information in the proposal that the Consultant desires to claim as proprietary and exempt from disclosure under the provisions of Chapter 42.56 RCW **or other state or federal law that provides for the nondisclosure of your document** must be clearly designated. The information must be clearly identified and the particular exemption from disclosure upon which the Consultant is making the claim must be cited. Each page containing the information claimed to be exempt from disclosure must be clearly identified by the words "Proprietary Information" printed on the lower right hand corner of the page. Marking the entire proposal exempt from disclosure or as Proprietary Information will not be honored.

If a public records request is made for the information that the Consultant has marked as "Proprietary Information," the Agency will notify the Consultant of the request and of the date that the records will be released to the requester unless the Consultant obtains a court order enjoining that disclosure. If the Consultant fails to obtain the court order enjoining disclosure, the Agency will release the requested information on the date specified. If a Consultant obtains a court order from a court of competent jurisdiction enjoining disclosure pursuant to Chapter 42.56 RCW, or other state or federal law that provides for nondisclosure, the Agency shall maintain the confidentiality of the Consultant's information per the court order. (This recently changed.)

A charge will be made for copying and shipping, as outlined in RCW 42.56. No fee shall be charged for inspection of contract files, but twenty-four (24) hours notice to the RFP Coordinator is required. Inspection will not be allowed until questions of exemption from disclosure are resolved. All requests for information should be directed to the RFP Coordinator.

J. Minority and Women-Owned Business Participation

In accordance with the legislative findings and policies set forth in Chapter 39.19 RCW, the state of Washington encourages participation in all of its contracts by firms certified by the Office of Minority and Women's Business Enterprises (OMWBE). Participation may be either on a direct basis in response to this solicitation or on a subcontractor basis. However, no preference will be included in the evaluation of proposals, no minimum level of MWBE participation shall be required as a condition for receiving an award, and proposals will not be rejected or considered non-responsive on that basis.

K. Acceptance Period

With respect to this RFP, the proposal and associated prices must remain valid for 180 days following receipt of the proposal, except for any price reductions that may occur during the interim.

L. Responsiveness

All proposals will be reviewed by the RFP Coordinator to determine compliance with administrative requirements and instructions specified in this RFP. The Vendor is specifically notified that failure to comply with any part of the RFP may result in rejection of the proposal as non-responsive.

The AGENCY also reserves the right, however, at its sole discretion to waive minor administrative irregularities.

M. Award Based On Multiple Factors

The evaluation process is designed to award the contract to the Vendor whose proposal best meets the requirements of this RFP. The AGENCY'S Executive Selection Team will make the final selection after analysis of the proposals has been submitted.

N. Contract and General Terms and Conditions

The apparent successful contractor will be expected to enter into a contract that is substantially the same as the sample contract and its general terms and conditions attached as APPENDIX I. In no event is a Vendor to submit its own general contract terms and conditions in response to this solicitation. Special terms and conditions covering licensing agreements, escrow, and other matters unique to the services proposed will be considered. The Vendor may submit exceptions to APPENDIX I as allowed in the Certifications and Assurances section, APPENDIX J to this solicitation. The AGENCY will review requested exceptions and accept or reject the same at its sole discretion.

O. Costs to Propose

The AGENCY will not be liable for any costs incurred by the Vendor in preparation of a proposal submitted in response to this RFP, in conduct of a presentation, or any other activities related to responding to this RFP.

P. No Obligation to Contract

This RFP does not obligate the state of Washington or the AGENCY to contract for services specified herein.

Q. Funding

Any contract awarded as a result of this procurement is contingent upon the availability of funding.

R. Rejection Of Proposals

The AGENCY reserves the right at its sole discretion to reject any and all proposals received without penalty and not to issue a contract as a result of this RFP.

S. Failure to Comply

Vendors must provide a response to all sections and requirements of this RFP to be considered complete. Vendor's failure to comply with any part of AGENCY's Request for Proposal may result in the Vendor's proposal being disqualified for being non-responsive to the AGENCY's request.

T. Waivers

AGENCY reserves the right to waive specific terms and conditions contained in this RFP. It shall be understood by Vendors that the proposal is predicated upon acceptance of all terms and conditions contained in this RFP, unless the Vendor has obtained such a waiver in writing from the AGENCY prior to submission of the proposal. Such a waiver, if granted, will be granted to all Vendors.

U. Commitment of Funds

The Director of the AGENCY or his/her delegate are the only individuals who may legally commit the AGENCY to the expenditures of funds for a contract resulting from this RFP. No cost chargeable to the proposed contract may be incurred before receipt of a fully executed contract.

V. Electronic Payment

The state of Washington prefers to utilize electronic payment in its transactions. The successful contractor will be provided a form to complete with the contract to authorize such payment method.

W. Insurance Coverage

The Contractor is to furnish the AGENCY with a certificate(s) of insurance executed by a duly authorized representative of each insurer, showing compliance with the insurance requirements set forth in the sample contract in APPENDIX I.

The Contractor shall, at its own expense, obtain and keep in force insurance coverage that shall be maintained in full force and effect during the term of the contract. The Contractor shall furnish evidence in the form of a Certificate of Insurance that insurance shall be provided, and a copy shall be forwarded to the AGENCY within fifteen (15) days of the contract effective date.

X. Response Property of the Agency

All materials submitted in response to this procurement become the property of the AGENCY. The AGENCY has the right to use any of the ideas presented in any response. Selection or rejection of a response does not affect this right.

Y. Minor Administrative Irregularities

The AGENCY reserves the right to waive, at its sole discretion, minor administrative irregularities contained in any Vendor response.

Z. Errors In Response

The AGENCY is not liable for any errors in Vendor responses. Vendors will not be allowed to alter response documents after the deadline for response submission. Vendors are liable for all errors or omissions contained in their responses.

AA. RFP Amendments

The AGENCY reserves the right to change the acquisition schedule or to amend the RFP or subsequent solicitation documents related to the original RFP at any time.

The AGENCY reserves the right to make corrections or amendments due to errors or misunderstandings identified in the RFP or subsequent solicitation documents related to the original RFP. Any changes will be date and time stamped and attached to, and made a part of the RFP. All changes must be coordinated in writing with, authorized by, and made by the RFP Coordinator. All corrections and amendments will be posted to the GA/OSP Web site.

All Vendors who received the original solicitation document which was later amended will be notified of the amendment and given the opportunity to resubmit their proposals in relation to the amendment. Vendors are responsible for checking the Web site for this information. The AGENCY will not send corrections and amendments to Vendors.

BB. Points of Clarification

The AGENCY reserves the right to contact Vendors for clarification of anything contained in any response; however, Vendors should not assume that deficient answers will result in clarification requests. The right of clarification is not a Vendor's right; it is a The AGENCY'S right that will be employed only if the AGENCY believes it is absolutely necessary.

CC. Right to Cancel

The AGENCY reserves the right to cancel or reissue this RFP at any time without obligation or liability.

DD. No Multiple Award

The AGENCY anticipates that only one (1) Apparent Successful Vendor will be identified via this procurement and that only one (1) Contract will be awarded.

EE. Incorporation of Solicitation Document(s) Into Contract

This RFP, in addition to the Vendor's response, will be incorporated into any resulting Contract.

FF. Payment for Project Deliverables

Vendor payments will be paid thirty (30) days following receipt and satisfactory acceptance of project deliverables or invoices as applicable.

Specific payment amounts and project deliverables will be negotiated with the Apparent Successful Vendor.

GG. No Costs Chargeable

No costs chargeable to the proposed Contract may be incurred before receipt of a fully executed Contract.

HH. Non-Endorsement

The selection of a Vendor to supply products and/or services to the State of Washington does not mean that the State is endorsing or suggesting that the Vendor's products and/or services are the best or only solution. The Vendor will make no reference to the AGENCY or the State of Washington in any literature, promotional material, brochures, sales presentation, or the like, without the express prior written consent of the AGENCY.

II. Single Response

If there is a response from only one Vendor, then the AGENCY may deem the procurement as a failure of competition and, at the sole option of the AGENCY, may cancel the RFP. Alternatively, the AGENCY may choose to name the single Vendor as the Apparent Successful Vendor.

JJ. Withdrawal of Response

Vendors may withdraw submitted responses at any time up to the response due date and time identified in the Acquisition Schedule. To accomplish this, a written request signed by an authorized representative of the Vendor must be submitted to the RFP Coordinator. The AGENCY will accept a faxed or e-mailed letter of withdrawal. After withdrawing a previously submitted response, the Vendor may submit another response at any time up to the response due date and time.

KK. Announcement of Apparently Successful Vendor

All Vendors responding to the procurement shall be notified by the RFP coordinator by e-mail when the Apparently Successful Vendor has been determined. The tentative schedule for the announcement is identified in the Evaluation Schedule.

In the event that contract negotiations or due diligence prior to contract signing, or subsequent performance during the trial period of the contract with the Apparently Successful Vendor are unacceptable or unsuccessful, the AGENCY reserves the right to

approach the remaining finalist Vendor to, at the AGENCY'S option, designate that Vendor as the Apparently Successful Vendor and enter into negotiations.

LL. Optional Vendor Debriefing

Vendors who submit a response may request an optional debriefing conference to discuss the evaluation of their response. The requested debriefing conference must occur on or before the date specified in the Acquisition Schedule. The request must be in writing addressed to the RFP Coordinator within three business days of announcement of the apparently successful Vendor. The AGENCY will accept the request via fax or e-mail. The debriefing will occur within five business days of the request. The debriefing will not include any comparison between the Vendor's response and any other responses submitted. Debriefing conferences may be conducted in person or by telephone and will be scheduled for a maximum of one (1) hour.

MM. Vendor Complaints

A complaint may be made before a Vendor responds to the RFP if the Vendor believes that the RFP unduly constrains competition or contains inadequate or improper criteria. The written complaint must be submitted to the RFP Coordinator at the address specified and received at least one working day prior to the Vendor Proposal due date. The solicitation process may, however, continue.

NN. Protest Procedures

Protest procedures are available to Vendors who have submitted a response to this RFP and have received a debriefing conference. Protests may be made after the AGENCY has announced the Apparent Successful Vendor (ASV) and after the protesting Vendor has had a debriefing conference with the AGENCY. Protests may be made on only these grounds:

1. Arithmetic errors were made in computing the score.
2. The AGENCY failed to follow procedures established in the solicitation document, the IT Investment Policy, the IT Investment Standards, or applicable state or federal laws or regulations.
3. There was bias, discrimination, or conflict of interest on the part of an evaluator.

Protests shall be in writing and made to the RFP Coordinator serving on behalf of the AGENCY within five (5) business days of the Vendor's debriefing conference.

If the protesting bidder is not satisfied with the AGENCY's decision, it may appeal. Appeal is made to the director of the Washington State DIS.

Written notice of appeal to DIS must be received by DIS within five business days after the bidder receives notification of the AGENCY's decision. In conducting its review, DIS will

consider all available relevant facts. DIS will resolve the appeal in one of the following ways:

- Find that the protest lacks merit and uphold the AGENCY's action.
- Find only technical or harmless errors in the AGENCY's acquisition process, determining the AGENCY to be in substantial compliance, and rejecting the protest; or
- Find merit in the protest and provide options to the AGENCY, including:
 - » Correcting errors and reevaluating all proposals;
 - » Reissuing the solicitation document; or
 - » Making other findings and determining other courses of action as appropriate.

DIS will issue a written decision within five business days after receipt of the notice of appeal, unless more time is needed. The protesting bidder will be notified if additional time is necessary. DIS' determination is final; no further administrative appeal is available.

OO. Covered Services

Products and services available under any resulting Contract will be consistent with those specified in this RFP.

PP. Certifications and Assurances

The Certifications and Assurances form (APPENDIX J) must be signed and dated by a person authorized to legally bind the Vendor to a contractual relationship and submitted with the remaining proposal elements.

Exceptions to the contract (APPENDIX I) must be identified and attached to the Certifications and Assurances Form.

Note that DIS has a clause it requires to be in the standard contract regarding secure use of their facilities in the event that the vendor may require use of DIS capabilities in the future.



Appendix A

ACCESS Message Formats

Appendix A – ACCESS Message Formats

This appendix presents the current ACCESS message formats. The purpose of the tables and images in this section is to provide an informative view of the current ACCESS functional level. Although it is required that the ACCESS replacement must provide functionality at least at the level of the current ACCESS, and message transaction formatting must remain the same, this section does not necessarily represent specific requirements. For example, the forms and screens are not required to look as they appear in this section, and vendors are encouraged to propose alternative presentation forms or screens.

NOTE: Regional system interfaces cannot be changed (either message format or protocol) with the implementation of the new system.

WSP Regional Message Header Format (WRG)

From Mnemonic	AUX	To List	D	Message Content
---------------	-----	---------	---	-----------------

Field Name	Type	Size	Edit Rules or Range of Values
From Mnemonic	Alpha-Numeric	2 to 5	Required.
AUX	Alpha-Numeric	4	Value Not Required. - If not 4 bytes, must be blank filled. - Information placed in the input message by Regional to be returned in the output message.
To List	Alpha-Numeric	2 to 5	Required. - A list of mnemonics for which the message is to be sent. - If there is a list of mnemonics, they must be separated by commas. - If this message is a MSS command, then this field must be empty, 0 bytes long. - The mnemonics cannot be more than 5 bytes.
D (delimiter)	Alpha	1	A period “.”.
Message Content	Alpha-Numeric	1 to XXX	Text.

WSP Database Message Header Format (WSPDB)

From Mnemonic	AUX	To List	D	Message Content
----------------------	------------	----------------	----------	------------------------

Field Name	Type	Size	Edit Rules or Range of Values
From Mnemonic	Alpha-Numeric	2 to 5	Required.
AUX	Alpha-Numeric	4	Value Not Required. - If not 4 bytes, must be blank filled. - Information placed in the input message by Regional to be returned in the output message.
To List	Alpha-Numeric	2 to 5	- Required. - A list of mnemonics for which the message is to be sent. - If there is a list of mnemonics, they must be separated by commas. - If this message is a MSS command, then this field must be empty, 0 bytes long. - The mnemonics cannot be more than 5 bytes.
D (delimiter)	Alpha	1	A period “.”.
Message Content	Alpha-Numeric	1 to XXX	Text.

Terminal-to-Terminal Message Format

In-State Message Headers

Single Address: **T.XXXXX;(send)**

Multiple Address: **T.XXXXX,YYYYY,ZZZZ;(send)**

Out-of-State Message Headers

Single Address: **T.NLTAP,XXXXX;AM.CA0192000.*LASO062699.(send)**

The Optional Control Field, if used, is preceded by an asterisk () and ended with a period (.). When answering a message that contains the optional Control Field, it **MUST** be included as received in the response.*

Multiple Address: **T.NLTAP,XXXXX;AM.CA0194200,OR0260200.(send)**

Standard Message Format

Vendors are encouraged to present alternate solutions/screens to provide the current functionality.

T.XXXXX,YYYYY,ZZZZ,NLTAP;AM.OR0260200.	ACCESS/NLETS Header
PD SEATTLE SP VANCOUVER PD PORTLAND OR	Literal Address
REFER STOLEN VEHICLE RECORD, NIC/V123456789 MESSAGE TEXT.....TEXT TEXT	Referral (if any) Text of message
CHIEF MCCULLEY PD ELMA WA DW	Authority Signature/Operator initials

On NLETS messages, the first line of text, which in most cases is the literal address, **MUST** begin on the line below the header.

The terminal address for out-of-state AM messages via NLETS is "NLTAP." This is an ACCESS system mnemonic for the NLETS "application." **DO NOT** use "NLETS" as the terminal address in your out-of-state AM messages, they will be sent to an error queue and will not reach their intended destination.

ONLINE MESSAGE RECALL

ACCESS provides the ability to recall transactions and messages sent or received by your terminal or printer from the system log files. Messages remain in the system log file for approximately 7 days before being overwritten. You can only recall messages sent or received by your specific terminal. Message recall is accomplished through the use of a "form" similar to a WACIC entry form. Begin the recall by entering the following command:

To recall messages sent from
your
or received on your terminal screen:
RECALL(send)

To recall messages received on
printer:
RECALLP(send)

You will be presented with the following form:

M. @.RECALL.001

ON LINE RECALL

MM/DD/YY

HH:MM

DATE: 12/25/99

STARTING TIME: 13:15

DATE: 12/25/99

ENDING TIME: 14:15

__RECEIVED BY STATION __SENT BY STATION

SEQUENCE NUMBER RANGE

FROM: _____ TO: _____

**IF NOT ENTERED, ENDING TIME IS ONE HOUR LATER THAN STARTING TIME IF
SEQUENCE NUMBER ENTERED THEN ENTIRE DAY IS SCANNED (CURRENT DAY IF
NO DATE ENTERED)**

NEW DESTINATION MNEMONIC: _____

By default, the starting and ending dates and times will be set to one hour prior to the current time, you may change either or both.

Place an "X" in the space before either "RECEIVED BY STATION" or "SENT BY STATION" (not both). The "TAB" key moves the cursor forward to the next field in the form. Using the TAB key, position the cursor on the line below the last line of the form ("NEW DESTINA-

Vendors are encouraged to present alternate solutions/screens to provide the current functionality.

TION MNEMONIC.....”) and transmit the form. You will then be presented with another form, illustrated below, which will allow you to select the message(s) you wish to recall.

```

M.@.RCLSUM.001 6C0100I1SEAPD394008W
      ONLINE RECALL MESSAGE SUMMARY                __ NEXT __
PREV                                     PAGE
  SEQ NUM FROM:  ____ TO:  ____ NEW DESTINATION MNEMONIC  __ PAGE
01 OF 03
S SSN DATE   TIME FROM TO      MESSAGE
_ 02086 12/25/99 1320 SEAPD SEASO MSG TEXT MSG TEXT MSG TEXT
_ 02088 12/25/99 1335 SEAPD TACPD MSG TEXT MSG TEXT MSG TEXT MSG TEXT
_ 02089 12/25/99 1350 SEAPD      MSG TEXT MSG TEXT
-----/\/\-----/\/\-----
      (PLACE AN 'X' IN THE 'S' COLUMN TO RECALL THE ENTIRE MESSAGE)
  
```

If there is more than one page in the recall summary, successive pages can be retrieved by placing the page number (“2”, “3”, “15”, etc.) in the “PAGE ## OF ##” field, or an “X” in either the “NEXT” or “PREV PAGE” fields and transmitting the form. To recall one or more message(s) from the summary, place an “X” in the field at the beginning of the appropriate line(s) and transmit the form. Sent messages will return to your screen, received messages will return to the screen or printer depending on length.

System Memo File

Single Memo Inquiry

I;151(send)

Multiple Memo Inquiry (prints all memos in the specified range)

I;201-220(send)

Update Memo

(You may only update memos that have been assigned to your agency and your terminal has been authorized to update).

M;A.memo #;

text(send)

Vendors are encouraged to present alternate solutions/screens to provide the current functionality.

WebMSS Browser-Based Entry Format

Vendors are encouraged to present alternate solutions/ screens to provide the current functionality.

Workstation - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Media Mail Print View Source

Address <https://access.wsp.wa.gov/webmss/index.html> Go Links

MKE/ ECO ORI/ SID/ SEX/ RAC/ POB/ DOB/

NAM/ WGT/ EYE/ HAI/ FBI/ SKN/

SMT/ FPC/ MNU/

SOC/ OLN/ OLS/ OLY/ LIC/

LIS/ LIY/ LIT/ VIN/ VYR/

VMA/ VMO/ VST/ VCO/ OOC/

CMC/ SCI/ DOA/

INC/ DSS/ SUPORI/

DPE/ SUPNAM/

OCA/

SUPTTEL/ CONTEL/ TMNE/

(supervision) DOE/ ARI/

LOC/ WNO/

CRI/ S/F NAM/

S/F DOB/ S/F SOC/ S/F MNU/

S/F OLN/ S/F OLS/ S/F OLY/ DNA/

DLO/

(notify) FLAG/ N

MIS/

CNDNO/ CND/ CNDLiteral/

CNDLiteralShort/ (condition) DATE/

(condition) DOE/ ARRFLAG/ N NCIC Submit/

EML/

NONE SP08 Send Receive Clear Command Mask Config History

Done Internet

start RR Guide 0506 - Mig... Workstation - Microso...

3:36 PM



Appendix B

ACCESS Message Keys

Appendix B – ACCESS Message Keys

This appendix presents the current ACCESS message keys. The purpose of the table is to provide an informative view of the current ACCESS functional level.

TRANSACTION ID	LITERAL	FROM	TO	CREATES	RESPONSE EXPECTED	STARTING
CAA	CLEAR ARTICLE GROUP	Agency	ACCESS	CASA CAA, CAAT	Y	CAA
CASA	CLEAR ARTICLE GROUP	ACCESS	W2/WACIC		Y	
CAA	CLEAR ARTICLE GROUP	W2/WACIC	NCIC		Y	
CAAT	CLEAR ARTICLE GROUP TEST	W2/WACIC	ACCESS	CAA	Y	
CAS	CLEAR ARTICLE STOLEN	Agency	W2/WACIC	CA, CAT	Y	CAS
CA	CLEAR STOLEN ARTICLE	W2/WACIC	NCIC		Y	
CAT	CLEAR STOLEN ARTICLE TEST	W2/WACIC	ACCESS	CA	Y	
CCO	CLEAR SUPERVISED PERSON	Agency	W2/WACIC	CC, CCT	Y	CCO
CC	CLEAR SUPERVISED PERSON	W2/WACIC	NCIC		Y	
CCT	CLEAR SUPERVISED PERSON TEST	W2/WACIC	ACCESS	CC		
CC	CLEAR SUPERVISED PERSON TEST	ACCESS	NCIC TEST		Y	
CAP	CLEAR PAWNED ARTICLE	Agency	W2/WACIC		Y	
CAR	CLEAR RECOVERED ARTICLE	Agency	W2/WACIC		Y	
CBS	CLEAR STOLEN BOAT	Agency	NCIC	CB	Y	CBS
CGP	CLEAR PAWNED GUN	Agency	W2/WACIC		Y	
CPP	CLEAR PAWNED PART	Agency	W2/WACIC		Y	
CPR	CLEAR RECOVERED PART	Agency	W2/WACIC		Y	
CSM	CLEAR SINGLE SECURITY	Agency	NCIC	CS	Y	CSM
CSSM	CLEAR GROUP SECURITY	CSSM	NCIC	CSS CFG, CFGT	Y	CSSM
CGF	CLEAR GUN FELONY	Agency	W2/WACIC		Y	CGF
CFG	CLEAR FELONY GUN	W2/WACIC	NCIC		Y	
CFGT	CLEAR GUN FELONY TEST	W2/WACIC	ACCESS	CFG CLG, CLGT	Y	
CGM	CLEAR GUN MISSING	Agency	W2/WACIC		Y	CGM
CLG	CLEAR LOST GUN	W2/WACIC	NCIC		Y	
CLGT	CLEAR LOST GUN TEST	W2/WACIC	ACCESS	CLG	Y	
CGS	CLEAR STOLEN GUN	Agency	W2/WACIC	CG, CGT	Y	CGS
CG	CLEAR GUN	W2/WACIC	NCIC		Y	

TRANSACTION ID	LITERAL	FROM	TO	CREATES	RESPONSE EXPECTED	STARTING
CGT	CLEAR STOLEN GUN TEST	W2/WACIC	ACCESS	CG	Y	
CLS	CLEAR LICENSE PLATE STOLEN	Agency	W2/WACIC	CL, CLT	Y	CLS
CL	CLEAR LICENSE PLATE STOLEN	W2/WACIC	NCIC		Y	
CLT	CLEAR LICENSE PLATE STOLEN TEST	W2/WACIC	ACCESS	CL	Y	
CM	CLEAR MISSING PERSON	Agency	W2/WACIC	CMT	Y	CM
CM	CLEAR MISSING PERSON	W2/WACIC	NCIC		Y	
CMT	CLEAR MISSING PERSON TEST	W2/WACIC	ACCESS	CM	Y	
CPO	CLEAR PROTECTION ORDER	Agency	W2/WACIC	CPOT	Y	CPO
CPO	CLEAR PROTECTION ORDER	W2/WACIC	NCIC		Y	
CPOT	CLEAR PROTECTION ORDER TEST	W2/WACIC	ACCESS	CPO CTO, CTOT	Y	
CPO	CLEAR TEMP PROTECTION ORDER	Agency	W2/WACIC		Y	CPO
CTO	CLEAR TEMP PROTECTION ORDER	W2/WACIC	NCIC			
CTOT	CLEAR TEMP PROTECTION ORDER TEST	W2/WACIC	ACCESS	CTO	Y	
CPS	CLEAR STOLEN PART	Agency	W2/WACIC	CP, CPT	Y	CPS
CP	CLEAR STOLEN PART	W2/WACIC	NCIC		Y	
CPT	CLEAR STOLEN PART TEST	W2/WACIC	ACCESS	CP CGR, CRGT	Y	
CRG	CLEAR RECOVERED GUN	Agency	W2/WACIC		Y	CRG
CGR	CLEAR RECOVERED GUN	W2/WACIC	NCIC		Y	
CRGT	CLEAR RECOVERED GUN TEST	W2/WACIC	ACCESS	CGR	Y	
CTF	CLEAR TEMPORARY FELONY WANT	Agency	W2/WACIC	CT, CTT	Y	CTF
CT	CLEAR TEMPORARY FELONY WANT	W2/WACIC	NCIC		Y	
CTT	CLEAR TEMPORARY FELONY WANT TEST	W2/WACIC	ACCESS	CT		
CT	CLEAR TEMPORARY FELONY WANT TEST	ACCESS	NCIC TEST		Y	
CU	CLEAR UNIDENTIFIED PERSON	Agency	W2/WACIC	CUT	Y	CU
CU	CLEAR UNIDENTIFIED PERSON	W2/WACIC	NCIC		Y	
CUT	CLEAR UNIDENTIFIED PERSON TEST	W2/WACIC	ACCESS	CU CV, CVS, CVT	Y	
CVS	CLEAR STOLEN VEHICLE	Agency	W2/WACIC		Y	CVS
LE	LOJACK	ACCESS	NLETS		N	
CVS	CLEAR STOLEN VEHICLE	W2/WACIC	DOL		N	
CV	CLEAR STOLEN VEHICLE	W2/WACIC	NCIC		Y	
CVT	CLEAR STOLEN VEHICLE TEST	W2/WACIC	ACCESS	CV		

TRANSACTION ID	LITERAL	FROM	TO	CREATES	RESPONSE EXPECTED	STARTING
CT	CLEAR STOLEN VEHICLE TEST	ACCESS	NCIC TEST		Y	
CVI	CLEAR STOLEN VEHICLE IMPOUND	Agency	W2/WACIC	NCI	Y	CVI
NCI	NICB CANCEL IMPOUND VEHICLE NICB CANCEL IMPOUND VEHICLE	W2/WACIC	NLETS	NCA	Y	
NCA	RESPONSE	NLETS	Agency			
CVW	CLEAR WANTED FELONY VEHICLE	Agency	W2/WACIC	CF, CFT	Y	CVW
CF	CLEAR FELONY VEHICLE	W2/WACIC	NCIC		Y	
CFT	CLEAR FELONY VEHICLE TEST	W2/WACIC	ACCESS	CF		
CF	CLEAR FELONY VEHICLE TEST	ACCESS	NCIC TEST		Y	
CWF	CLEAR WANTED FELONY	Agency	W2/WACIC	CW, CWT	Y	CWF
CW	CLEAR WANTED PERSON	W2/WACIC	NCIC		Y	
CWT	CLEAR WANTED PERSON TEST	W2/WACIC	ACCESS	CW		
CW	CLEAR WANTED PERSON TEST	ACCESS	NCIC TEST		Y	
CWJ	CLEAR WANTED JUVENILE	Agency	W2/WACIC	CW	Y	CWJ
CW	CLEAR WANTED CLEAR WANTED MISDEMEANOR (IF TYPE MN)	W2/WACIC Agency	NCIC W2/WACIC		Y Y	
CWW				CW		CWW
CW	CLEAR WANTED CLEAR WANTED MISDEMEANOR (IF TYPE MS)	W2/WACIC Agency	NCIC W2/WACIC		Y Y	
CWW						CWW
CXS	CLEAR SEX OFFENDER WANTED PERSON AND DRIVER	W2/WACIC	NCIC		Y	
DW	INQUIRY	Agency	ACCESS	D, QW	Y	DW
D	DRIVER QUERY	ACCESS	DOL		Y	
QW	WANTED QUERY	ACCESS	W2/WACIC		Y	
QW	WANTED QUERY	W2/WACIC	NCIC		Y	
EAA	ENTER ARTICLE GROUP	Agency	ACCESS	EASA EAA, EAAT	N	EAA
EASA	ENTER ARTICLE GROUP	ACCESS	W2/WACIC		Y	
EAA	ENTER ARTICLE GROUP	W2/WACIC	NCIC		Y	
EAAT	ENTER ARTICLE GROUP TEST	W2/WACIC	ACCESS	EAA	Y	
EASN	ENTER STOLEN ARTICLE (W2 & NCIC)	Agency	W2/WACIC	EA, EAT	Y	EASN
EA	ENTER STOLEN ARTICLE	W2/WACIC	NCIC		Y	
EAT	ENTER STOLEN ARTICLE TEST	W2/WACIC	ACCESS	EA ECN, ECNT	Y	
EN	ENTER SUPV PERSON SUPP DATA	Agency	W2/WACIC		Y	EN
ECN	ENTER SUPV PERSON SUPP DATA	W2/WACIC	NCIC		Y	

TRANSACTION ID	LITERAL	FROM	TO	CREATES	RESPONSE EXPECTED	STARTING
ECNT	ENTER SUPV PERSON SUPP DATA TEST	W2/WACIC	ACCESS	ECN		
ECN	ENTER SUPV PERSON SUPP DATA TEST	ACCESS	NCIC TEST		Y	
ENS	ENTER S/F SUPP DATA	Agency	W2/WACIC	ECNS, ECST	Y	ENS
ECNS	ENTER S/F SUPP DATA	W2/WACIC	NCIC		Y	
ECST	ENTER S/F SUPP DATA TEST	W2/WACIC	ACCESS	ECNS	Y	
ENS	ENTER S/F SUPP DATA	Agency	W2/WACIC	ENST	Y	ENS
ENS	ENTER S/F SUPP DATA	W2/WACIC	NCIC		Y	
ENST	ENTER S/F SUPP DATA TEST	W2/WACIC	ACCESS	ENS	Y	
ECO	ENTER SUPERVISED PERSONS (NCIC SUB = Y)	Agency	W2/WACIC	EC, ECT	Y	ECO
EC	ENTER SUPERVISED PERSONS	W2/WACIC	NCIC		Y	
ECT	ENTER SUPERVISED PERSONS TEST	W2/WACIC	ACCESS	EC		
EC	ENTER SUPERVISED PERSONS TEST	ACCESS	NCIC TEST		Y	
ECO	ENTER SUPERVISED PERS CAUTION (NCIC SUB = Y)	Agency	W2/WACIC	EC, ECCT	Y	ECO
EC	ENTER SUPERVISED PERS CAUTION	W2/WACIC	NCIC		Y	
ECCT	ENTER SUPERVISED PERSON CAUTION TEST	W2/WACIC	ACCESS	EC-C		
EC-C	ENTER SUPERVISED PERSON CAUTION TEST	ACCESS	NCIC TEST		Y	
ECO	ENTER SUPERV PERSONS NCIC (SUB = N)	Agency	W2/WACIC		Y	ECO
ECO	ENTER SUPERVISED PERSONS CAUTION NCIC (SUB = N)	Agency	W2/WACIC		Y	ECO
EDP	ADD STATE INDEX NICS	Agency	NCIC		Y	
EAP	ENTER PAWNED ARTICLE	Agency	W2/WACIC		Y	
EAR	ENTER RECOVERED ARTICLE	Agency	W2/WACIC		Y	
EAS	ENTER STOLEN ARTICLE W2 ONLY	Agency	W2/WACIC		Y	
EBS	ENTER BOAT STOLEN	Agency	ACCESS	EB		EBS
EB	ENTER BOAT STOLEN	ACCESS	NCIC		Y	
EBSA	ENTER STOLEN BOAT ARMED	Agency	ACCESS	EB-A		EBSA
EB-A	ENTER STOLEN BOAT ARMED	ACCESS	NCIC		Y	
EBSF	ENTER STOLEN BOAT ARMED/LATENTS	Agency	ACCESS	EB-F		EBSF

TRANSACTION ID	LITERAL	FROM	TO	CREATES	RESPONSE EXPECTED	STARTING
EB-F	ENTER STOLEN BOAT ARMED/LATENTS	ACCESS	NCIC		Y	
EBSP	ENTER STOLEN BOAT LATENTS	Agency	ACCESS	EB-P		EBSP
EB-P	ENTER STOLEN BOAT LATENTS	ACCESS	NCIC		Y	
ECOC	ENTER CORRECTIONS CONDITIONS	Agency	W2/WACIC		Y	
ECUS	ENTER CUSTODY STATUS	DOC	W2/WACIC		N	
EGG	ENTER GANG	Agency	NCIC		Y	
EGGM	ENTER GANG MEMBER	Agency	ACCESS	EGM		EGGM
EGM	ENTER GANG MEMBER	ACCESS	NCIC		Y	
EGGN	ENTER GANG SUPPLEMENT	Agency	NCIC		Y	
EGGT	ENTER TERRORIST ORGANIZATION	Agency	NCIC		Y	
EGMN	ENTER GANG MEMBER SUPPLEMEN- TAL	Agency	NCIC		Y	
EGMT	ENTER TERRORIST ORG MEMBER	Agency	NCIC		Y	
EGP	ENTER PAWNED GUN	Agency	W2/WACIC		Y	
EGR	ENTER RECOVERED GUN	Agency	W2/WACIC	ERG, ERGT	Y	
ERG	ENTER RECOVERED GUN	W2/WACIC	NCIC		Y	
ERGT	ENTER RECOVERED GUN TEST	W2/WACIC	ACCESS		Y	
EID	ENTER VIN INSPECTION DATA	Agency	W2/WACIC		Y	
EIDS	ENTER VIN INSPECTION SUPP DATA	Agency	W2/WACIC		Y	
EIP	ENTER PERSON OF INTEREST	Agency	W2/WACIC		Y	
EIPC	ENTER PERSON OF INTEREST CAUTION	Agency	W2/WACIC		Y	
EPP	ENTER PAWNED PART	Agency	W2/WACIC		Y	
EPR	ENTER RECOVERED PART	Agency	W2/WACIC		Y	
ESM	ENTER SINGLE SECURITY	Agency	NCIC	ES	Y	ESM
ESSM	ENTER GROUP SECURITY	Agency	NCIC	ESS	Y	ESSM
EVPQ	ENTER QUESTIONABLE VIN(ATS OLY	Agency	W2/WACIC		Y	
EVR	ENTER REPOSSESSED VEHICLE	Agency	W2/WACIC		Y	
EYN	WATCH YOUR CAR SUPPLEMENTAL	Agency	W2/WACIC		Y	
EYV	WATCH YOUR CAR ENTRY	Agency	W2/WACIC		Y	
EDD	ENTER DENTAL DATA	Agency	W2/WACIC	ED, EDT	Y	EDD
ED	ENTER DENTAL DATA	W2/WACIC	NCIC		Y	
EDT	ENTER DENTAL DATA TEST	W2/WACIC	ACCESS	ED		
EDW	ENTER DETAINER WANTED	Agency	W2/WACIC	DW, DWT	Y	EDW

TRANSACTION ID	LITERAL	FROM	TO	CREATES	RESPONSE EXPECTED	STARTING
DW	ENTER DETAINER WANTED	W2/WACIC	NCIC		Y	
DWT	ENTER DETAINER WANTED TEST	W2/WACIC	ACCESS	DW EFG, EFGT	Y	
EGF	ENTER GUN FELONY	Agency	W2/WACIC		Y	EGF
EFG	ENTER FELONY GUN	W2/WACIC	NCIC		Y	
EFGT	ENTER GUN FELONY TEST	W2/WACIC	ACCESS	EFG EFGP, EFXT	Y	
EGFP	ENTER GUN FELONY LATENT	Agency	W2/WACIC		Y	EGFP
EFGP	ENTER FELONY GUN LATENT	W2/WACIC	NCIC		Y	
EFXT	ENTER GUN FELONY LATENT TEST	W2/WACIC	ACCESS	EFGP ELG, ELGT	Y	
EGM	ENTER MISSING GUN	Agency	W2/WACIC		Y	EGM
ELG	ENTER LOST GUN	W2/WACIC	NCIC		Y	
ELGT	ENTER LOST GUN TEST	W2/WACIC	ACCESS	ELG	Y	
EGMP	ENTER MISSING GUN HOLD PRINTS	Agency	W2/WACIC	ELGP	Y	EGMP
ELGP	ENTER LOST GUN HOLD PRINTS	W2/WACIC	NCIC		Y	
EGS	ENTER STOLEN GUN	Agency	W2/WACIC	EG, EGT	Y	EGS
EG	ENTER STOLEN GUN	W2/WACIC	NCIC		Y	
EGT	ENTER STOLEN GUN TEST	W2/WACIC	ACCESS	EG EG-P, EGPT	Y	
EGSP	ENTER STOLEN GUN HOLD PRINTS	Agency	W2/WACIC		Y	EGSP
EG-P	ENTER STOLEN GUN HOLD PRINTS	W2/WACIC	NCIC		Y	
EGPT	ENTER STOLEN GUN HOLD PRINTS TEST	W2/WACIC	ACCESS	EG-P	Y	
EIM	ENTER IMAGE	Agency	W2/WACIC	EIM, EIMT	Y	
EIM	ENTER IMAGE	W2/WACIC	NCIC		Y	
EIMT	ENTER IMAGE TEST	W2/WACIC	ACCESS	EIM	Y	
EIT	ENTER ID THEFT VICTIM	Agency	W2/WACIC	EID, EIDT	Y	EIT
EID	ENTER ID THEFT VICTIM	W2/WACIC	NCIC		Y	
EIDT	ENTER ID THEFT VICTIM TEST	W2/WACIC	ACCESS	EID		
EID	ENTER ID THEFT VICTIM TEST	ACCESS	NCIC TEST		Y	
EITC	ENTER ID THEFT CAUTION	Agency	W2/WACIC	EIDC, EICT	Y	EITC
EIDC	ENTER ID THEFT CAUTION	W2/WACIC	NCIC		Y	
EICT	ENTER ID THEFT CAUTION TEST	W2/WACIC	ACCESS	EIDC		
EIDC	ENTER ID THEFT CAUTION TEST	ACCESS	NCIC TEST		Y	
EN	ENTER ID THEFT SUPP DATA	Agency	W2/WACIC	EIN, EINT	Y	

TRANSACTION ID	LITERAL	FROM	TO	CREATES	RESPONSE EXPECTED	STARTING
EIN	ENTER ID THEFT SUPP DATA	W2/WACIC	NCIC		Y	
EINT	ENTER ID THEFT SUPP DATA TEST	W2/WACIC	ACCESS	EIN		
EIN	ENTER ID THEFT SUPP DATA TEST	ACCESS	NCIC TEST		Y	
ELS	ENTER LICENSE PLATE STOLEN	Agency	W2/WACIC	EL	Y	ELS
EL	ENTER STOLEN LICENSE PLATE	W2/WACIC	NCIC		Y	
ELSA	ENTER STOLEN LICENSE PLATE - ARMED	Agency	W2/WACIC	EL-A, ELAT	Y	ELSA
EL-A	ENTER STOLEN LICENSE PLATE ARMED	W2/WACIC	NCIC		Y	
ELAT	ENTER STOLEN LICENSE PLATE ARMED TEST	W2/WACIC	ACCESS	EL-A		
EL-A	ENTER STOLEN LICENSE PLATE ARMED TEST	ACCESS	NCIC TEST		Y	
ELSF	ENTER STOLEN LICENSE PLATE – ARMED/ PRINTS	Agency	W2/WACIC	EL-F	Y	ELSF
EL-F	ENTER STOLEN LICENSE PLATE – ARMED/PRINTS	W2/WACIC	NCIC		Y	
ELSP	ENTER LICENSE STOLEN – PRINTS	Agency	W2/WACIC	EL-P, ELPT	Y	ELSP
EL-P	ENTER LICENSE STOLEN – PRINTS	W2/WACIC	NCIC		Y	
ELPT	ENTER LICENSE STOLEN – PRINTS TEST	W2/WACIC	ACCESS	EL-P		
EL-P	ENTER LICENSE STOLEN – PRINTS TEST	ACCESS	NCIC TEST		Y	
EMD	ENTER MISSING PERSON DISABLED	Agency	W2/WACIC	EMDT	Y	EMD
EMD	ENTER MISSING PERSON DISABLED	W2/WACIC	NCIC		Y	
EMDT	ENTER MISSING PERSON DISABLED TEST	W2/WACIC	ACCESS	EMD		
EMD	ENTER MISSING PERSON DISABLED TEST	ACCESS	NCIC TEST		Y	
EMDC	ENTER MISSING DISABLE CAUTION	Agency	W2/WACIC	EDCT	Y	
EMDC	ENTER MISSING DISABLE CAUTION	W2/WACCI	NCIC		Y	
EDCT	ENTER MISSING DISABLE CAUTION TEST	W2/WACCI	ACCESS	EMDC		
EMDC	ENTER MISSING DISABLE CAUTION TEST	ACCESS	NCIC TEST		Y	
EME	ENTER MISSING ENDANGERED	Agency	W2/WACIC	EMET	Y	EME
EME	ENTER MISSING ENDANGERED	W2/WACIC	NCIC		Y	

TRANSACTION ID	LITERAL	FROM	TO	CREATES	RESPONSE EXPECTED	STARTING
EMET	ENTER MISSING ENDANGERED TEST	W2/WACIC	ACCESS	EME		
EME	ENTER MISSING ENDANGERED TEST	ACCESS	NCIC TEST		Y	
EMEC	ENTER MISS ENDANGERED CAUTION	Agency	W2/WACIC	EECT	Y	EMEC
EMEC	ENTER MISS ENDANGERED CAUTION	W2/WACIC	NCIC		Y	
EECT	ENTER MISS ENDANGERED CAUTION TEST	W2/WACIC	ACCESS	EMEC		
EMEC	ENTER MISS ENDANGERED CAUTION TEST	ACCESS	NCIC TEST		Y	
EMI	ENTER MISSING INVOLUNTARY	Agency	W2/WACIC	EMIT	Y	EMI
EMI	ENTER MISSING INVOLUNTARY	W2/WACIC	NCIC		Y	
EMIT	ENTER MISSING INVOLUNTARY TEST	W2/WACIC	ACCESS	EMI		
EMI	ENTER MISSING INVOLUNTARY TEST	ACCESS	NCIC TEST		Y	
EMIC	ENTER MISSING INVOLUNTARY CAUTION	Agency	W2/WACIC		Y	
EMJ	ENTER MISSING JUVENILE	Agency	W2/WACIC	EMJT	Y	EMJ
EMJ	ENTER MISSING JUVENILE	W2/WACIC	NCIC		Y	
EMJT	ENTER MISSING JUVENILE TEST	W2/WACIC	ACCESS	EMJ		
EMJ	ENTER MISSING JUVENILE TEST	ACCESS	NCIC TEST		Y	
EMJC	ENTER MISSING JUVENILE CAUTION	Agency	W2/WACIC	EMMT	Y	EMJC
EMJC	ENTER MISSING JUVENILE CAUTION	W2/WACIC	NCIC		Y	
EMMT	ENTER MISSING JUVENILE CAUTION TEST	W2/WACIC	ACCESS	EMJC		
EMJC	ENTER MISSING JUVENILE CAUTION TEST	ACCESS	NCIC TEST		Y	
EMN	ENTER MISSING SUPPLEMENT DATA	Agency	W2/WACIC	EMNT	Y	EMN
EMN	ENTER MISSING SUPPLEMENT DATA	W2/WACIC	NCIC		Y	
EMNT	ENTER MISSING SUPPLEMENT DATA TEST	W2/WACIC	ACCESS	EMN		
EMN	ENTER MISSING SUPPLEMENT DATA TEST	ACCESS	NCIC TEST		Y	
EMO	ENTER MISSING OTHER	Agency	W2/WACIC	EMOT	Y	EMO
EMO	ENTER MISSING OTHER	W2/WACIC	NCIC		Y	
EMOT	ENTER MISSING OTHER TEST	W2/WACIC	ACCESS	EMO		
EMO	ENTER MISSING OTHER TEST	ACCESS	NCIC TEST		Y	
EMOC	ENTER MISSING OTHER CAUTION	Agency	W2/WACIC		Y	
	ENTER MISSING OTHER CAUTION	W2/WACIC	NCIC		Y	
EMV	ENTER MISSING DISASTER VICTIM	Agency	W2/WACIC	EMVT	Y	EMV

TRANSACTION ID	LITERAL	FROM	TO	CREATES	RESPONSE EXPECTED	STARTING
EMV	ENTER MISSING DISASTER VICTIM	W2/WACIC	NCIC		Y	
EMVT	ENTER MISSING DISASTER VICTIM TEST	W2/WACIC	ACCESS	EMV		
EMV	ENTER MISSING DISASTER VICTIM TEST	ACCESS	NCIC TEST		Y	
EMVC	ENTER MISS DISASTER VICT CAUTION	Agency	W2/WACIC		Y	
	ENTER MISS DISASTER VICT CAUTION	W2/WACIC	NCIC		Y	
EN	ENTER SUPPLEMENTAL DATA	Agency	W2/WACIC	ENT	Y	EN
EN	ENTER SUPPLEMENTAL DATA	W2/WACIC	NCIC		Y	
ENT	ENTER SUPPLEMENTAL DATA TEST	W2/WACIC	ACCESS	EN		
EN	ENTER SUPPLEMENTAL DATA TEST	ACCESS	NCIC TEST		Y	
	ENTER SUPP DATA PROTECTION ORDER			ENPO, ENPT		
EN	ENTER SUPP DATA PROTECTION ORDER	Agency	W2/WACIC		Y	EN
ENPO	ENTER SUPP DATA PROTECTION ORDER	W2/WACIC	NCIC		Y	
ENPT	ENTER SUPP DATA PROTECTION ORDER TEST	W2/WACIC	ACCESS	ENPO		
	ENTER SUPP DATA PROTECTION ORDER TEST	ACCESS	NCIC TEST		Y	
ENPO	ENTER PROTECTION ORDER	Agency	W2/WACIC	EPOT	Y	EPO
EPO	ENTER PROTECTION ORDER	W2/WACIC	NCIC		Y	
EPOT	ENTER PROTECTION ORDER TEST	W2/WACIC	ACCESS	EPO		
EPO	ENTER PROTECTION ORDER TEST	ACCESS	NCIC TEST		Y	
	ENTER PROTECTION ORDER TEMPORARY			ETO, ETOT		
EPO	ENTER PROTECTION ORDER TEMPORARY	Agency	W2/WACIC		Y	EPO
ETO	ENTER PROTECTION ORDER TEMPORARY	W2/WACIC	NCIC		Y	
ETOT	ENTER PROTECTION ORDER TEMPORARY TEST	W2/WACIC	ACCESS	ETO		
	ENTER PROTECTION ORDER TEMPORARY TEST	ACCESS	NCIC TEST		Y	
ETOC	ENTER PROTECTION ORDER CAUTION	Agency	W2/WACIC	EPCT	Y	EPOC
EPOC	ENTER PROTECTION ORDER CAUTION	W2/WACIC	NCIC		Y	

TRANSACTION ID	LITERAL	FROM	TO	CREATES	RESPONSE EXPECTED	STARTING
EPCT	ENTER PROTECTION ORDER CAUTION TEST	W2/WACIC	ACCESS	EPOC		
EPOC	ENTER PROTECTION ORDER CAUTION TEST	ACCESS	NCIC TEST		Y	
EPS	ENTER STOLEN PART	Agency	W2/WACIC	EP, EPT	Y	EPS
EP	ENTER STOLEN PART	W2WACIC	NCIC		Y	
EPT	ENTER STOLEN PART TEST	W2WACIC	ACCESS	EP	Y	
				EP-P,		
EPSP	ENTER STOLEN PART – PRINTS	Agency	W2/WACIC	EPPT	Y	EPSP
EP-P	ENTER STOLEN PART LATENT	W2/WACIC	NCIC		Y	
EPPT	ENTER STOLEN PART PRINTS TEST	W2/WACIC	ACCESS	EP-P	Y	
ESKA	UPDATE SOR ADDRESS	Agency	W2/WACIC	MXS	Y	
MXS	MODIFY SOR RECORD	W2/WACIC	NCIC		Y	
ETF	ENTER TEMPORARY FELONY	Agency	W2/WACIC	ET, ETT	Y	ETF
ET	ENTER TEMPORARY FELONY	W2/WACIC	NCIC		Y	
ETT	ENTER TEMPORARY FELONY TEST	W2/WACIC	ACCESS	ET		
ET	ENTER TEMPORARY FELONY TEST	ACCESS	NCIC TEST		Y	
				ET-C,		
ETFC	ENTER TEMP FELONY CAUTION	Agency	W2/WACIC	ETCT	Y	ETFC
ET-C	ENTER TEMP FELONY CAUTION	W2/WACIC	NCIC		Y	
ETCT	ENTER TEMP FELONY CAUTION TEST	W2/WACIC	ACCESS	ET-C		
ET-C	ENTER TEMP FELONY CAUTION TEST	ACCESS	NCIC TEST		Y	
EUD	ENTER UNIDENTIFIED DECEASED	Agency	W2/WACIC	EUDT	Y	EUD
EUD	ENTER UNIDENTIFIED DECEASED	W2/WACIC	NCIC		Y	
	ENTER UNIDENTIFIED DECEASED TEST	W2/WACIC	ACCESS	EUD		
	ENTER UNIDENTIFIED DECEASED TEST	ACCESS	NCIC TEST		Y	
EUL	ENTER UNIDENTIFIED LIVING	Agency	W2/WACIC	EULT	Y	EUL
EUL	ENTER UNIDENTIFIED LIVING	W2/WACIC	NCIC		Y	
EULT	ENTER UNIDENTIFIED LIVING TEST	W2/WACIC	ACCESS	EUL		
EUL	ENTER UNIDENTIFIED LIVING TEST	ACCESS	NCIC TEST		Y	
	ENTER UNIDENTIFIED PERSON SUPP DATA	Agency	W2/WACIC	EUNT	Y	EUN
EUN	ENTER UNIDENTIFIED PERSON SUPP DATA	W2/NCIC	NCIC		Y	

TRANSACTION ID	LITERAL	FROM	TO	CREATES	RESPONSE EXPECTED	STARTING
EUNT	ENTER UNIDENTIFIED PERSON SUPP DATA TEST	W2/NCIC	ACCESS	EUN		
EUN	ENTER UNIDENTIFIED PERSON SUPP DATA TEST	ACCESS	NCIC TEST		Y	
EUV	ENTER UNIDENT DISASTER VICTIM	Agency	W2/WACIC	EUVT	Y	EUV
EUV	ENTER UNIDENT DISASTER VICTIM	W2/WACIC	NCIC		Y	
EUVT	ENTER UNIDENT DISASTER VICTIM TEST	W2/WACIC	ACCESS	EUV		
EUV	ENTER UNIDENT DISASTER VICTIM TEST	ACCESS	NCIC TEST		Y	
EUVC	ENTER UNIDENT DISASTER VICTIM CAUTION	Agency	W2/WACIC		Y	
EUVC	ENTER UNIDENT DISASTER VICTIM CAUTION	W2/WACIC	NCIC		Y	
EVI	ENTER IMPOUND VEHICLE	Agency	W2/WACIC	NEI	Y	EVI
NEI	NICB ENTER IMPOUND VEHICLE	W2/WACIC	NLETS	NEA	Y	
NEA	NICB ENTER IMPOUND VEHICLE RESPONSE	NLETS	Agency			
EVS	ENTER VEHICLE STOLEN	Agency	W2/WACIC	EV, EVS, LE, EVT	Y	EVS
EVS	ENTER VEHICLE STOLEN	W2/WACIC	DOL		N	
EV	ENTER VEHICLE STOLEN	W2/WACIC	NCIC		Y	
LE	LOJACK	ACCESS	NLETS		Y	
EVT	ENTER VEHICLE STOLEN TEST	W2/WACIC	ACCESS	EV		
EV	ENTER VEHICLE STOLEN TEST	ACCESS	NCIC TEST		Y	
EVSA	ENTER STOLEN VEHICLE – ARMED	Agency	W2/WACIC	EV-A, EVAT	Y	EVSA
EV-A	ENTER STOLEN VEHICLE – ARMED	W2/WACIC	NCIC		Y	
EVAT	ENTER STOLEN VEHICLE – ARMED TEST	W2/WACIC	ACCESS	EV-A		
EV-A	ENTER STOLEN VEHICLE – ARMED TEST	ACCESS	NCIC TEST		Y	
EVSF	ENTER STOLEN VEH – ARMED/PRINT	Agency	W2/WACIC	EV-F	Y	EVSF
EV-F	ENTER STOLEN VEH – ARMED/PRINT	W2/WACIC	NCIC		Y	
EVSP	ENTER STOLEN VEHICLE – PRINTS	Agency	W2/WACIC	EV-P, EVPT	Y	EVSP

TRANSACTION ID	LITERAL	FROM	TO	CREATES	RESPONSE EXPECTED	STARTING
EV-P	ENTER STOLEN VEHICLE – PRINTS	W2/WACIC	NCIC		Y	
EVPT	ENTER STOLEN VEHICLE – PRINTS TEST	W2/WACIC	ACCESS	EV-P		
EV-P	ENTER STOLEN VEHICLE – PRINTS TEST	ACCESS	NCIC TEST		Y	
EVW	ENTER WANTED FELONY VEHICLE	Agency	W2/WACIC	EF, EFT	Y	EVW
EF	ENTER FELONY VEHICLE	W2/WACIC	NCIC		Y	
EFT	ENTER FELONY VEHICLE TEST	W2/WACIC	ACCESS	EF	Y	
EF	ENTER FELONY VEHICLE TEST	ACCESS	NCIC TEST		Y	
EVWA	ENTER WANTED FELONY VEHICLE – ARMED	Agency	W2/WACIC	EF-A, EFAT	Y	EVWA
EF-A	ENTER WANTED FELONY VEHICLE – ARMED	W2/WACIC	NCIC		Y	
EFAT	ENTER WANTED FELONY VEHICLE – ARMED TEST	W2/WACIC	ACCESS	EF-A		
EF-A	ENTER WANTED FELONY VEHICLE – ARMED TEST	ACCESS	NCIC TEST		Y	
EVWF	ENTER WANTED VEH ARMED/PRINTS	Agency	W2/WACIC	EF-F, EFFT	Y	EVWF
EF-F	ENTER WANTED VEH ARMED/PRINTS	W2/WACIC	NCIC		Y	
EFFT	ENTER WANTED VEH ARMED/PRINTS TEST	W2/WACIC	ACCESS	EF-F		
EF-F	ENTER WANTED VEH ARMED/PRINTS TEST	ACCESS	NCIC TEST		Y	
EVWP	ENTER WANTED VEHICLE – PRINTS	Agency	W2/WACIC	EF-P, EFPT	Y	EVWP
EF-P	ENTER WANTED VEHICLE – PRINTS	W2/WACIC	NCIC		Y	
EFPT	ENTER WANTED VEHICLE – PRINTS TEST	W2/WACIC	ACCESS	EF-P		
EF-P	ENTER WANTED VEHICLE – PRINTS TEST	ACCESS	NCIC TEST		Y	
EVIP	ENTER IMPOUND VEHICLE PRIVATE	Agency	W2/WACIC	EVIP	Y	
EWf	ENTER WANTED FELONY	Agency	W2/WACIC	EW, EWT	Y	EWf
EW	ENTER WANTED PERSON	W2/WACIC	NCIC		Y	
EWT	ENTER WANTED PERSON TEST	W2/WACIC	ACCESS	EW		
EW	ENTER WANTED PERSON TEST	ACCESS	NCIC TEST		Y	
EWFC	ENTER WANTED FELONY CAUTION	Agency	W2/WACIC	EW-C, EWCT	Y	EWFC

TRANSACTION ID	LITERAL	FROM	TO	CREATES	RESPONSE EXPECTED	STARTING
EW-C	ENTER WANTED PERSON CAUTION	W2/WACIC	NCIC		Y	
EWCT	ENTER WANTED PERSON CAUTION TEST	W2/WACIC	ACCESS	EW-C		
EW-C	ENTER WANTED PERSON CAUTION TEST	ACCESS	NCIC TEST		Y	
EWJ	ENTER WANTED JUVENILE	Agency	W2/WACIC	EWJ, EWJT	Y	EWJ
EWJ	ENTER WANTED JUVENILE	W2/WACIC	NCIC		Y	
EWJT	ENTER WANTED JUVENILE TEST	W2/WACIC	ACCESS	EWJ		
EWJ	ENTER WANTED JUVENILE TEST	ACCESS	NCIC TEST		Y	
EWJC	ENTER WANTED JUVENILE CAUTION	Agency	W2/WACIC	EWJC, EJCT	Y	EWJC
EWJC	ENTER WANTED JUVENILE CAUTION	W2/WACIC	NCIC		Y	
EJCT	ENTER WANTED JUVENILE TEST	W2/WACIC	ACCESS	EWJC		
EWJC	ENTER WANTED JUVENILE TEST	ACCESS	NCIC TEST		Y	
EWJ	ENTER WANTED MISDEMEANOR (IF TYPE MN)	Agency	W2/WACIC	EW	Y	EWJ
EW	ENTER WANTED PERSON	W2/WACIC	NCIC		Y	
EWJ	ENTER WANTED MISDEMEANOR (IF TYPE MS)	Agency	W2/WACIC		Y	EWJ
EWWC	ENTER WANTED MISDEMEANOR – CAUTION	Agency	W2/WACIC	EW-C	Y	EWWC
EW-C	ENTER WANTED MISDEMEANOR – CAUTION	W2/WACIC	NCIC		Y	
EXS	ENTER SEX OFFENDER	W2/WACIC	NCIC	EXS, EXST	Y	EXS
EXST	ENTER SEX OFFENDER TEST	W2/WACIC	ACCESS	EXS	Y	
G	GUN INQUIRY	Agency	W2/WACIC	QG	Y	G
QG	GUN INQUIRY	W2/WACIC	NCIC		Y	
LAA	LOCATE ARTICLE GROUP	Agency	ACCESS	LASA, LAAT		LAA
LASA	LOCATE ARTICLE GROUP	ACCESS	W2/WACIC	LAA	Y	
LAA	LOCATE ARTICLE GROUP	W2/WACIC	NCIC		Y	
LAAT	LOCATE ARTICLE GROUP	W2/WACIC	ACCESS	LAA	Y	
LAS	LOCATE STOLEN ARTICLE	Agency	W2/WACIC	LA	Y	LAS
LA	LOCATE STOLEN ARTICLE	W2/WACIC	NCIC		Y	
LBS	LOCATE STOLEN BOAT	Agency	NCIC	LB	Y	LBS

TRANSACTION ID	LITERAL	FROM	TO	CREATES	RESPONSE EXPECTED	STARTING
LSM	LOCATE SINGLE SECURITY	Agency	NCIC	LS	Y	LSM
LSSM	LOCATE GROUP SECURITY	Agency	NCIC	LSS	Y	LSSM
LGF	LOCATE GUN FELONY	Agency	W2/WACIC	LFG, LFGT	Y	LGF
LFG	LOCATE GUN FELONY	W2/WACIC	NCIC		Y	
LFGT	LOCATE GUN FELONY TEST	W2/WACIC	ACCESS	LFG LLG, LLGT	Y	
LGM	LOCATE MISSING GUN	Agency	W2/WACIC	LLGT	Y	LGM
LLG	LOCATE LOST GUN	W2/WACIC	NCIC		Y	
LLGT	LOCATE LOST GUN TEST	W2/WACIC	ACCESS	LLG	Y	
LGS	LOCATE STOLEN GUN	Agency	W2/WACIC	LG, LGT	Y	LGS
LG	LOCATE STOLEN GUN	W2/WACIC	NCIC		Y	
LGT	LOCATE STOLEN GUN TEST	W2/WACIC	ACCESS	LG	Y	
LLS	LOCATE STOLEN LICENSE PLATE	Agency	W2/WACIC	LL, LLT	Y	LLS
LL	LOCATE STOLEN LICENSE PLATE	W2/WACIC	NCIC		Y	
LLT	TEST	W2/WACIC	ACCESS	LL	Y	
LM	LOCATE MISSING PERSON	Agency	W2/WACIC	LM, LMT	Y	LM
LM	LOCATE MISSING PERSON	W2/WACIC	NCIC		Y	
LMT	LOCATE MISSING PERSON TEST	W2/WACIC	ACCESS	LM		
LM	LOCATE MISSING PERSON TEST	ACCESS	NCIC TEST		Y	
LPS	LOCATE STOLEN PART	Agency	W2/WACIC	LP, LPT	Y	LPS
LP	LOCATE STOLEN PART	W2/WACIC	NCIC		Y	
LPT	LOCATE STOLEN PART TEST	W2/WACIC	ACCESS	LP		
LP	LOCATE STOLEN PART TEST	ACCESS	NCIC TEST		Y	
LTF	LOCATE TEMPORARY FELONY WANT	Agency	W2/WACIC	LT, LTT	Y	LTF
LT	LOCATE TEMPORARY FELONY WANT	W2/WACIC	NCIC		Y	
LTT	TEST	W2/WACIC	ACCESS	LT		
LT	LOCATE TEMPORARY FELONY WANT TEST	ACCESS	NCIC TEST		Y	
LVS	LOCATE STOLEN VEHICLE	Agency	W2/WACIC	LV, LVS, LVT	Y	LVS
LVS	LOCATE STOLEN VEHICLE	W2/WACIC	DOL		N	
LV	LOCATE STOLEN VEHICLE	W2/WACIC	NCIC		Y	
LE	LOJACK	ACCESS	NLETS		N	
LVT	LOCATE STOLEN VEHICLE TEST	W2/WACIC	ACCESS	LV		

TRANSACTION ID	LITERAL	FROM	TO	CREATES	RESPONSE EXPECTED	STARTING
LV	LOCATE STOLEN VEHICLE TEST	ACCESS	NCIC TEST		Y	
LVW	LOCATE WANTED FELONY VEHICLE	Agency	W2/WACIC	LF, LFT	Y	LVW
LF	LOCATE WANTED FELONY VEHICLE	W2/WACIC	NCIC		Y	
	LOCATE WANTED FELONY VEHICLE					
LFT	TEST	W2/WACIC	ACCESS	LF		
	LOCATE WANTED FELONY VEHICLE					
LF	TEST	ACCESS	NCIC TEST		Y	
LWF	LOCATE WANTED FELONY	Agency	W2/WACIC	LW, LWT	Y	LWF
LW	LOCATE WANTED PERSON	W2/WACIC	NCIC		Y	
LWT	LOCATE WANTED PERSON TEST	W2/WACIC	ACCESS	LW		
LW	LOCATE WANTED PERSON TEST	ACCESS	NCIC TEST		Y	
LWJ	LOCATE WANTED JUVENILE	Agency	W2/WACIC	LW	Y	LWJ
LW	LOCATE WANTED PERSON	W2/WACIC	NCIC		Y	
	LOCATE WANTED MISDEMEANOR (IF					
LWW	TYPE MN)	Agency	W2/WACIC	LW	Y	LWW
LW	LOCATE WANTED PERSON	W2/WACIC	NCIC		Y	
	LOCATE WANTED MISDEMEANOR (IF					
LWW	TYPE MS)	Agency	W2/WACIC		Y	LWW
MAA	MODIFY ARTICLE GROUP	Agency	ACCESS	MASA, MAAT	N	MAA
MASA	MODIFY ARTICLE GROUP	ACCESS	W2/WACIC	MAA	Y	
MAA	MODIFY ARTICLE GROUP	W2/WACIC	NCIC		Y	
MAAT	MODIFY ARTICLE GROUP TEST	W2/WACIC	ACCESS	MAA	Y	
MAS	MODIFY STOLEN ARTICLE	Agency	W2/WACIC	MA, MAT	Y	MAS
MA	MODIFY STOLEN ARTICLE	W2/WACIC	NCIC		Y	
MAT	MODIFY STOLEN ARTICLE TEST	W2/WACIC	ACCESS	MA	Y	
MAP	MODIFY PAWNED ARTICLE	Agency	W2/WACIC		Y	
MAR	MODIFY RECOVERED ARTICLE	Agency	W2/WACIC		Y	
MBS	MODIFY STOLEN BOAT	Agency	ACCESS	MB		MBS
MB	MODIFY STOLEN BOAT	ACCESS	NCIC		Y	
MCOC	MODIFY CORRECTIONS CONDITIONS	Agency	W2/WACIC		Y	
MGG	MODIFY GANG/TERRORIST ORG	Agency	NCIC		Y	
MGGM	MODIFY GANG MEMBER	Agency	NCIC	MGM	Y	MGGM
MGP	MODIFY PAWNED GUN	Agency	W2/WACIC		Y	
				MRG, MRGT		
MGR	MODIFY RECOVERED GUN	Agency	W2/WACIC		Y	MRG
MRG	MODIFY RECOVERED GUN	W2/WACIC	NCIC		Y	

TRANSACTION ID	LITERAL	FROM	TO	CREATES	RESPONSE EXPECTED	STARTING
MRGT	MODIFY RECOVERED GUN TEST	W2/WACIC	ACCESS	MRG	Y	
MIP	MODIFY PERSON OF INTEREST	Agency	W2/WACIC		Y	
MPP	MODIFY PAWNED PART	Agency	W2/WACIC		Y	
MPR	MODIFY RECOVERED PART	Agency	W2/WACIC		Y	
MSM	MODIFY SINGLE SECURITY	Agency	NCIC	MS	Y	MSM
MSSM	MODIFY GROUP SECURITY	Agency	NCIC	MSS	Y	MSSM
MVI	MODIFY IMPOUNDED VEHICLE	Agency	W2/WACIC	NUI	Y	
NUI	MODIFY IMPOUNDED VEHICLE	W2/WACIC	NLETS	NUA	Y	
NUA	MODIFY IMPOUNDED VEHICLE RESPONSE	NLETS	Agency		Y	
MCO	MODIFY SUPERVISED PERSON	Agency	W2/WACIC	MC, MCT	Y	MCO
MC	MODIFY SUPERVISED PERSON	W2/WACIC	NCIC		Y	
MCT	MODIFY SUPERVISED PERSON TEST	W2/WACIC	ACCESS	MC		
MC	MODIFY SUPERVISED PERSON TEST	ACCESS	NCIC TEST		Y	
MDD	MODIFY DENTAL DATA	Agency	W2/WACIC	MD, MDT	Y	MDD
MD	MODIFY DENTAL DATA	W2/WACIC	NCIC		Y	
MDT	MODIFY DENTAL DATA TEST	W2/WACIC	ACCESS	MD		
MD	MODIFY DENTAL DATA TEST	ACCESS	NCIC TEST		Y	
MDP	MODIFY DENIED PERSON	Agency	NCIC		Y	
MGF	MODIFY GUN FELONY	Agency	W2/WACIC	MFG, MFGT	Y	MGF
MFG	MODIFY GUN FELONY	W2/WACIC	NCIC		Y	
MFGT	MODIFY GUN FELONY TEST	W2/WACIC	ACCESS	MFG MLG, MLGT	Y	
MGM	MODIFY MISSING GUN	Agency	W2/WACIC	MLGT	Y	MLG
MLG	MODIFY MISSING GUN	W2/WACIC	NCIC		Y	
MLGT	MODIFY MISSING GUN TEST	W2/WACIC	ACCESS	MLG	Y	
MGS	MODIFY STOLEN GUN	Agency	W2/WACIC	MG, MGT	Y	MGS
MG	MODIFY STOLEN GUN	W2/WACIC	NCIC		Y	
MGT	MODIFY STOLEN GUN TEST	W2/WACIC	ACCESS	MG	Y	
MII	IMAGE MODIFY	Agency	W2/WACIC	MII, MIIT	Y	MII
MII	IMAGE MODIFY	W2/WACIC	NCIC		Y	
MIIT	IMAGE MODIFY TEST	W2/WACIC	ACCESS	MII MID, MIDT	Y	
MIT	MODIFY ID THEFT VICTIM	Agency	W2/WACIC	MIDT	Y	MIT
MID	MODIFY ID THEFT VICTIM	W2/WACIC	NCIC		Y	

TRANSACTION ID	LITERAL	FROM	TO	CREATES	RESPONSE EXPECTED	STARTING
MIDT	MODIFY ID THEFT VICTIM TEST	W2/WACIC	ACCESS	MID		
MID	MODIFY ID THEFT VICTIM TEST	ACCESS	NCIC TEST		Y	
MLS	MODIFY STOLEN LICENSE PLATE	Agency	W2/WACIC	ML, MLT	Y	MLS
ML	MODIFY STOLEN LICENSE PLATE	W2/WACIC	NCIC		Y	
	MODIFY STOLEN LICENSE PLATE					
MLT	TEST	W2/WACIC	ACCESS	ML	Y	
MM	MODIFY MISSING PERSON	Agency	W2/WACIC	MMT	Y	MM
MM	MODIFY MISSING PERSON	W2/WACIC	NCIC		Y	
MMT	MODIFY MISSING PERSON TEST	W2/WACIC	ACCESS	MM		
MM	MODIFY MISSING PERSON TEST	ACCESS	NCIC TEST		Y	
MPO	MODIFY PROTECTION ORDER	Agency	W2/WACIC	MPOT	Y	MPO
MPO	MODIFY PROTECTION ORDER	W2/WACIC	NCIC		Y	
MPOT	MODIFY PROTECTION ORDER TEST	W2/WACIC	ACCESS	MPO		
MPO	MODIFY PROTECTION ORDER TEST	ACCESS	NCIC TEST		Y	
	MODIFY TEMPORARY PROTECTION			MTOT		
MPO	ORDER	Agency	W2/WACIC	MTOT	Y	
	MODIFY TEMPORARY PROTECTION					
MTO	ORDER	W2/WACIC	NCIC		Y	
	MODIFY TEMPORARY PROTECTION					
MTOT	ORDER TEST	W2/WACIC	ACCESS	MTO		
	MODIFY TEMPORARY PROTECTION					
MTO	ORDER TEST	ACCESS	NCIC TEST		Y	
MPS	MODIFY STOLEN PART	Agency	W2/WACIC	MP, MPT	Y	MPS
MP	MODIFY STOLEN PART	W2/WACIC	NCIC		Y	
MPT	MODIFY STOLEN PART TEST	W2/WACIC	ACCESS	MP	Y	
MXS	MODIFY SEX/KIDNAPPING OFFENDER	W2/WACIC	NCIC	MXST	Y	MXS
	MODIFY SEX/KIDNAPPING OFFENDER					
MXST	TEST	W2/WACIC	ACCESS		Y	
MTF	MODIFY TEMPORARY FELONY WANT	Agency	W2/WACIC	MT, MTT	Y	MTF
MT	MODIFY TEMPORARY FELONY WANT	W2/WACIC	NCIC		Y	
	MODIFY TEMPORARY FELONY WANT					
MTT	TEST	W2/WACIC	ACCESS	MT		
	MODIFY TEMPORARY FELONY WANT					
MT	TEST	ACCESS	NCIC TEST		Y	
MU	MODIFY UNIDENTIFIED PERSON	Agency	W2/WACIC	MUT	Y	MU
MU	MODIFY UNIDENTIFIED PERSON	W2/WACIC	NCIC		Y	
MUT	MODIFY UNIDENTIFIED PERSON TEST	W2/WACIC	ACCESS	MU		

TRANSACTION ID	LITERAL	FROM	TO	CREATES	RESPONSE EXPECTED	STARTING
MU	MODIFY UNIDENTIFIED PERSON TEST	ACCESS	NCIC TEST		Y	
MVS	MODIFY VEHICLE STOLEN	Agency	W2/WACIC	MV, MVS, MVT	Y	MVS
LE	LOJACK	ACCESS	NLETS		Y	
MVS	MODIFY VEHICLE STOLEN	W2/WACIC	DOL		N	MVS
MV	MODIFY VEHICLE STOLEN	W2/WACIC	NCIC		Y	
MVT	MODIFY VEHICLE STOLEN TEST	W2/WACIC	ACCESS	MV	Y	
MV	MODIFY VEHICLE STOLEN TEST	ACCESS	NCIC TEST		Y	
MVW	MODIFY WANTED FELONY VEHICLE	Agency	W2/WACIC	MF, MFT	Y	MVW
MF	MODIFY WANTED FELONY VEHICLE	W2/WACIC	NCIC		Y	
MFT	MODIFY WANTED FELONY VEHICLE TEST	W2/WACIC	ACCESS	MF		
MF	MODIFY WANTED FELONY VEHICLE TEST	ACCESS	NCIC TEST		Y	
MWF	MODIFY WANTED FELONY	Agency	W2/WACIC	MW, MWT	Y	MWF
MW	MODIFY WANTED FELONY	W2/WACIC	NCIC		Y	
MWT	MODIFY WANTED FELONY TEST	W2/WACIC	ACCESS	MW		
MW	MODIFY WANTED FELONY TEST	ACCESS	NCIC TEST		Y	
MWJ	MODIFY WANTED JUVENILE	Agency	W2/WACIC	MW	Y	MWJ
MW	MODIFY WANTED JUVENILE	W2/WACIC	NCIC		Y	
MWW	MODIFY WANTED MISDEMEANOR (IF TYPE MN)	Agency	W2/WACIC	MW	Y	MWW
MW	MODIFY WANTED MODIFY WANTED MISDEMEANOR (IF TYPE MS)	W2/WACIC	NCIC		Y	
MWW	MODIFY WANTED MISDEMEANOR (IF TYPE MS)	Agency	W2/WACIC		Y	MWW
MVIP	MODIFY PRIVATE IMPOUND	Agency	W2/WACIC		Y	
MVR	MODIFY REPOSSESSED VEHICLE	Agency	W2/WACIC		Y	
MYV	WATCH YOUR CAR MODIFY	Agency	W2/WACIC		Y	
NLN	NICS DELAY MESSAGE	Agency	NCIC		Y	
NDN	NICS DENIED MESSAGE	Agency	NCIC		Y	
NDO	NICS DENIAL OVERTURN	Agency	NCIC		Y	
NPN	NICS PROCEED MESSAGE	Agency	NCIC		Y	
ORIMAIN	ENTER ORI INFORMATION	Admin		EORI, EAF		
EORI	ENTER ORI INFORMATION	Terminal	ACCESS		Y	
EAF	ENTER ORI INFORMATION	ACCESS	W2/WACIC		Y	
		ACCESS	W2/WACIC		Y	

TRANSACTION ID	LITERAL	FROM	TO	CREATES	RESPONSE EXPECTED	STARTING
ORIMAIN	MODIFY ORI INFORMATION	Admin		MORI, MAF, MO, TU	Y	
MORI	MODIFY ORI INFORMATION	Terminal	ACCESS		Y	
MAF	MODIFY ORI INFORMATION	ACCESS	W2/WACIC		Y	
MO	MODIFY ORI INFORMATION	ACCESS	W2/WACIC		Y	
TU	MODIFY ORI INFORMATION	ACCESS	NCIC		Y	
		ACCESS	NLETS		Y	
ORIMAIN	DELETE ORI INFORMATION	Admin		XORI, XAF	Y	
XORI	DELETE ORI INFORMATION	Terminal	ACCESS		Y	
XAF	DELETE ORI INFORMATION	ACCESS	W2/WACIC		Y	
				MORI, MAF, MO, TU		
ORIUPDT	MODIFY ORI INFORMATION	Agency	ACCESS		Y	
MORI	MODIFY ORI INFORMATION	ACCESS	W2/WACIC		Y	
MAF	MODIFY ORI INFORMATION	ACCESS	W2/WACIC		Y	
MO	MODIFY ORI INFORMATION	ACCESS	NCIC		Y	
TU	MODIFY ORI INFORMATION	ACCESS	NLETS		Y	
MO	MODIFY NCIC ORI	ACCESS			Y	
A	ARTICLE INQUIRY	Agency	NCIC		Y	
QA	ARTICLE INQUIRY	Agency	ACCESS	QA	Y	A
QA	ARTICLE INQUIRY	W2/WACIC	NCIC		Y	
	ARTICLE INQUIRY	Agency	W2/WACIC	QA	Y	
	ARTICLE INQUIRY	W2/WACIC	NCIC		Y	
B	BOAT INQUIRY	Agency	ACCESS	QB		
QB	BOAT INQUIRY	ACCESS	NCIC		Y	
QB	BOAT INQUIRY	Agency	NCIC	QB	Y	
QDD	DENTAL INFO INQUIRY	Agency	ACCESS	QD	Y	
QD	DENTAL INFO INQUIRY	Agency	W2/WACIC		Y	
QDNA	WASIS DNA INQUIRY	W2/WACIC	NCIC		Y	
QDP	WASIS DNA INQUIRY	Agency	W2/WACIC		Y	
QAF	NICS QUERY STATE INDEX	Agency	NCIC		Y	
QGG	WACIC AGENCY FUNCTION INQUIRY	Agency	W2/WACIC		Y	
QGM	GANG INQUIRY	Agency	NCIC		Y	
QI	QUERY GANG MEMBER	Agency	NCIC		Y	
QID	CRIMINAL HISTORY INQUIRY	Agency	W2/WACIC		Y	
QNR	VIN INSPECTION DATA INQUIRY	Agency	W2/WACIC		Y	
	NICS QUERY BY SID #	Agency	W2/WACIC		Y	

TRANSACTION ID	LITERAL	FROM	TO	CREATES	RESPONSE EXPECTED	STARTING
QO	NCIC ORI INQUIRY	Agency	NCIC		Y	
QORI	WACIC ORI INQUIRY	Agency	W2/WACIC		Y	
QS	SECURITY INQUIRY	Agency	NCIC		Y	
QVC	VIN VALIDITY INQUIRY	Agency	W2/WACIC		Y	
QX	HOT SHEET INQUIRY	Agency	W2/WACIC		Y	
QYV	WATCH YOUR CAR INQUIRY	Agency	W2/WACIC		Y	
G	GUN INQUIRY	Agency	ACCESS	QG		
QG	GUN INQUIRY	ACCESS	W2/WACIC		Y	
QH	III INQUIRY	Agency	ACCESS			
		ACCESS	W2/WACIC		Y	
		ACCESS	NCC		Y	
QII	QUERY IMAGE	Agency	W2/WACIC		Y	
		W2/WACIC	NCIC		Y	
QIT	QUERY ID THEFT VICTIM	Agency	W2/WACIC	QID	Y	
QID	QUERY ID THEFT VICTIM	W2/WACIC	NCIC		Y	
QM	MISSING PERSON INQUIRY	Agency	W2/WACIC		Y	
		W2/WACIC	NCIC		Y	
QM	MISSING PERSON INQUIRY(NON UNIQUE IDENTIFIER)	Agency	ACCESS			
		ACCESS	NCIC		Y	
QN	NICS INQUIRY (NAM/DOB)	Agency	W2/WACIC		Y	
		W2/WACIC	NCIC		Y	
QNR	NICS INQUIRY	Agency	W2/WACIC		Y	
		W2/WACIC	NCIC		Y	
QPO	PROTECTION ORDER INQUIRY	Agency	W2/WACIC		Y	
		W2/WACIC	NCIC		Y	
QR	CRIMINAL HISTORY INQUIRY	Agency	W2/WACIC		Y	
		W2/WACIC	NCIC		Y	
QU	UNIDENTIFIED INQUIRY	Agency	W2/WACIC		Y	
		W2/WACIC	NCIC		Y	
QU	UNIDENTIFIED INQUIRY (NON UNIQUE IDENTIFIER)	Agency	ACCESS			
		ACCESS	NCIC		Y	
QUD	DENTAL INFO INQUIRY	Agency	W2/WACIC		Y	
		W2/WACIC	NCIC		Y	
V	VEHICLE INQUIRY	Agency	ACCESS	QV	Y	V

TRANSACTION ID	LITERAL	FROM	TO	CREATES	RESPONSE EXPECTED	STARTING
QV	VEHICLE INQUIRY	ACCESS	W2/WACIC		Y	
		W2/WACIC	NCIC		Y	
W	WANTED PERSON INQUIRY	Agency	ACCESS	QW		W
QW	WANTED PERSON INQUIRY	ACCESS	W2/WACIC		Y	
		W2/WACIC	NCIC		Y	
QWH	WANTED/CHRI INQUIRY	Agency	W2/WACIC	QW, QH	Y	QWH
QW	WANTED PERSON	W2/WACIC	NCIC		Y	
QH	QUERY CRIM HISTORY	W2/WACIC	NCIC		Y	
QWO	WANTED ONLY INQUIRY	Agency	W2/WACIC	QW	Y	QWO
		W2/WACIC	NCIC		Y	
QXS	SEX OFFENDER INQUIRY	Agency	NCIC		Y	
				V, QV, NAQ,		
RNV	WACIC/NCIC/DOL/NICB INQUIRY	Agency	ACCESS		Y	RNV
V	DOL VEH INQUIRY	ACCESS	DOL		Y	
QV	WACIC VEH INQUIRY	ACCESS	W2/WACIC		Y	
QV	WACIC VEH INQUIRY	ACCESS	NCIC		Y	
NAQ	NLETS NICB INQUIRY	ACCESS	NLETS	NAR	Y	
NAR	NLETS NICB INQUIRY RESPONSE	NLETS	Agency			
RV	DOL VIN/LICENSE INQUIRY	Agency	ACCESS	L, V, QV,		RV
L	DOL LICENSE	ACCESS	DOL		Y	
V	DOL VIN	ACCESS	DOL		Y	
QV	QUERY VEHICLE	ACCESS	W2/WACIC		Y	
QV	QUERY VEHICLE	ACCESS	NCIC		Y	
S	SECURITY INQUIRY	Agency	NCIC	QS	Y	S
QS	SECURITY INQUIRY	Agency	NCIC		Y	
	NICS ADD SUPP DATA TO DENIED					
SDP	PERSON	Agency	NCIC		Y	
SPO	NOTICE OF SERVICE	Agency	W2/WACIC		Y	
SWQ	NLETS STATE WARRANT QUERY	NLETS	ACCESS	QWO	Y	SWQ
QWO	WACIC WARRANT ONLY QUERY	ACCESS	W2/WACIC		Y	
	WACIC WARRANT ONLY QUERY	W2/WACIC	ACCESS	SWR	N	
SWR	NLETS WARRANT QUERY RESPONSE	ACCESS	NLETS		Y	
UV	QUERY VEHICLE BY PARTIAL VIN	Agency	W2/WACIC		Y	
W	WANTED PERSON INQUIRY	Agency	ACCESS	QW		W
QW	WANTED PERSON INQUIRY	ACCESS	W2/WACIC		Y	
		W2/WACIC	NCIC			

TRANSACTION ID	LITERAL	FROM	TO	CREATES	RESPONSE EXPECTED	STARTING
XAA	CANCEL ARTICLE GROUP	Agency	ACCESS	XASA, XAAT		XAA
XASA	CANCEL ARTICLE GROUP	ACCESS	W2/WACIC	XAA	Y	
XAA	CANCEL ARTICLE GROUP	W2/WACIC	NCIC		Y	
XAAT	CANCEL ARTICLE GROUP TEST	W2/WACIC	ACCESS	XAA	Y	
XAS	CANCEL STOLEN ARTICLE	Agency	W2/WACIC	XA, XAT	Y	XA
XA	CANCEL STOLEN ARTICLE	W2/WACIC	NCIC		Y	
XAT	CANCEL STOLEN ARTICLE TEST	W2/WACIC	ACCESS	XA	Y	
XCO	CANCEL SUPERVISED PERSON	Agency	W2/WACIC	XC, XCT	Y	XCO
XC	CANCEL SUPERVISED PERSON	W2/WACIC	NCIC		Y	
XCT	CANCEL SUPERVISED PERSON TEST	W2/WACIC	ACCESS	XC		
XC	CANCEL SUPERVISED PERSON TEST	ACCESS	NCIC TEST		Y	
XDD	CANCEL DENTAL DATA	Agency	W2/WACIC	XD, XDT	Y	XDD
XD	CANCEL DENTAL DATA	W2/WACIC	NCIC		Y	
XDT	CANCEL DENTAL DATA TEST	W2/WACIC	ACCESS	XD	Y	
XDW	CANCEL DETAINER FILE	Agency	W2/WACIC	XDWT	Y	
XDW	CANCEL DETAINER FILE	W2/WACIC	NCIC		Y	
XDWT	CANCEL DETAINER FILE TEST	W2/WACIC	ACCESS	XDW	Y	
XDW	CANCEL DETAINER FILE TEST	ACCESS	NCICTEST		Y	
XDP	CANCEL STATE INDEX NICS	Agency	NCIC		Y	
XGF	CANCEL GUN FELONY	Agency	W2/WACIC	XFG, XFGT	Y	XGF
XFG	CANCEL GUN FELONY	W2/WACIC	NCIC		Y	
XFGT	CANCEL GUN FELONY TEST	W2/WACIC	ACCESS		Y	
XGM	CANCEL MISSING GUN	Agency	W2/WACIC	XLG, XLGT	Y	XGM
XLG	CANCEL MISSING GUN	W2/WACIC	NCIC		Y	
XLGT	CANCEL MISSING GUN TEST	W2/WACIC	ACCESS	XLG	Y	
XGS	CANCEL STOLEN GUN	Agency	W2/WACIC	XG, XGT	Y	XGS
XG	CANCEL STOLEN GUN	W2/WACIC	NCIC		Y	
XGT	CANCEL STOLEN GUN TEST	W2/WACIC	ACCESS	XG	Y	
XIM	IMAGE CANCEL	Agency	W2/WACIC		Y	
XIM	IMAGE CANCEL	W2/WACIC	NCIC		Y	
XIT	CANCEL ID THEFT VICTIM	Agency	W2/WACIC	XID, XIDT	Y	XIT
XID	CANCEL ID THEFT VICTIM	W2/WACIC	NCIC		Y	
XIDT	CANCEL ID THEFT VICTIM TEST	W2/WACIC	ACCESS	XID		

TRANSACTION ID	LITERAL	FROM	TO	CREATES	RESPONSE EXPECTED	STARTING
XID	CANCEL ID THEFT VICTIM TEST	ACCESS	NCIC TEST		Y	
XN	CANCEL ID THEFT VICTIM SUPP DATA	Agency	W2/WACIC	XIN, XINT	Y	XN
XIN	CANCEL ID THEFT VICTIM SUPP DATA	W2/WACIC	NCIC		Y	
XINT	CANCEL ID THEFT VICTIM SUPP DATA TEST	W2/WACIC	ACCESS	XIN		
XIN	CANCEL ID THEFT VICTIM SUPP DATA TEST	ACCESS	NCIC TEST		Y	
XLS	CANCEL STOLEN LICENSE PLATE	Agency	W2/WACIC	XL, XLT	Y	XLS
XL	CANCEL STOLEN LICENSE PLATE	W2/WACIC	NCIC		Y	
XLT	CANCEL STOLEN LICENSE PLATE TEST	W2/WACIC	ACCESS	XL	Y	
XM	CANCEL MISSING PERSON	Agency	W2/WACIC	XMT	Y	
XM	CANCEL MISSING PERSON	W2/WACIC	NCIC		Y	
XMT	CANCEL MISSING PERSON TEST	W2/WACIC	ACCESS	XM	Y	
XM	CANCEL MISSING PERSON TEST	ACCESS	NCIC TEST		Y	
XMN	CANCEL MISSING SUPP DATA	Agency	W2/WACIC	XMNT	Y	
XMN	CANCEL MISSING SUPP DATA	W2/WACIC	NCIC		Y	
XMNT	CANCEL MISSING SUPP DATA TEST	W2/WACIC	ACCESS	XMN		
XMN	CANCEL MISSING SUPP DATA TEST	ACCESS	NCIC TEST		Y	
XN	CANCEL SUPPLEMENTAL DATA	Agency	W2/WACIC	XNT	Y	
XN	CANCEL SUPPLEMENTAL DATA	W2/WACIC	NCIC		Y	
XNT	CANCEL SUPPLEMENTAL DATA TEST	W2/WACIC	ACCESS	XNT	Y	
XN	CANCEL SUPP PER SUPPLEMENTAL DATA	Agency	W2/WACIC	XCNT	Y	
XCNT	CANCEL SUPP PER SUPPLEMENTAL DATA	W2/WACIC	NCIC		Y	
XCNT	CANCEL SUPP PER SUPPLEMENTAL DATA TEST	W2/WACIC	ACCESS	XCNT	Y	
XNS	CANCEL SUPPLEMENTAL S/FDATA	Agency	W2/WACIC	XNST	Y	
XNS	CANCEL SUPPLEMENTAL S/FDATA	W2/WACIC	NCIC		Y	
XNST	CANCEL SUPPLEMENTAL S/FDATA TEST	W2/WACIC	ACCESS	XNS	Y	
XNS	CANCEL SUPP SUPERVISED PERSON S/FDATA	Agency	W2/WACIC	XCNS, XCST	Y	
XCNS	CANCEL SUPP SUPERVISED PERSON S/FDATA	W2/WACIC	NCIC		Y	

TRANSACTION ID	LITERAL	FROM	TO	CREATES	RESPONSE EXPECTED	STARTING
XCST	CANCEL SUPP SUPERV PERSON S/FDATA TEST	W2/WACIC	ACCESS	XCNS XPO, XPOT	Y	
XPO	CANCEL RESTRAINING ORDER	Agency	W2/WACIC		Y	
XPO	CANCEL RESTRAINING ORDER	W2/WACIC	NCIC		Y	
XPOT	CANCEL RESTRAINING ORDER TEST	W2/WACIC	ACCESS	XPO	Y	
XPO	CANCEL RESTRAINING ORDER TEST	ACCESS	NCIC TEST		Y	
XPS	CANCEL STOLEN PART	Agency	W2/WACIC	XP, XPT	Y	XPS
XP	CANCEL STOLEN PART	W2/WACIC	NCIC		Y	
XPT	CANCEL STOLEN PART TEST	W2/WACIC	ACCESS	XP	Y	
XTF	CANCEL TEMPORARY FELONY WANT	Agency	W2/WACIC	XT, XTT	Y	XTF
XT	CANCEL TEMPORARY FELONY WANT	W2/WACIC	NCIC		Y	
	CANCEL TEMPORARY FELONY WANT					
XTT	TEST	W2/WACIC	ACCESS	XT		
	CANCEL TEMPORARY FELONY WANT					
XT	TEST	ACCESS	NCIC TEST		Y	
XU	CANCEL UNIDENTIFIED PERSON	Agency	W2/WACIC	XUT	Y	
XU	CANCEL UNIDENTIFIED PERSON	W2/WACIC	NCIC		Y	
	CANCEL UNIDENTIFIED PERSON					
XUT	TEST	W2/WACIC	ACCESS	XU		
	CANCEL UNIDENTIFIED PERSON					
XU	TEST	ACCESS	NCIC TEST		Y	
XUN	CANCEL UNIDENT PERS SUPP DATA	Agency	W2/WACIC	XUNT	Y	
XUN	CANCEL UNIDENT PERS SUPP DATA	W2/WACIC	NCIC		Y	
	CANCEL UNIDENT PERS SUPP DATA					
XUNT	TEST	W2/WACIC	ACCESS	XUN		
	CANCEL UNIDENT PERS SUPP DATA					
XUN	TEST	ACCESS	NCIC TEST		Y	
XVI	CANCEL IMPOUND VEHICLE (POLICE)	Agency	W2/WACIC	NCI	Y	XVI
NCI	CANCEL IMPOUND VEHICLE	W2/WACIC	ACCESS			
NCI	NICB CANCEL IMPOUND VEHICLE	ACCESS	NLETS	NCA	Y	
NCA	NICB CANCEL IMPOUND VEHICLE	NLETS	Agency		Y	
	CANCEL IMPOUND VEHICLE					
XVIP	(PRIVATE)	Agency	W2/WACIC		Y	
XVS	CANCEL STOLEN VEHICLE	Agency	W2/WACIC	XV, XVS, XVT	Y	XVS
			ACCESS	LE	N	

TRANSACTION ID	LITERAL	FROM	TO	CREATES	RESPONSE EXPECTED	STARTING
LE	LOJACK	ACCESS	NLETS		Y	
XVS	CANCEL STOLEN VEHICLE	W2/WACIC	DOL		N	
XV	CANCEL STOLEN VEHICLE	W2/WACIC	NCIC		Y	
XVT	CANCEL STOLEN VEHICLE TEST	W2/WACIC	ACCESS	XV		
XV	CANCEL STOLEN VEHICLE TEST	ACCESS	NCIC TEST		Y	
XVW	CANCEL WANTED FELONY VEHICLE	Agency	W2/WACIC	XF, XFT	Y	XVW
XF	CANCEL WANTED FELONY VEHICLE	W2/WACIC	NCIC		Y	
XFT	CANCEL WANTED FELONY VEHICLE TEST	W2/WACIC	ACCESS	XF		
XF	CANCEL WANTED FELONY VEHICLE TEST	ACCESS	NCIC TEST		Y	
XWF	CANCEL WANTED FELONY	Agency	W2/WACIC	XW, XWT	Y	XWF
XW	CANCEL WANTED FELONY	W2/WACIC	NCIC		Y	
XWT	CANCEL WANTED FELONY TEST	W2/WACIC	ACCESS	XW		
XW	CANCEL WANTED FELONY TEST	ACCESS	NCIC TEST		Y	
XWJ	CANCEL WANTED JUVENILE	Agency	W2/WACIC	XW	Y	XWJ
XW	CANCEL WANTED PERSON	W2/WACIC	NCIC		Y	
XWW	CANCEL WANTED MISDEMEANOR (IF TYPE MN)	Agency	W2/WACIC	XW	Y	XWW
XW	CANCEL WANTED PERSON	W2/WACIC	NCIC		Y	
XWW	CANCEL WANTED MISDEMEANOR (IF TYPE MS)	Agency	W2/WACIC		Y	XWW
XAP	CANCEL PAWNED ARTICLE	Agency	W2/WACIC		Y	
XAR	CANCEL RECOVERED ARTICLE	Agency	W2/WACIC		Y	
XBS	CANCEL STOLEN BOAT	Agency	ACCESS	XB		XBS
XB	CANCEL STOLEN BOAT	ACCESS	NCIC		Y	
XGG	CANCEL GANG/TERRORIST ORG	Agency	NCIC		Y	
XGGM	CANCEL GANG MEMBER	Agency	ACCESS	XGM	Y	XGGM
XGM	CANCEL GANG MEMBER	ACCESS	NCIC			
XGGN	CANCEL GANG SUPPLEMENTAL DATA	Agency	NCIC		Y	
XGMN	CANCEL GANG MEMBER SUPP DATA	Agency	NCIC		Y	
XGP	CANCEL PAWNED GUN	Agency	W2/WACIC		Y	
XGR	CANCEL RECOVERED GUN	Agency	W2/WACIC		Y	
XID	CANCEL VIN INSPECTION DATA	Agency	W2/WACIC		Y	
XIP	CANCEL PERSON OF INTEREST	Agency	W2/WACIC		Y	
XPP	CANCEL PAWNED PART	Agency	W2/WACIC		Y	

TRANSACTION ID	LITERAL	FROM	TO	CREATES	RESPONSE EXPECTED	STARTING
XPR	CANCEL RECOVERED PART	Agency	W2/WACIC		Y	
XSM	CANCEL SINGLE SECURITY	Agency	ACCESS	XS		XSM
XS	CANCEL SINGLE SECURITY	ACCESS	NCIC		Y	
XSSM	CANCEL GROUP SECURITY	Agency	ACCESS	XSS		XSSM
XSS	CANCEL GROUP SECURITY	ACCESS	NCIC		Y	
XVPQ	CANCEL QUESTIONABLE VIN	Agency	W2/WACIC		Y	
XVR	CANCEL REPOSSESSED VEHICLE	Agency	W2/WACIC		Y	
XYN	WATCH YOUR CAR SUP CANCEL	Agency	W2/WACIC		Y	
XYV	WATCH YOUR CAR CANCEL	Agency	W2/WACIC		Y	
XXS	CANCEL SEX OFFENDER	W2/WACIC	NCIC	XXST	Y	
XXST	CANCEL SEX OFFENDER TEST	W2/WACIC	ACCESS	XXS		
ZO	NCIC ORI INQUIRY	Agency	NCIC		Y	
CA	DEPT OF CORRECTIONS FORS INQ	Agency	DOC		Y	
CB	DEPT OF CORRECTIONS FORS INQ	Agency	DOC		Y	
CC	DEPT OF CORRECTIONS FORS INQ	Agency	DOC		Y	
CD	DEPT OF CORRECTIONS FORS INQ	Agency	DOC		Y	
CE	DEPT OF CORRECTIONS FORS INQ	Agency	DOC		Y	
CF	DEPT OF CORRECTIONS FORS INQ	Agency	DOC		Y	
CG	DOC FORS SEX OFFENDER REG INQ	Agency	DOC		Y	
CH	DOC FORS INQUIRY	Agency	DOC		Y	
P	DEPT OF CORRECTIONS INQUIRY	Agency	DOC		Y	
QP	DEPT OF CORRECTION INQUIRY	Agency	DOC		Y	
AVL	DOL ABANDONED VEH CHK BY LIC	Agency	DOL		Y	
AVP	DOL ABANDONED VEH CHK BY LIC	Agency	DOL		Y	
AVV	DOL ABANDONED VEH CHK BY VIN	Agency	DOL		Y	
BD	BOAT DECAL INQUIRY VIA DRDOL	Agency	DOL		Y	
BH	BOAT REGISTRATION VIA DRDOL	Agency	DOL		Y	
BR	BOAT REGISTRATION VIA DRDOL	Agency	DOL		Y	
D	DRIVER INQUIRY	Agency	DOL		Y	
F	DOL GUN REGISTRATION	Agency	DOL		Y	
FN	DOL GUN REGISTRATION	Agency	DOL		Y	
FP	DOL GUN REGISTRATION	Agency	DOL		Y	
K	DOL DRIVER HISTORY INQUIRY	Agency	DOL		Y	
L	DOL LICENSE INQUIRY	Agency	DOL		Y	
P	DOL DISABLED PLACARD INQUIRY	Agency	DOL		Y	
T	DOL REG BY TAB NUMBER INQUIRY	Agency	DOL		Y	

TRANSACTION ID	LITERAL	FROM	TO	CREATES	RESPONSE EXPECTED	STARTING
V	DOL VIN INQUIRY	Agency	DOL		Y	
V2	DOL VIN INQUIRY PAGE 2	Agency	DOL		Y	
V3	DOL VIN INQUIRY PAGE 3	Agency	DOL		Y	
V4	DOL VIN INQUIRY PAGE 4	Agency	DOL		Y	
V5	DOL VIN INQUIRY PAGE 5	Agency	DOL		Y	
\$.8.	APPSV DOLLAR 8 DRDOL	NCIC	DOL	8	N	
ACQ	COMMERCIAL VEH CARRIER INQUIRY	Agency	NLETS		Y	
AM	ADMIN MESSAGE	Agency	NLETS		N	
AML	ADMIN MSG – LAW ENF ONLY	Agency	NLETS		N	
AQ	CRIMINAL HISTORY INQUIRY	Agency	NLETS		Y	
AR	CRIMINAL HISTORY RESPONSE	NLETS	Agency			
AVQ	COMMERCIAL VEH VEHICLE STATUS	Agency	NLETS		Y	
BQ	BOAT REGISTRATION INQ	Agency	NLETS		Y	
BR	BOAT REGISTRATION RESPONSE	NLETS	Agency			
CAQ	CANADIAN ARTICLE INQUIRY	Agency	NLETS		Y	
CAR	CANADIAN ARTICLE RESPONSE	NLETS	Agency			
CBQ	CANADIAN BOAT/ MOTOR QUERY	Agency	NLETS		Y	
CBR	CANADIAN BOAT RESPONSE	NLETS	Agency			
	CANADIAN CRIMINAL HISTORY					
CFQ	QUERY	Agency	NLETS		Y	
CGQ	CANADIAN GUN QUERY	Agency	NLETS		Y	
CGR	CANADIAN GUN RESPONSE	NLETS	Agency			
	CANADIAN CRIMINAL HISTORY					
CIQ	QUERY	Agency	NLETS		Y	
CR	CRIMINAL HISTORY RESPONSE	NLETS	Agency			
CSQ	CANADIAN SECURITIES QUERY	Agency	NLETS		Y	
CSR	CANADIAN SECURITIES RESPONSE	NLETS	Agency			
DNQ	NAME ONLY DRIVER INQUIRY	Agency	NLETS		Y	
DNR	NLETS NAME ONLY DRVR RESPONSE	NLETS	Agency			
DQ	DRIVER QUERY	Agency	NLETS		Y	
DR	DRIVER RESPONSE	NLETS	Agency			
DQG	REGIONAL DRIVER QUERY	Agency	NLETS		Y	
DRG	DRIVER RESPONSE	NLETS	Agency			
ER	ERROR MESSAGE	NLETS	Agency		Y	
FPQ	INTERPOL WANTED PER FULL INQ	Agency	NLETS		Y	
FQ	CANADA CRIMINAL HISTORY INQUIRY	Agency	NLETS		Y	

TRANSACTION ID	LITERAL	FROM	TO	CREATES	RESPONSE EXPECTED	STARTING
FR	CANADA CRIMINAL HISTORY INQUIRY RESPONSE	NLETS	Agency			
FTQ	INTERPOL STOLEN TRAVEL DOC ID	Agency	NLETS		Y	
FVQ	INTERPOL STOLEN VEH INQ ID	Agency	NLETS		Y	
GQ	AIRCRAFT REG INQUIRY	Agency	NLETS		Y	
GR	AIRCRAFT REG RESPONSE	NLETS	Agency			
HQ	WEATHER INQUIRY	Agency	NLETS		Y	
HR	WEATHER RESPONSE	Agency	NLETS		Y	
IAQ	INS ALIEN INQUIRY	Agency	NLETS		Y	
IPQ	INTERPOL WANTED INQ NAME DOB	Agency	NLETS		Y	
IQ	CRIMINAL HISTORY INQUIRY	Agency	NLETS		Y	
IR	CRIMINAL HISTORY RESPONSE	NLETS	Agency		Y	
ITQ	INTERPOL STOLEN TRAVEL DOC INQ	Agency	NLETS		Y	
IVQ	INTERPOL STOLEN VEH INQ BY VIN	Agency	NLETS		Y	
JQ	AIRCRAFT TRACKING INQUIRY	Agency	NLETS		Y	
JR	AIRCRAFT TRACKING RESPONSE	NLETS	Agency			
KQ	DRIVER HISTORY INQUIRY	Agency	NLETS		Y	
KR	DRIVER HISTORY RESPONSE	NLETS	Agency			
LJQ	LOJACK QUIET	Agency	NLETS		Y	
LQ	GENERIC MESSAGE INQUIRY	Agency	NLETS			
LR	GENERIC MESSAGE RESPONSE	NLETS	Agency			
MQ	HAZMAT INQUIRY	Agency	NLETS		Y	
MR	HAZMAT RESPONSE	NLETS	Agency		Y	
NQ	CAPTIS OWNER ID # FILE INQUIRY	Agency	NLETS		Y	
NAQ	NICB INQUIRY – ALL FILES	Agency	NLETS		Y	
NFQ	ACCESS TO NLETS JOURNAL DATA	ACCESS	NLETS		Y	
NIQ	NICB – IMPORT/EXPORT INQUIRY	Agency	NLETS		Y	
NIR	NICB RESPONSE	NLETS	Agency			
NLQ	ACCESS TO NLETS JOURNAL DATA	ACCESS	NLETS		Y	
OS	NLETS III STATE OUT OF SVC MSG	NLETS	Agency		Y	
PAQ	NLETS PAR/PROB/CORR INQUIRY	Agency	NLETS		Y	
PAR	PAR/PROB/CORR RESPONSE	NLETS	Agency		Y	
PBQ	NLETS PROBATION INQUIRY	Agency	NLETS		Y	
PBR	PROBATION INQUIRY RESPONSE	NLETS	Agency			
PCQ	NLETS CORRECTIONS INQUIRY	Agency	NLETS		Y	
PCR	CORRECTIONS INQUIRY RESPONSE	NLETS	Agency			

TRANSACTION ID	LITERAL	FROM	TO	CREATES	RESPONSE EXPECTED	STARTING
PPQ	NLETS PAROLE INQUIRY	Agency	NLETS		Y	
PPR	PAROLE INQUIRY RESPONSE	NLETS	Agency			
PR	CAPTIS PRISONER TRANSPORT RESPONSE	NLETS	Agency			
PT	CAPTIS PRISONER TRANSPORT INQUIRY	Agency	NLETS		Y	
RNQ	REGISTRATION BY NAME INQUIRY	Agency	NLETS		Y	
RNR	REG BY NAME RESPONSE	NLETS	Agency			
RQ	REGISTRATION INQUIRY	Agency	NLETS		Y	
RQG	REGIONAL REGISTRATION INQUIRY	Agency	NLETS		Y	
RR	REGISTRATION RESPONSE	NLETS	Agency			
RRG	REGIONAL REGISTRATION RE- SPONSE	NLETS	Agency			
SM	SERVICE MESSAGE	Agency	NLETS		Y	
SON	SEX OFFENDER NOTIFICATION	Agency	NLETS		Y	
SOQ	NLETS SEX OFFENDER INQUIRY	Agency	NLETS		Y	
SOR	SEX OFFENDER RESPONSE	NLETS	Agency			
SQ	SNOWMOBILE INQUIRY	Agency	NLETS		Y	
SR	SNOWMOBILE RESPONSE	NLETS	Agency			
SWQ	STATE WARRANT QUERY	Agency	NLETS		Y	
SWR	STATE QW RESPONSE	NLETS	Agency			
TA	ORI FILE ADD	Admin Terminal	NLETS		Y	
TD	ORI FILE DELETE	Admin Terminal	NLETS		Y	
TQ	ORI INQUIRY	Agency	NLETS		Y	
TR	ORION RESPONSE	NLETS	Agency			
TU	ORI FILE UPDATE	ACCESS	NLETS		Y	
TV	ORI FILE REVIEW	Agency	NLETS		Y	
UQ	CANADA DRIVER INQUIRY	Agency	NLETS		Y	
UR	CANADA DRIVER INQUIRY RESPONSE	NLETS	Agency			
VQ	CANADA STOLEN VEH CHECK	Agency	NLETS		Y	
VR	CANADA STOLEN VEH CHECK RESPONSE	NLETS	Agency			
WQ	CANADA WANTED PERSON INQUIRY	Agency	NLETS		Y	
WR	CANADA WANTED PERSON RESPONSE	NLETS	Agency			

TRANSACTION ID	LITERAL	FROM	TO	CREATES	RESPONSE EXPECTED	STARTING
XQ	CANADA REGISTRATION	Agency	NLETS		Y	
YQ	HIT CONFIRMATION INQUIRY	Agency	NLETS		Y	
YR	HIT CONFIRMATION RESPONSE	NLETS	Agency		N	
SM	SERVICE MESSAGE	NLETS	Agency		Y	
XQ	CANADIAN VEH REG INQ	Agency	NLETS		Y	
XR	CANADIAN VEH REG RESPONSE	NLETS	Agency		N	
FROM III – UNSOLICITED MESSAGES						
\$.A.CHR.	CRIMINAL HISTORY REQUEST	NCIC	W2/WACIC		Y	
\$.A.NPR.	NO PRIOR RECORD	NCIC	W2/WACIC		N	
	SID REJECTED – NO PRIOR NCIC					
\$.A.RNP.	RECORD	NCIC	W2/WACIC		N	
\$.A.PIR.	PRIOR RECORD	NCIC	W2/WACIC		N	
	SID REJECTED – PRIOR NCIC					
\$.A.RPR.	RECORD	NCIC	W2/WACIC		N	
\$.A.SSO.	SINGLE SOURCE OFFENDER	NCIC	W2/WACIC		N	
\$.A.MSO.	MULTI-SOURCE OFFENDER	NCIC	W2/WACIC		N	
\$.A.EXP.	FBI NUMBER EXPUNGED	NCIC	W2/WACIC		N	
\$.A.EXS.	SID NUMBER EXPUNGED	NCIC	W2/WACIC		N	
\$.A.FNC.	FBI NUMBER CHANGED	NCIC	W2/WACIC		N	
\$.A.REA.	REACTIVATION MESSAGE	NCIC	W2/WACIC		N	
\$.A.DEC.	DECEASED SID RETIRED	NCIC	W2/WACIC		N	
\$.A.CON.	FBI CONSOLIDATION	NCIC	W2/WACIC		N	
\$.A.NMS.	SID CONSOLIDATION	NCIC	W2/WACIC		N	
\$.A.CFN.	APPLICANT FINGERPRINT NO IDENT	NCIC	W2/WACIC		N	
\$.A.CFR.	APPLICANT FINGERPRINT IDENT	NCIC	W2/WACIC		N	
\$.A.PES.	ERRONEOUS SINGLE SOURCE SUB	NCIC	W2/WACIC		N	
\$.A.PEM.	ERRONEOUS MULTI SOURCE SUB	NCIC	W2/WACIC		N	
NCIC – ADMINISTRATIVE MESSAGES TO ACCESS						
\$.U.	NCIC III FILE OUT OF SERVICE	NCIC	ACCESS		N/A	
\$.V.	NCIC III FILE IN FULL SERVICE	NCIC	ACCESS		N/A	
\$.W.	NCIC III FILE IN RESTRICTED SERVICE	NCIC	ACCESS		N/A	
	NCIC FILE CONTINUE RESTRICTED					
\$.X.	SERVICE	NCIC	ACCESS		N/A	

TRANSACTION ID	LITERAL	FROM	TO	CREATES	RESPONSE EXPECTED	STARTING
\$.Y.	NCIC LINE REOPENED/III FULL SERVICE	NCIC	ACCESS		N/A	
\$.Z.	NCIC LINE REOPENED III RESTRICTED SERVICE	NCIC	ACCESS		N/A	
\$.1.	NCIC GOING OUT OF SERVICE	NCIC	ACCESS		N/A	
\$.2.	NCIC BACK IN FULL SERVICE	NCIC	ACCESS		N/A	
\$.3.	RESEND TIMEOUT	NCIC	Agency		N/A	
\$.4.	NCIC RESTRICTED SERVICE	NCIC	Agency		N/A	
\$.5.	EXTENDED RESTRICTED SERVICE	NCIC	Agency		N/A	
\$.6.	NCIC FILES IN FULL SERVICE	NCIC	Agency		N/A	
\$.7.	NCIC FILES IN RESTRICTED SERVICE	NCIC	Agency		N/A	
\$.8.	MISC NOTIFICATIONS (except stolen vehicle)	NCIC	Agency		N/A	
\$.10.	FINGERPRINT MATCHER OUT OF SERVICE	NCIC	Agency		N/A	
\$.11.	FINGERPRINT MATCHER IN FULL SERVICE	NCIC	Agency		N/A	
\$.B.	FILE TRANSFER READY	NCIC	Agency		N/A	
\$.C.	REQUEST FOR VALIDATION	NCIC	Agency		N/A	
\$.D.	DUPLICATE VEHICLE NOTIFICATION	NCIC	Agency		N/A	
\$.E.	SERIOUS ERROR NOTIFICATION	NCIC	Agency		N/A	
\$.F.	FAIL TO VALIDATE	NCIC	Agency		N/A	
\$.G.	REFERENCE GROUP OWNERSHIP	NCIC	Agency		N/A	
\$.H.	ORIGINATING AGENCY NOTIFICATION	NCIC	Agency		N/A	
\$.I.	DELAYED INQUIRY HIT NOTIFICATION	NCIC	Agency		N/A	
\$.J.	EMANCIPATION NOTIFICATION	NCIC	Agency		N/A	
\$.L.	LOCATE NOTIFICATION	NCIC	Agency		N/A	
\$.K.	MISSING INFORMATION	NCIC	Agency		N/A	
\$.M.	UNIDENTIFID/MISSING PERSON MATCH	NCIC	Agency		N/A	
\$.N.	WANTED PERSON NO DENTAL MATCH	NCIC	Agency		N/A	
\$.O.	SUPERVISED RELEASE NOTIFICA- TION	NCIC	Agency		N/A	
\$.P.	PURGE/PURGE FAILURE	NCIC	Agency		N/A	
\$.Q.	SEXUAL OFFENDER NOTIFICATION	NCIC	Agency		N/A	
\$.R.	BENEFITS DATA	NCIC	Agency		N/A	

TRANSACTION ID	LITERAL	FROM	TO	CREATES	RESPONSE EXPECTED	STARTING
\$.S.	STATISTICAL MODE NOTIFICATION	NCIC	Agency		N/A	
\$.NICS.	NICS OUT OF SERVICE	NCIC	Agency		N/A	
MKE	INTERSTATE IDENTIFICATION INDEX – III	FROM	TO		RESPONSE EXPECTED	
EHN	ENTER SUPPLEMENTAL IDENTIFIERS	W2/WACIC	NCIC		Y	
DRS	DELETE RECORD SID	W2/WACIC	NCIC		Y	
DEC	DECEASE RECORD SID IN III	W2/WACIC	NCIC		Y	
MRS	MODIFY RECORD SID	W2/WACIC	NCIC		Y	
ZR	RECORD MAINTENANCE	W2/WACIC	NCIC		Y	
ZRS	RECORD MAINTENANCE	W2/WACIC	NCIC		Y	
ZI	RECORD MAINTENANCE	W2/WACIC	NCIC		Y	
XHN	CANCEL SUPPLEMENTAL IDENTIFI- ERS	W2/WACIC	NCIC		Y	
	UNKNOWN MKE'S					
FQC	IFTA INQUIRY	Agency	NLETS		Y	
FRC	IFTA RESPONSE	NLETS	Agency			
HMLND	HOMELAND AUTO-UPDATE	?	EAST		Y	
HMLND	HOMELAND AUTO-UPDATE	?	OLYEM		Y	
HMLND	HOMELAND AUTO-UPDATE	?	WEST		Y	
HMLND	HOMELAND AUTO-UPDATE	?	WSPAS		Y	
HS	HOMELAND SECURITY	?	NLETS		Y	
HSL	HOMELAND SECURITY	?	NLETS		Y	
DRA	NDPIX RENEW ENTRY RESPONSE	NLETS	Agency			
DRX	NDPIX RENEW ENTRY	Agency	NLETS		Y	
DTA	NDPIX USER REPORT RESPONSE	NLETS	Agency			
DTX	NDPIX USER REPORT REQUEST	Agency	NLETS		Y	
DUA	NDPIX UPDATE RESPONSE	NLETS	Agency			
DUX	NDPIX UPDATE	Agency	NLETS		Y	
DEA	NDPIX ENTRY RESPONSE	NLETS	Agency			
DEX	NDPIX ENTRY	Agency	NLETS		Y	



Appendix C

Functional Requirements

Appendix C – Functional Requirements

BUSINESS PROCESS

The table below presents the core functional business components of the future ACCESS environment, and it includes the modules necessary to meet business needs such as data query and messaging.

The M/D/O column of this table indicates the nature of each requirement as follows:

M – Mandatory.

D – Desirable.

O – Optional.

Req. ID	M/D/O	General	Current Capability or Configurable Item	Custom Development	Future Release	Not Available
BP-1	M	The proposed solution must accommodate changes to existing message keys by WSP administrators and the addition of new message keys as required, specifically allowing WSP administrators to add new and change existing message keys without vendor programming assistance.				
BP-2	M	The proposed solution must minimally provide all of the functionality of the current ACCESS environment, as detailed in Section II and APPENDIX A.				
BP-3	D	The proposed solution should provide transaction-level/group user authorization capabilities.				
BP-4	D	The proposed solution should provide a means for real-time end-user notifications regarding system availability. Examples include, but are not limited to, “system down” or “system not responding.”				
BP-5	M	The proposed solution must process batch transactions from local agencies (e.g., processing a group of inquiries on a batch of data items or processing groups of record entries or modifications).				

Req. ID	M/D/O	General	Current Capability or Configurable Item	Custom Development	Future Release	Not Available
BP-6	M	The proposed solution must handle message header and destination errors (both user and application) in a consistent manner with the return of a message that indicates the problem.				
BP-7	M	The proposed solution must allow users to receive priority messages (to be defined by WSP administrators) first, regardless of what other information is queued.				
BP-8	D	The proposed solution should utilize compression techniques for data, message, and image packets to maximize system performance, including an explanation of the compression method used.				
BP-9	D	For existing interfaces where hardware encryption is in place, the proposed solution should utilize encryption techniques to maximize protection from unauthorized access or monitoring, including an explanation of the encryption technique utilized, as required by CJIS Security Policy.				
BP-10	D	The proposed solution should accommodate network elements that may already be encrypted at the originating source, including hardware encryption. In this case, network elements are the packets with header and data that have been encrypted by hardware or software. The proposed application should be able to decrypt packets whether delivered as part of the present text protocol or a future Web service or similar protocol.				
BP-11	D	The proposed solution should, when appropriate, automatically route NCIC response transactions to WACIC for update (e.g., \$ msgs).				
BP-12	D	The proposed solution should utilize nonsequential message and response return techniques to improve performance and timeliness of information. The arrival and processing of messages should be independent. As message A arrives before message B, processing starts on both, perhaps to different applications. Thus, message B should finish first and be returned first. This out-of-sequence response or process should not be a problem.				
BP-13	O	The proposed solution should enable integration with a recognized, proven, and deployed NCIC-required user certification program.				

Req. ID	M/D/O	General	Current Capability or Configurable Item	Custom Development	Future Release	Not Available
BP-14	D	The proposed solution should provide timely updates to NCIC and WACIC code tables. WSP updates WACIC as the changes become available from NCIC. These changes do not arrive at a particular interval. "Timely" means that WSP can make the changes to any such tables without calling upon the vendor to make the change. This could be for edit values in the user interface or as distribution files to other dispatch or records systems that interface with ACCESS.				
BP-15	D	The proposed solution should print any of the reports or other outputs at administratively configurable locations/printers (e.g., as an applet or function).				
BP-16	M	The solution must enable every component of the message switch system to be modified by system administrators to meet changing federal and state standards without the need to contract with a vendor to make changes.				
BP-17	M	For future new interfaces in support of XML formats, the proposed solution must utilize encryption techniques to maximize protection from unauthorized access or monitoring, including an explanation of the encryption technique utilized, as required by CJIS Security Policy.				

ANALYSIS

The table below presents the components required of the future ACCESS solution relative to the use of the data captured for subsequent analytical decision making, including various types of online and hard copy reporting requirements.

The M/D/O column of this table indicates the nature of each requirement as follows:

M – Mandatory.

D – Desirable.

O – Optional.

Req. ID	M/D/O	Analysis	Current Capability or Configurable Item	Custom Development	Future Release	Not Available
AN-1	M	The proposed solution must log every inbound and outbound transaction and messaging action. Images must be cited without including the image file in the log, unless specified by the user. Logging must be configurable by ACCESS administrators.				
AN-2	D	The proposed solution should provide all reports in a format that is viewable on screen. The solution should provide the capability to print any report.				
AN-3	D	The proposed solution should have online detailed transaction logs for a WSP-configurable period of time.				
AN-4	M	The proposed solution must provide the capability to export log data into any of the standard and commercially available software/report packages or formats such as: .xls, .csv, .txt, PDF, and XML.				
AN-5	M	The solution must provide WSP staff with the ability to create/generate custom or ad hoc reports on any of the data elements in the ACCESS log, without vendor intervention. The proposed solution should provide the ability to modify report headers, exclude columns, sort by and/or filter on any key data field (including filtering on date range), and save any modified report format for subsequent use.				

Req. ID	M/D/O	Analysis	Current Capability or Configurable Item	Custom Development	Future Release	Not Available
AN-6	D	The solution should provide standardized daily, weekly, and monthly system management and quality assurance reports, modifiable by WSP.				
AN-7	D	The solution should provide the ability to generate NCIC validation reports on demand, and modifiable by WPS.				
AN-8	M	The proposed solution must have the ability to query the log data based on specific search criteria.				
AN-9	D	The proposed solution should provide reports defined by WSP ACCESS auditors. These standard or ad hoc reports should be made available in real time and authorized via the user provisioning screen. Examples include, but are not limited to, types of messages used by a jurisdiction (ORI) during a specific span of time, details on random messages, and details on requested or selected messages.				
AN-10	D	The proposed solution should provide a set of standard system and data reports for message switch operations, regardless of format, minimally including the following:				
	D	List of transaction types (warrants, missing, etc.) for various agencies run over a user-defined period.				
	D	List of all transactions for a certain ORI, organized by message key or record type.				
	D	Ability to schedule reports.				
AN-11	D	The proposed solution should produce daily activity reports by operator.				
AN-12	M	The proposed solution must provide access to audit trails for authorized users, based on configurable security roles. These audit logs should come with robust reporting and search tools.				

ACTION AND DECISION

The table below describes the components required to allow users of the future ACCESS solution to render business decisions based on the analytical information presented. These decisions will have a downstream effect on other system users. For example, notifications can be made to validate information contained in the system prior to enforcement action being taken.

The M/D/O column of this table indicates the nature of each requirement as follows:

M – Mandatory.

D – Desirable.

O – Optional.

Req. ID	M/D/O	Action and Decision	Current Capability or Configurable Item	Custom Development	Future Release	Not Available
AD-1	M	The proposed solution must assist in enforcement of the 10-minute rule, that is, upon receipt of an urgent request for hit confirmation, the entering agency must provide a substantive answer within 10 minutes. If no confirmation is received, the system sends another request to the agency and to the designated state control point. If no response is received within 10 minutes, a third request is sent to the agency, NCIC, and WSP. If the request is going to another state, the control point for that state and NCIC quality control also receive the request.				

WORK FLOW

The table below describes requirements related to the routing, verification, and storage of information in the future ACCESS environment.

The M/D/O column of this table indicates the nature of each requirement as follows:

M – Mandatory.

D – Desirable.

O – Optional.

Req. ID	M/D/O	General Work Flow	Current Capability or Configurable Item	Custom Development	Future Release	Not Available
WF-1	M	The proposed solution must ensure that administrative messages can be sent or routed to:				
	M	• Users and groups of users.				
	M	• Agencies and groups of agencies.				
	M	• Defined devices.				
	M	• Computer interfaces.				
	M	• Any of the above within a defined geographic area or defined group.				
WF-2	M	The proposed solution must allow for the maintenance of user-defined, reusable group destination codes or lists of users.				
WF-3	D	The proposed solution should enable configurable routing based on message or transaction type and content. For example, a hit on a wanted person destined for a mobile device is automatically “copied” to a dispatch center device.				
WF-4	M	The proposed solution must provide guaranteed message and transaction delivery, including an explanation of how this is accomplished.				

Req. ID	M/D/O	General Work Flow	Current Capability or Configurable Item	Custom Development	Future Release	Not Available
WF-5	D	The proposed solution should provide for optional message and transaction escalation and alternative delivery. For example, Agency A experiences a power outage, so Agency B is designated to receive Agency A's messages (set by end-user agency).				
WF-6	M	The proposed solution must provide queuing that allows messages and transactions to accumulate for subsequent delivery (guaranteed delivery) in the event of connectivity or system downtime; such queues are to be configurable by WSP both by duration and message type.				
WF-7	D	The proposed solution should allow group queues with the option to delete messages on first read or require that messages be deleted manually.				
WF-8	D	The proposed solution should allow messages to queue and present them based on message priorities.				
WF-9	M	The proposed solution must handle the delivery of all messages and responses from all sources to the appropriate end user. This capability must be table-driven.				
WF-10	M	The message switching application must have the ability to accurately time- and date-stamp all transactions processed based on the operating system clock.				



Appendix D

Technical Requirements

Appendix D – Technical Requirements

INFRASTRUCTURE

The table below describes elements that provide technology solutions and deliver secure and reliable systems. These elements are primarily hardware and networking components.

The M/D/O column of this table indicates the nature of each requirement as follows:

M – Mandatory.

D – Desirable.

O – Optional.

Req. ID	M/D/O	General	Current Capability or Configurable Item	Custom Development	Future Release	Not Available
IN-1	M	The proposed solution must minimally provide the operational capacity of the current ACCESS environment, including photos. "Operational capacity" regarding the number of expected messages processed through ACCESS is defined in subsection II.D.3 of this RFP.				
IN-2	D	The proposed solution should utilize a system architecture that is open, nonproprietary, and portable.				
IN-3	D	The proposed solution should be adaptive and use extensible architecture for future expansion and scalability without the need for major architectural modifications.				
IN-4	M	The future ACCESS solution environment must utilize a Windows operating system, and the operating system must not be altered.				
IN-5	M	The proposed solution must provide system diagnostics, including, but not limited to, error correction and detection.				

Req. ID			Current Capability or Configurable Item	Custom Development	Future Release	Not Available
	M/D/O	General				
IN-6	M	The proposed solution must provide production, test, training, and development environments. The user's access level must allow him/her to select the system desired.				
IN-7	M	The proposed solution's internal processing time must be 1 second or less, unless the operation is external to ACCESS; the vendor should include a description of how the solution will meet this response requirement as well as methods for verification of performance.				
IN-8	M	The hardware must provide the capability for remote maintenance and troubleshooting.				
IN-9	M	There must be no hardware or software/application restrictions limiting the number of users capable of using the ACCESS System.				

Req. ID	M/D/O	Hardware	Current Capability or Configurable Item	Custom Development	Future Release	Not Available
IN-10	D	The proposed solution should allow the addition of third-party hardware and software components (e.g., certification application, SAN, and NAS) through open architecture.				
IN-11	D	The proposed solution should provide WSP with the right to contract directly with hardware providers for servers if it believes it is in its best interest to do so. A decision to acquire hardware independently of the vendor should not result in a price penalty. Vendors should confirm no price penalty. Vendors should also identify their preferences for a hardware acquisition approach.				
IN-12	M	The proposed solution must be designed to allow for the addition of hardware and capacity to accommodate increases in ACCESS throughput and workload over a 5-year period.				
IN-13	M	All hardware must be new and not remanufactured/refurbished.				
IN-14	M	If any hardware component is of proprietary design or manufacture, the manufacturer must guarantee the availability or replacement parts for a period of not less than 10 years.				
IN-15	M	The hardware must be current technology that is commercially installed and operational prior to proposal due date.				
IN-16	M	The system must have sufficient hardware to provide fault tolerant processing.				
IN-17	M	The hardware will reside at the current WSP facility location.				
IN-18	M	The storage medium used for backup/recovery data must be reusable. The DR process must utilize the reusable storage medium.				
IN-19	M	The proposed hardware solution must come with the maximum warranty available (e.g., 3 years). The length of the warranty shall be a minimum of 12 months.				
IN-20	M	The warranty clock for the application software must not start until final acceptance of the ACCESS solution.				

Req. ID	M/D/O	Network	Current Capability or Configurable Item	Custom Development	Future Release	Not Available
IN-21	M	The proposed solution must be compatible with IP networking standards.				
IN-22	D	The proposed solution should provide Simple Network Management Protocol (SNMP) and the Web-based tool set for centralized control of the system using an enterprise management platform.				
IN-23	M	The proposed solution must be compatible with current wired networking standards (e.g., 10 Mb/100 Mb/1 Gb) for WSP.				
IN-24	M	The proposed solution must provide TCP/IP addressability for all components throughout the network.				
IN-25	D	The proposed solution should recognize addressable agency ORIs.				
IN-26	D	The proposed solution should have the future capability of operating a DR hot site located in Eastern Washington. This capability should be acquired without alteration of the software beyond adjustment of parameters or tables that are under the control of WSP.				

APPLICATIONS

The following table describes components required of the software solutions that ensure operability in the target environment and includes software platform, storage, and data model requirements:

The M/D/O column of this table indicates the nature of each requirement as follows:

M – Mandatory.

D – Desirable.

O – Optional.

Req. ID	M/D/O	General	Current Capability or Configurable Item	Custom Development	Future Release	Not Available
AP-1	D	The proposed solution should provide at least one simple, easy-to-manage, and inexpensive secondary user authentication strategy, in accordance with CJIS Security Policy.				
AP-2	D	The proposed solution should provide multilevel security to restrict access and control functionality, in accordance with CJIS Security Policy.				
AP-3	D	The solution should provide an administrative or dashboard monitor view of the application and its status.				
AP-4	D	The proposed solution should afford system administrators the ability to easily update security parameters while the system is online.				
AP-5	D	The proposed solution should process data in real time. This means that any parameter change or data change should be done while the system is online. The change should take effect immediately.				
AP-6	D	The proposed solution should utilize HTTPS, especially for the user application component. Vendors may propose an alternative that achieves the same level of or a higher level of security and accessibility.				

Req. ID	M/D/O	General	Current Capability or Configurable Item	Custom Development	Future Release	Not Available
AP-7	D	The proposed solution should provide the export or import of system code tables for WSP use with other systems.				
AP-8	D	The proposed solution should utilize application server technology that allows tasks to be off-loaded onto other computers or processors to prevent a loss in performance as system usage grows.				
AP-9	M	The ACCESS application software must have a minimum 12 months of Warranty against defects.				
AP-10	M	The ACCESS application must use an industry standard programming language.				
AP-11	M	The ACCESS application must have interactive debugging and trace aids.				
AP-12	M	The ACCESS application software must provide fault tolerant processing.				
AP-13	M	The development environment must include version control and provide source code change tracking. It will also track changes to message switch configurations and program modifications.				
AP-14	M	The proposed solution must provide NCIC file transfer capability.				

Req. ID	M/D/O	User Interface	Current Capability or Configurable Item	Custom Development	Future Release	Not Available
AP-15	M	The proposed solution must allow for the establishment of user accounts and passwords, and should be fully compliant with, the guidelines and specifications established in the FBI Criminal Justice Information Services Security Policy.				
AP-16	D	The proposed solution should provide the identification and credentialing of individual users on the local agency interface to ACCESS for agencies accessing via a secure HTTP session.				
AP-17	M	The proposed solution must allow the system administrator to authorize users to log in to the system, set allowable functions for each user, and reset user passwords.				
AP-18	M	The proposed solution must allow a user to log on with his/her current password and then change his/her own password.				
AP-19	M	The proposed solution must allow WSP to define how long a password will remain valid within the following secure password attributes established by the FBI Criminal Justice Information Services Security Policy: • Minimum length of eight characters. • Not a dictionary word or proper name. • Not the same as the user ID. • Changed at a maximum of once every 90 days. • Prevents reuse of the last 10 passwords. • Shall not be transmitted in the clear, outside the secure domain. • Password must minimally include two of the following: alphabetical, numeric, and special characters. User account termination should be automatic based on certification date or cancellation by an authorized manager-level command.				

Req. ID	M/D/O	User Interface	Current Capability or Configurable Item	Custom Development	Future Release	Not Available
AP-20	D	The proposed solution should utilize user-driven (e.g., user ID, ORI, or combination) security profiles to determine system access to the following:				
	D	• “Read” authority.				
	D	• “Add” authority.				
	D	• “Modify” authority.				
	D	• “Delete” access.				
	D	• Each function key for which authority is granted.				
	D	• Each command for which authority is granted.				
	D	• User classification or role.				
	D	• Production (live) or training mode.				
AP-21	M	The proposed solution must require users to log on to the system before receiving access to any function. The solution should generally provide one user, system-wide with agency associations. This sign-on should include, at a minimum:				
		• Agency ID (may be user-specified).				
		• A unique user ID and password.				
AP-22	D	The proposed solution should allow for the ability to change password at setup, at sign-on, and during the course of a logged-in session.				
AP-23	M	The proposed solution must provide a means for users to recall or reset their password using techniques including, but not limited to: • Forgot My Password techniques used extensively on Internet sites. • Challenge questions and answers established during user setup. • A temporary complex password if the user successfully answers the challenge question and a required new user password upon successful session sign-on. • Ability for the terminal agency coordinator to reset a password if necessary.				

Req. ID	M/D/O	User Interface	Current Capability or Configurable Item	Custom Development	Future Release	Not Available
AP-24	M	The proposed solution must be able to be configured such that users are notified of impending password expiration. If a user's password has expired, the system should prompt the user to change the password at sign-on.				
AP-25	D	The proposed solution should have a single centralized repository for users and their access information (authentication, authorization, and accounting, also referred to as "AAA") so that users have one username and one set of authentication credentials (such as a password) and so that all user attributes and authorization, including date of entry, are managed in one place. This may be accomplished by using a Lightweight Directory Access Protocol (LDAP) server.				
AP-26	D	The proposed solution should produce an audit trail of all user logon transactions, including password resets, for the direct-connect, secure HTTP clients.				
AP-27	D	The solution should allow for the use of pointing devices, hot keys, key combinations, buttons, and hyperlinks.				
AP-28	M	The proposed solution's client application must be Web browser-based and utilize best-of-breed Web form design and usability elements.				
AP-29	D	The proposed solution's client application screens should be printable to configurable local or networked printers, using print commands provided by the browser. The proposed solution's client application screens should be able to be captured using commands provided by the browser.				

Req. ID	M/D/O	User Interface	Current Capability or Configurable Item	Custom Development	Future Release	Not Available
AP-30	D	The proposed solution should allow automatic printing of messages as specified.				
AP-31	O	The proposed solution should provide value-added features normally associated with a mail system, including:				
		Saving draft messages for finalizing and sending at a later time. These should be available to other supervisors/users as authorized in the user profile.				
		Recovering and resending messages at all levels of the system.				
AP-32	M	The proposed solution must provide a user interface with a single primary inquiry form or presentation that includes common inquiries (80 to 100 percent of all inquiries available).				
AP-33	M	The proposed solution must provide users with a consistent user interface throughout the application, in order to minimize user training and system administration.				
AP-34	M	The proposed solution must provide a command line, as well as screen entry. Users should be able to enter messages on the command line without affecting operations in the forms or other work area.				
AP-35	M	The proposed solution must allow tasks to be entered by keystroke and/or mouse action. However, the system should allow all commands to be initiated by keystroke if desired.				
AP-36	D	The proposed solution should provide standard UI items, such as drop-down menus, to make selection easier for frequently used fields, such as message keys, all code tables, and agency IDs.				
AP-37	D	The proposed solution should provide "auto complete" functionality for code table lookups as the user begins to enter data in the code table lookup field.				
AP-38	M	The proposed solution must allow for automated updates to the user interface application.				

Req. ID	M/D/O	User Interface	Current Capability or Configurable Item	Custom Development	Future Release	Not Available
AP-39	M	The proposed solution must utilize pre-fill fields in appropriate pre-formatted screens, eliminating redundant data entry without impacting the usability.				
AP-40	D	The proposed solution should provide quick entry methods such as hot keys to minimize the keystrokes required to perform inquiries. Such hot keys would enable the entry of single data inquiries on the command line, and the inquiry would then be executed according to the hot key used. The single data inquiries include:				
		• Driver's license number (DLN).				
		• License plate number.				
		• Name.				
		• Vehicle identification number.				
AP-41	D	The proposed solution should provide menus to facilitate access to less frequently used functions and to aid users with applications used infrequently.				
AP-42	D	The proposed solution should allow users to move forward and backward to complete data fields.				
AP-43	D	The proposed solution should allow users to correct spelling errors without having to retype the entire field.				
AP-44	D	The proposed solution should provide users with standard form navigation and allow easy movement from one work area to another via mouse or keyboard.				
AP-45	O	The proposed solution should provide hot keys for frequently used functions and associate them with the user profile. Hot keys could be standard key assignments (e.g., F1 through F4), and user keys would be optional key assignments (e.g., F5 through F9).				
AP-46	D	The proposed solution should enable users to recall (configurable by WSP) and resend recently sent messages. The solution should also provide Windows cut-and-paste functionality.				

Req. ID	M/D/O	User Interface	Current Capability or Configurable Item	Custom Development	Future Release	Not Available
AP-47	D	The solution should provide default, configurable values for fields based on previous input, referential lookup, or other mechanisms. It should incorporate currently used defaults.				
AP-48	D	The proposed solution should provide the ability to load a Microsoft Word file onto the system that is then available as a bulletin to advise of system updates and other information.				
AP-49	M	The solution must provide lookup tables for valid values for fields.				
AP-50	D	The vendor should highlight other functionality or capabilities available in the solution beyond those noted above.				
AP-51	M	The solution must allow the submitter to stack multiple transactions in one submission (e.g., a QW with data, a DQ with data, a QV with data) and more.				

Req. ID	M/D/O	Database and Backups	Current Capability or Configurable Item	Custom Development	Future Release	Not Available
AP-52	M	The proposed solution must provide an ORI table. The elements within the table should be configurable by WSP.				
AP-53	M	The proposed solution must utilize Microsoft SQL database solutions.				
AP-54	D	The solution should provide for access to and manipulation of the data (e.g., ORI data) in the database through a standard management system.				
AP-55	M	The solution must provide tools for monitoring and enhancing database organization and performance.				
AP-56	D	The solution should provide tools for database design and development, including documentation, diagramming, normalization, database generation, screen design and generation, report design and generation, and procedure maintenance tools.				
AP-57	D	Whatever databases exist for the support of ACCESS, including, but not limited to, message definitions, user authorization, or destination/source definitions, should be available to WSP personnel..				
AP-58	M	The proposed solution must have the capability to execute scheduled, unattended online system backups without affecting system performance.				
AP-59	M	The proposed solution must have the ability to restore from system backups.				
AP-60	M	The solution must provide robust system backup/archiving tools and strategies.				

PUBLICATION

The table below lists components required to ensure user access to information captured by the desired solution and includes such elements as global search engine indexing, report-writing services, data transformation services, and subscription and notification systems.

The M/D/O column of this table indicates the nature of each requirement as follows:

M – Mandatory.

D – Desirable.

O – Optional.

Req. ID	M/D/O	Dissemination and Reports	Current Capability or Configurable Item	Custom Development	Future Release	Not Available
PU-1	D	The proposed solution should have a report batch monitor that controls the number of reports that may be run at a given time for each server.				
PU-2	O	The proposed solution should have a report scheduler that can schedule reports to be automatically run at user-defined times.				
PU-3	D	The proposed solution should provide reports, both of real-time and snapshot data, that are publishable to an intranet or the Internet.				

INTEGRATION

The table below describes components involved in the exchange of information between the future ACCESS and related public safety systems. Requirements here are relative to the interfaces that move information between systems at a predetermined time (i.e., batch and/or real-time interfaces).

The M/D/O column of this table indicates the nature of each requirement as follows:

M – Mandatory.

D – Desirable.

O – Optional.

Req. ID	M/D/O	Interfaces	Current Capability or Configurable Item	Custom Development	Future Release	Not Available
IT-1	M	The proposed solution must minimally provide the interface and protocol capabilities of the current ACCESS environment, as detailed in Sections II and IV.				
IT-2	M	The proposed solution must interface with NCIC and provide file transfer functionality.				
IT-3	M	The proposed solution must interface with Nlets.				
IT-4	M	The proposed solution must interface with W2.				
IT-5	M	The proposed solution must interface with DOC.				
IT-6	M	The proposed solution must seamlessly enable all current regional system interfaces to send properly formatted NCIC messages and transactions. This capability must be in place on the first day of implementation.				
IT-7	M	The proposed solution must interface with Washington DOL.				
IT-8	M	The proposed solution must be compliant with, recognize, and allow for data transactions according the NIEM data model.				

Req. ID	M/D/O	Interfaces	Current Capability or Configurable Item	Custom Development	Future Release	Not Available
IT-9	D	The proposed solution should provide transaction-based electronic data access to third-party systems (e.g., WASIS, WACIC, DOL) for query/exchange (for example, Web services, XML, or other transaction-based exchanges).				
IT-10	D	The proposing vendor should explain the approach to Web services.				
IT-11	D	WSP desires the option of implementing a means of authenticating a data source other than relying on network routing and firewalls. Is the message valid? Is the source valid (i.e., did this message come from DOL as it should have)?				
IT-12	D	The proposed solution should have the ability to search multiple (e.g., spawn inquiries) external systems and/or databases via a single query.				
IT-13	D	The proposed solution should have the ability to receive and respond to queries from authorized external systems and/or databases.				
IT-14	D	The proposed solution should save or print images regardless and independent of the response. This refers primarily to the user interface. Printing, image processing, file saving, and file retrieval should be dependent upon operating system or browser services. That includes independence from Windows, Linux, Apple Macintosh Internet Explorer, and Mozilla Firefox.				

Req. ID	M/D/O	Images	Current Capability or Configurable Item	Custom Development	Future Release	Not Available
IT-15	M	The proposed solution must process images as defined by NCIC.				
IT-16	M	The proposed solution must provide batch file processing from NCIC (e.g., \$.B).				
IT-17	D	The proposed solution should access other documents or images stored on a local or networked drive.				
IT-18	D	The proposed solution should retrieve and route images stored in various sources.				
IT-19	D	The proposed solution should retrieve and route other documents or images stored on a local or networked drive.				

STRATEGIC AND TACTICAL ANALYSIS

Enhanced strategic and tactical analysis is achieved with a system that successfully addresses the functional layers above. The components detailed in the table below provide complex relational information to criminal justice users from existing information systems. The components include summary data sets that can be used to build comprehensive data warehouses designed to drive business decisions between organizations.

The M/D/O column of this table indicates the nature of each requirement as follows:

M – Mandatory.

D – Desirable.

O – Optional.

Req. ID	M/D/O	Strategic and Tactical Analysis	Current Capability or Configurable Item	Custom Devel- opment	Future Release	Not Available
ST-1	D	The proposed solution should provide the ability for authorized end users to retrieve transaction log activity to report on actions and responses for a period of time. The parameters should be configurable by WSP.				

MANAGEMENT AND ADMINISTRATION

The table below lists components associated with the management and administration of the system, including the components necessary to ensure successful operation in the desired technical environment, as well as applicable standards and vendor support.

The M/D/O column of this table indicates the nature of each requirement as follows:

M – Mandatory.

D – Desirable.

O – Optional.

Req. ID	M/D/O	System Administration	Current Capability or Configurable Item	Custom Development	Future Release	Not Available
MA-1	M	The proposed solution must continually perform interface connectivity monitoring, hardware self-diagnosis, self-checking, and report errors to the operator console for remedial action.				
MA-2	M	The proposed solution must provide for software up-grades/maintenance that do not affect the production system (no downtime) in a load-balanced environment.				
MA-3	M	The proposed solution must provide a logging feature that logs entries, changes, and/or deletions to any configuration data (data transaction recovery log).				
MA-4	M	The proposed solution must be designed to allow for remote maintenance and troubleshooting.				
MA-5	M	The proposed solution must be able to set date, time, and time zone using the operating system or a time server date and time settings.				

Req. ID	M/D/O	Vendor Support	Current Capability or Configurable Item	Custom Development	Future Release	Not Available
MA-6	M	The proposing vendor must provide ongoing services and support, including, but not limited to, the following: toll-free 24/7 customer service, annual training classes, an online customer service Web site, and online software maintenance.				
MA-7	D	To maintain configuration integrity, the proposed solution should provide control for all configurable elements, including auditing, rollback, roll-forward, and configuration change transactions, with the ability to both import and export configurations.				
MA-8	D	The proposed solution should accommodate changes to production applications without impact to operations, and the vendor should explain how this is accomplished.				

Req. ID	M/D/O	Standards	Current Capability or Configurable Item	Custom Development	Future Release	Not Available
MA-9	D	The proposed solution should comply with established WSP and State of Washington technology standards and policies outlined in Section IV of the RFP.				
		Washington State IT Security Standards, Policy 401-S3.				
		Washington State Standards for Internet Markup Language, Policy 801-S2.				
MA-10	D	The proposed solution should be compliant with all national standards and policies outlined in Section IV of the RFP.				
		FBI NCIC 2000.				
		FBI CJIS Security Policy (V4.4), or latest.				
		NIEM.				
MA-11	D	The proposed solution should meet response time, delivery and transmittal requirements for NCIC 2000, Nlets and WSP. See subsections II.D.1 and II.D.3 of the RFP for information regarding availability, and see Req. ID IN-7 for WSP system response time.				
MA-12	D	The proposed solution should use standard NCIC codes and descriptors.				

Req. ID	M/D/O	Training, Documentation, and Testing	Current Capability or Configurable Item	Custom Development	Future Release	Not Available
MA-13	M	The proposed solution must provide access to online system help files (both user and application versions) that describe fields, forms, and data requirements, as well as procedures from system documentation.				
MA-14	D	The proposed solution should provide access to online NCIC manual files that describe fields, forms, and data requirements, as well as procedures and automatic updates.				
MA-15	D	The proposed solution should provide access to online Nlets manual files that describe fields, forms, and data requirements, as well as procedures and automatic updates.				
MA-16	D	The proposed solution should provide access to online ACCESS manual files that describe fields, forms, and data requirements, as well as procedures and automatic updates of the manual by WSP administrators.				
MA-17	D	The proposed solution should provide the ability to query the ACCESS manual and to allow automated updates by WSP administration.				
MA-18	M	The proposed solution must provide a detailed user-training program and include a syllabus of each class and sample training manual.				
MA-19	M	The proposed solution must provide sufficient training for the number and type of users described in the training plan outlined in the Management Response section of the proposal. This includes providing training during evening shifts. Vendors should provide a detailed definition of the number of training classes, class duration, class size, and class location.				
MA-20	M	The ACCESS application vendor must supply all documentation in English.				

Req. ID	M/D/O	Training, Documentation, and Testing	Current Capability or Configurable Item	Custom Development	Future Release	Not Available
MA-21	M	The ACCESS test system must include scripting tools. "Scripting tools" refers to tools that can generate messages with variations on values in the messages. The intervals between messages should be variable, as should the number of messages generated. The messages should be generated either for a time period, a number of messages, or until stopped. These are only a few of the types of things that could be done.				
MA-22	D	The ACCESS solution should contain load-testing software for measuring system performance.				



Appendix E

References Form

Appendix E – References Form

NOTE: Vendors must provide information for a minimum of **three (3)** relevant references but can add additional references as appropriate.

References					
1.	Name of Client Agency				
	Application Name				Year Contracted
	Client Address				
	Client City		State		ZIP Code
	Client Contact				Title
	Contact Telephone		Contact Fax		
	Contact E-Mail				
	Number of Years Contracted				
	Application Modules/Functions Operational				
	Application Modules/Functions Planned for Implementation				
	Total Contract Value				
	Number of Users				
	Number and Type of Federal Interfaces				
	Number and Type of Regional/Other Interfaces				
	2.	Name of Client Agency			
Application Name					Year Contracted
Client Address					
Client City			State		ZIP Code
Client Contact					Title
Contact Telephone			Contact Fax		
Contact E-Mail					
Number of Years Contracted					
Application Modules/Functions Operational					
Application Modules/Functions Planned for Implementation					
Total Contract Value					
Number of Users					
Number and Type of Federal Interfaces					
Number and Type of Regional/Other Interfaces					

References					
3.	Name of Client Agency				
	Application Name				Year Contracted
	Client Address				
	Client City		State		ZIP Code
	Client Contact				Title
	Contact Telephone		Contact Fax		
	Contact E-Mail				
	Number of Years Contracted				
	Application Modules/Functions Operational				
	Application Modules/Functions Planned for Implementation				
	Total Contract Value				
	Number of Users				
	Number and Type of Federal Interfaces				
	Number and Type of Regional/Other Interfaces				

Appendix F
Vendor Strength and Stability Form

Appendix F – Vendor Strength and Stability Form

Ref.	Vendor Response, Comments, or Explanation
Overview	
1	Vendor name.
2	Address.
3	Telephone number.
4	Contact person.
5	E-mail address.
6	Parent company or corporate headquarters.
7	Address.
8	Telephone number.
9	Contact person.
10	Telephone number.
11	E-mail address.
12	Information about any local branch offices or support centers that might serve an account in the northwestern United States. Number of employees and type(s) of services provided.
13	Name, address, and telephone number of each principal.
14	Year the vendor was established and any former vendor names.
15	Number of years the vendor has been in the software business.
16	Type of company (public or private).
17	Financial statements and annual reports for the past 3 years.
18	Amount/percentage of sales reinvested into research and development.
19	State and type of incorporation.
Personnel	
20	Total number of FTEs in the company.
21	Customer user support.
22	Customer technical support.
23	Research and development.
24	Project management.
25	Project implementation and rollout.
26	Total person years of experience for your company's employees (e.g., five support people with 3 years each = 15 person years).
27	Customer user support.

Ref.	Vendor Response, Comments, or Explanation
28	Customer technical support.
29	Research and development.
30	Project management.
31	Project implementation and rollout.
32	Estimated number of resources to be dedicated to this client.
Vendor Customer Support	
33	Are there user groups in place for your proposed hardware/software?
34	Does the vendor provide toll-free telephone support?
35	What are the hours of support (e.g., 9 a.m. to 5 p.m., ET – 24/7, etc.)?
36	How is after-hours support provided?
37	How are support calls classified and prioritized?
38	How are support calls escalated in an emergency?
39	What is the average response time to calls?
40	What is the average service call resolution time?
41	Will WSP have direct access to dedicated support personnel to solve a particular issue?
42	Does the vendor offer online access to general information and troubleshooting tools (e.g., searchable knowledge base, FAQs, training materials, and manuals)?
43	Will ongoing support for subsequent years be available through a maintenance agreement on a set-cost basis? What is included in this service?
44	What is the duration of warranty?
45	When does the warranty begin?
46	What is included in the software warranty?
47	What are the specifics for items to be typically performed for upgrades of the package?
Vendor Implementation History	
48	Number of years of experience for the vendor:
49	In public sector, state/local government.
50	In the mid to northwestern United States.
51	Total number of Web/Internet projects that the vendor has implemented:
52	In public sector, state/local government.
53	In the mid to northwestern United States.
54	Total number of Web/Internet projects that the vendor is currently undertaking:

Ref.	Vendor Response, Comments, or Explanation
55	In public sector, state/local government.
56	In the mid to northwestern United States.
<i>Pending Litigations</i>	
57	Number of pending litigations that the company has had in the past 5 years. Please attach a separate document with the details of each situation (client name, date, and description/cause).
58	Number of situations in which the company has been subject to liquidated damages in the past 5 years. Please attach a separate document with the details of each situation (client name, imposed amount, imposed date, collected amount, date collected, and description/cause).

Appendix G
Proposal Checklist

Appendix G – Proposal Checklist

Please note: Each response (management, technical, and cost) must be in its own distinct binder.

Ref.	Description	Yes	No
<i>Binder 1 – Management Response</i>			
1	Transmittal Letter		
2	Table of Contents		
3	Executive Summary		
4	Prior Experience		
5	Vendor References		
6	Vendor Strength and Stability		
7	Exceptions to Requirements of the RFP		
8	Contract Requirements		
9	Escrow Agreement Approach		
10	SOWs Required		
11	Conflict of Interest		
12	Project Management Approach		
13	Risk Management Approach		
14	Proposed Project Staff		
15	Data Conversion Approach		
16	Business Continuity Approach		
17	Implementation Approach		
18	Migration Approach		
19	Fail-Back Approach		
20	Test Plan Approach		
21	Training Approach		
22	System Documentation Approach		
23	Maintenance and Support Approach		
24	Optional Components Approach		
25	Project Oversight Acknowledgement		
26	SOW Acknowledgement		
27	Proposal Checklist		
<i>Binder 2 – Technical Response</i>			
1	Functional Specifications Response		
2	Technical Specifications Response		
3	Standards, Policies, and User Authentication Compliance Approach		
4	Overall Solution Approach		

Ref.	Description	Yes	No
5	Value-Added Services		
<i>Binder 3 – Cost Response</i>			
1	Cash Purchase Response		

Appendix H
Cost Forms: Cash Purchase Response

Appendix H – Cost Forms: Cash Purchase Response

Vendors are required to submit complete cost forms for the cash purchase of each proposed solution. All implementation costs for the entire project from discovery through final acceptance must be identified. The available state funding is limited to \$1,500,000 for the initial investment in the following components:

- Application software.
- System software.
- System hardware.
- Implementation.

Enterprise licenses listed in the cost proposal must apply to all users of the ACCESS solution. ACCESS users include agencies both in and out of the state of Washington, including:

- Local agencies (city and county).
- State agencies.
- Federal agencies.
- Regional consortia.

Please use the following table as a basis for calculating systems maintenance requirements and costs:

All Proposed	Required Maintenance Period	Maintenance Start Date
Hardware	4 years.	Time of purchase.
Systems Software (e.g., operating systems, databases)	4 years.	Time of purchase.

Vendor Software	4 years.	Time of WSP acceptance.
-----------------	----------	-------------------------

See Sections A, B, C, and D. Offerors shall bid a fixed price for these components. Bids exceeding this limit will be rejected as nonresponsive.

A. Application Software Costs

List all application software being proposed, including package cost, customization cost, and annual maintenance expense. The total for this subsection shall agree with the application software total in the Cost Summary subsection. The annual maintenance cost shall represent the average maintenance cost for Years 2–5. The warranty period for the application should begin with final acceptance of the application product. This does not include the installation and development period between contract signing and acceptance. Year 2 is a definite annual support period. Years 3–5 are optional annual support periods.

Application Software Description	Required Quantity	Package Name	Package Cost per License	Total Cost All Licenses	Annual Maintenance Cost
Message Switch Application – Production					
<i>User Interface Product</i>					
Message Switch Application – Development					
Message Switch Application – Test					
Message Switch Application – DR					

Application Software Description	Required Quantity	Package Name	Package Cost per License	Total Cost All Licenses	Annual Maintenance Cost
Interfaces					
TOTAL					

B. System Software Costs

List all system software, including costs and annual maintenance expense. The total from this subsection shall agree with the system software total in the Cost Summary subsection. The annual maintenance cost shall represent the average maintenance cost for Years 2–5. WSP reserves the right to utilize the state's enterprise software licensing or hardware master contracts for the procurement of the new ACCESS solution.

System Software Description	Release/Level	Cost	Annual Maintenance Cost
Production			

System Software Description	Release/Level	Cost	Annual Maintenance Cost
Development			
Test			
DR			
TOTAL			

C. System Hardware Costs

List all hardware required, including purchase costs and annual maintenance expense. The total from this subsection shall agree with the hardware total in the Cost Summary subsection. The annual maintenance cost shall represent the average maintenance cost for Years 2–5. WSP reserves the right to utilize the state's enterprise software licensing or hardware master contracts for the procurement of the new ACCESS solution.

Hardware Component Description	Make/Model, Part Number	Required Quantity	Total Purchase Cost	Annual Maintenance Cost
Production				
Development				
Test				
DR				
TOTAL				

D. Other Implementation Costs

Describe and list all other costs that would be associated with implementation of your system. Costs not identified shall become the responsibility of the vendor.

Conversion (existing electronic records)	\$ _____
Installation	_____
Migration	_____
Integration	_____
DR	_____
Project Management	_____
Training	_____
Documentation	_____
Out-of-Pocket-Expenses (travel, per diem, etc.)	_____
Other (please describe)	_____
_____	_____
TOTAL OTHER IMPLEMENTATION COSTS	\$ _____

E. Hourly Rate for Future Enhancements

During the term of the resulting contract WSP may determine that changes or enhancements are needed to the vendor product. Please refer to Section 57, Updating and Maintaining the Application Product, of the sample contract in APPENDIX I for a description of when time-and-materials work would be appropriate. Please submit an hourly rate for this type of work.

Hourly Rate	\$ _____
-------------	----------

F. Optional Component Costs

By utilizing the forms from Sections A, B, C, and D above, identify any and all costs associated with full implementation and maintenance of optional message switch components. Additional optional components should be included and noted to reflect additional capabilities that can be provided by the vendor, including addressing the following specific issues:

- Transfer of system licensing and code ownership to WSP.
- Business continuity approach.

G. Cost Summary

1. Total Onetime Costs

Provide a summary of all onetime costs for the system you are proposing. Any subtotals carried forward to this page shall agree with the corresponding detail pages.

	<u>Onetime Cost</u>
a. Application Software	\$ _____
b. System Software	_____
c. Hardware	_____
d. Other Implementation Costs	_____
Subtotal	\$ _____
e. Optional Costs:	_____
TOTAL ONETIME COST (INCLUDING OPTIONS) (not to exceed)	\$ _____

2. Annual Recurring Costs

Provide a summary of all recurring costs for the system you are proposing. Any subtotals carried forward to this page shall agree with the corresponding detail pages.

	<u>Annual Cost</u>
Application Software Maintenance	\$ _____
System Software Maintenance	_____
Hardware Maintenance	_____

Other Recurring Costs

TOTAL ANNUAL RECURRING COSTS
(without options)

\$

Total Recurring Costs on Optional Items

System Licensing and Code Ownership

\$

Business Continuity Approach

TOTAL ANNUAL RECURRING COSTS
(with options)

\$

Appendix I
Washington Sample Contract

Appendix I – Washington Sample Contract

This section provides an overview of the state of Washington terms and conditions that will apply to proposals submitted in response to this RFP.



WSP CONTRACT NUMBER _____
for
Message Switch Replacement Project
Between
The Washington State Patrol
And
(Vendor Name)

Table of Contents

1.	Definition and Terminology	7
----	----------------------------------	---

Contract Term

2.	Term	10
3.	Survivorship	10

Pricing, Invoice And Payment

4.	Pricing.....	10
5.	Advance Payment Prohibited	11
6.	Taxes	11
7.	Invoice and Payment	11
8.	Overpayments to Vendor	12

Vendor's Responsibilities

9.	Statement of Work	12
10.	Commencement of Work	13
11.	Ownership/Rights in Data	13
12.	Title to Equipment	14
13.	Shipping and Risk of Loss	14
14.	Equipment Compatibility/Specifications/Configurations.....	14
15.	Delivery	15
16.	Site Security.....	15
17.	Equipment Installation and Set-up	15
18.	Software Installation	16
19.	Standard of Performance and Acceptance.....	16
20.	Equipment Warranty	17
21.	Software Warranty	18
22.	Equipment Maintenance.....	18
23.	Software Upgrades and Enhancements.....	19
24.	Equipment and Maintenance Documentation	20
25.	Software Maintenance and Support Services.....	20
26.	Spare Parts for Equipment.....	21
27.	Vendor Commitments, Warranties and Representations	22
28.	Compliance with Standards	22
29.	Training.....	22
30.	Minority and Women's Business Enterprise (MWBE) Participation.....	22
31.	Protection of Purchaser's Confidential Information	22

Software License

32.	License Grant.....	23
33.	Software Ownership.....	24
34.	Software Code Escrow	24

35.	<i>Software Specifications</i>	26
36.	<i>Compliance with Standards</i>	26
37.	<i>Date Warranty.....</i>	26
38.	<i>Physical Media Warranty</i>	26
39.	<i>No Surreptitious Code Warranty</i>	27
40.	<i>Reauthorization Code.....</i>	27
41.	<i>Software Documentation.....</i>	27

Contract Administration

42.	<i>Legal Notices.....</i>	28
43.	<i>Vendor Contract Administration.....</i>	28
44.	<i>WSP Contract Administration.....</i>	29
45.	<i>Notification of Change to Personnel.....</i>	29
46.	<i>Section Headings, Incorporated Documents and Order of Precedence</i>	29
47.	<i>Entire Agreement</i>	30
48.	<i>Authority for Modifications and Amendments</i>	30
49.	<i>Independent Status of Vendor</i>	30
50.	<i>Governing Law.....</i>	30
51.	<i>Subcontractors</i>	30
52.	<i>Assignment</i>	31
53.	<i>Publicity</i>	31
54.	<i>Review of Vendor's Records</i>	31
55.	<i>Right of Inspection</i>	32
56.	<i>Participation in Purchaser's Quality Assurance Monitoring Programs</i>	32
57.	<i>Updating and Maintaining the Application Product.....</i>	32

General Provisions

58.	<i>Patent and Copyright Indemnification.....</i>	33
59.	<i>Save Harmless.....</i>	34
60.	<i>Insurance.....</i>	34
61.	<i>Industrial Insurance Coverage</i>	35
62.	<i>Licensing Standards.....</i>	35
63.	<i>OSHA/WISHA</i>	35
64.	<i>Uniform Commercial Code (UCC) Applicability.....</i>	36
65.	<i>Antitrust Violations</i>	36
66.	<i>Compliance with Civil Rights Laws</i>	36
67.	<i>Severability.....</i>	36
68.	<i>Waiver</i>	36
69.	<i>Treatment of Assets</i>	36
70.	<i>Vendor's Proprietary Information</i>	37

Disputes and Remedies

71.	<i>Disputes.....</i>	37
72.	<i>Attorneys' Fees and Costs.....</i>	38

73.	<i>Non-Exclusive Remedies</i>	38
74.	<i>Liquidated Damages</i>	38
75.	<i>Failure to Perform</i>	39
76.	<i>Limitation of Liability</i>	39

Contract Termination

77.	<i>Termination for Default</i>	40
78.	<i>Termination for Convenience.....</i>	40
79.	<i>Termination for Withdrawal of Authority</i>	40
80.	<i>Termination for Non-Allocation of Funds.....</i>	40
81.	<i>Termination for Conflict of Interest</i>	41
82.	<i>Termination Procedure</i>	41
83.	<i>Covenant Against Contingent Fees.....</i>	41

Contract Execution

84.	<i>Authority to Bind</i>	42
85.	<i>Counterparts</i>	42

Exhibits

Exhibit A: *[Purchaser] Request for [Proposal/Quotation/Qualifications and Quotation] for
[describe acquisition]*

Exhibit B: *Vendor's Response*

SCHEDULE E	53
Problem Report/Change Request Process.....	53

WSP CONTRACT NUMBER _____

for

Message Switch Contract

PARTIES

This Contract ("Contract") is entered into by and between the state of Washington, acting by and through Washington State Patrol, an agency of Washington State government ("WSP" or "WSP") located at PO Box 42602, Olympia WA 98504-2602; and the XXXXX, for the purpose of purchasing Equipment, Software licenses and related services for the Message Switch Replacement Project and Services

RECITALS

The State of Washington, acting by and through WSP, issued a Request For Proposals (RFP) No. _____ for the purpose of purchasing Equipment, Software licenses and related services for the Message Switch. This RFP is incorporated into this Contract as Exhibit A, RFP No. _____, as amended.

The Vendor submitted a timely Response to the RFP. This response is incorporated into this Contract as Exhibit B, Vendor's Proposal.

WSP evaluated all properly submitted Responses to the above-referenced RFP and has identified the Vendor as the apparently successful Vendor.

WHEREAS WSP has determined that entering into a contract with the Vendor will meet WSP's needs and will be in the best interest to the citizens of Washington State;

NOW THEREFORE, WSP awards to the Vendor this Contract, the terms and conditions of which shall govern Vendor's furnishing to WSP Equipment, Software licenses and related services. This Contract is not for personal use.

IN CONSIDERATION of the mutual promises as hereinafter set forth, the parties agree as follows:

1. Definition and Terminology

The following terms as used throughout this Contract shall have the meanings set forth below.

"Acceptance" shall mean that the Software has passed its Acceptance Testing and shall be formalized in a written notice from Purchaser to Vendor.

"Acceptance Date" shall mean the date Vendor delivers the Products.

"Business Days and Hours" shall mean Monday through Friday, 8:00 a.m. to 5:00 p.m., Pacific Time, except for holidays observed by the state of Washington.

"Concurrent User" shall mean the number of users accessing each separate module of the Software at the same time.

"Confidential Information" shall mean information that may be exempt from disclosure to the public or other unauthorized persons under either chapter 42.56 RCW or other state or federal statutes. Confidential Information includes, but is not limited to, names, addresses, Social Security numbers, e-mail addresses, telephone numbers, financial profiles, credit card information, driver's license numbers, medical data, law enforcement records, agency source code or object code, agency security data, or information identifiable to an individual that relates to any of these types of information.

“Contract” shall mean this document, all schedules and exhibits, and all amendments hereto.

“Delivery Date” shall mean the date by which the Products ordered hereunder must be delivered.

“Effective Date” shall mean the first date this Contract is in full force and effect. It may be a specific date agreed to by the parties; or, if not so specified, the date of the last signature of a party to this Contract.

“Equipment” shall mean the Equipment supplied by the Vendor and associated installation hardware as set forth in this Contract.

Exhibit A shall mean WSP Request for Proposals _____ dated February 2, 2009 as amended by Amendment 1 dated February 20, 2009; and Amendment 2 dated March 9, 2009.

“Exhibit B” shall mean the Vendor’s Proposal dated March 20, 2009 as amended by Vendor’s response to WSP’s Questions dated May 8, 2009; and Vendor’s Best And Final Offer documents dated June 12, 2009

“Help Desk” shall mean a service provided by Vendor for the support of Vendor’s Products. Purchaser shall report warranty or maintenance problems to Vendor’s Help Desk for initial troubleshooting and possible resolution of the problems or for the initiation of repair or replacement services.

“Installation Date” shall mean the date by which all Equipment and Software ordered hereunder shall be in place, in good working order.

“License” shall mean the rights granted to Purchaser to use the Software that is the subject of this Contract.

“Order” or “Order Document” shall mean any official document and attachments thereto specifying the Equipment, Software and/or Services to be licensed or purchased from Vendor under this Contract.

“Price” shall mean charges, costs, rates, and/or fees charged for the Products and Services under this Contract and shall be paid in United States dollars.

“Product(s)” shall mean any Vendor-supplied Equipment, Software, and documentation.

“Proprietary Information” shall mean information owned by Vendor to which Vendor claims a protectable interest under law. Proprietary Information includes, but is not limited to, information protected by copyright, patent, trademark, or trade secret laws.

“Purchaser” shall mean the State of Washington, Washington State Patrol (WSP) or an organization authorized by WSP to purchase Products and Services under this Contract.

“RCW” shall mean the Revised Code of Washington.

“Schedule A” shall mean the Authorized Product and Price List.

“Schedule B” shall mean the Acceptance Test Plan, which will be developed for incorporation into this Contract at a later date.

“Schedule C” shall mean the Sample Software Escrow Agreement.

“Schedule D” shall mean the Nondisclosure Agreement.

“Services” shall mean those Services provided under this Contract and related to the Hardware and Software License(s) being purchased that are appropriate to the scope of this Contract and includes such things as installation Services, maintenance, training, etc.

“Software” shall mean the object code version of the Omnixx Enterprise platform application and

associated modules identified in Schedule A, licensed pursuant to this Contract. Embedded code, firmware, internal code, microcode, and any other term referring to software residing in the Equipment that is necessary for the proper operation of the Equipment is not included in this definition of Software. Software includes all current, and future versions of the Software and all maintenance updates and error corrections, provided the service and maintenance terms of this Contract are in force.

“Specifications” shall mean the technical and other specifications set forth in RFP No. _____, Schedule A, and the specifications set forth in Vendor’s Product documentation, whether or not Vendor produces such documentation before or after this Contract’s Effective Date.

“Standard of Performance” shall mean the criteria that must be met before Hardware and Software Acceptance, as set forth in the section titled Standard of Performance and Acceptance. The Standard of Performance also applies to all additional, replacement or substitute Hardware and Software; and Software that is modified by or with the written approval of Vendor after having been accepted.

“Subcontractor” shall mean one not in the employment of Vendor, who is performing all or part of the business activities under this Contract under a separate contract with Vendor. The term “Subcontractor” means Subcontractor(s) of any tier.

“Vendor” shall mean the XXX, its employees and agents. Vendor also includes any firm, provider, organization, individual, or other entity performing the business activities under this Contract. It shall also include any Subcontractor retained by Vendor as permitted under the terms of this Contract.

“Vendor Account Manager” shall mean a representative of Vendor who is assigned after Acceptance as the primary contact person whom the WSP System Manager shall work with for the duration of this Contract and as further defined in the section titled Vendor Account Manager.

“Vendor Contracting Officer” shall mean the person to whom signature authority has been delegated in writing. This term includes, except as otherwise provided in this Contract, an authorized representative of Vendor Contracting Officer acting within the limits of his/her authority.

“Vendor Project Manager” shall mean the person designated by XXX who is assigned as the primary contact person whom WSP’s Project Manager shall work with through Acceptance. The role is further specified in the section titled “XXX Project Manager”.

“WSP” shall mean the state of Washington, Washington State Patrol, any division, section, office, unit or other entity of WSP or any of the officers or other officials lawfully representing WSP.

“WSP System Manager” shall mean the person designated by WSP who is assigned as the primary contact person whom Vendor’s representatives shall work with and as further defined in the section titled WSP System Manager.

“WSP Contract Manager” shall mean the person designated by WSP to administer this Contract on behalf of WSP for legal processes.

“WSP Contracting Officer” shall mean the Chief of the Washington State Patrol, or the person to whom signature authority has been delegated in writing. This term includes, except as otherwise provided in this Contract, an authorized representative of WSP Contracting Officer acting within the limits of his/her authority.

Contract Term

2. Term

2.1. Equipment and Software License Purchases

- a) This Contract's initial Equipment and Software purchase term shall be 24 months, commencing upon the Effective Date.

2.2. Equipment and Software Maintenance

- a) This Contract's initial Equipment and Software maintenance term shall be one (1) year, commencing the day following expiration of the Equipment's and Software's warranty.
- b) This Contract's Equipment and Software maintenance term shall be automatically extended for three additional one (1) year terms unless Purchaser terminates by giving written notice of its decision not to extend to Vendor not less than thirty (30) calendar days prior to the then-current Contract term's expiration. No change in terms and conditions shall be permitted during these extensions unless specifically agreed to in writing.

3. Survivorship

All purchase transactions executed pursuant to the authority of this Contract shall be bound by all of the terms, conditions, Prices and Price discounts set forth herein, notwithstanding the expiration of the initial term of this Contract or any extension thereof. Further, the terms, conditions and warranties contained in this Contract that by their sense and context are intended to survive the completion of the performance, cancellation or termination of this Contract shall so survive. In addition, the terms of the sections titled **Overpayments to Vendor; Vendor Commitments, Warranties and Representations; Protection of Purchaser's Confidential Information; License Grant; Software Ownership; Title to Equipment; Ownership/Rights in Data; Date Warranty; No Surreptitious Code Warranty; Section Headings, Incorporated Documents and Order of Precedence; Publicity; Review of Vendor's Records; Patent and Copyright Indemnification; Vendor's Proprietary Information; Disputes; and Limitation of Liability**, shall survive the termination of this Contract.

Pricing, Invoice and Payment Pricing

4. Pricing

- 4.1. Vendor agrees to provide the Products and Services at the Prices set forth in Schedule A. No other Prices shall be payable to Vendor.
- 4.2. Maintenance and support fees - Upon expiration of Vendor-provided warranty as set forth in the sections titled **Equipment Warranty** and **Software Warranty**, and upon election by Purchaser to receive maintenance and support services from Vendor, Purchaser shall pay maintenance and support fees to Vendor at the Prices set forth in Schedule A.
- 4.3. Prices may not be increased during the initial term of the Contract.
- 4.4. If Vendor reduces its Prices for any of the Equipment or Services during the term of this Contract, Purchaser shall have the immediate benefit of such lower Prices for new purchases. Vendor shall send notice to the Purchaser Contract Administrator with the reduced Prices within fifteen (15) Business Days of the reduction taking effect.

- 4.5. At least one hundred twenty (120) calendar days before the end of the then-current term of this Contract, Vendor may propose purchase Price and maintenance and support (service) rate increases by written notice to Purchaser Contract Administrator. Price adjustments will be taken into consideration by Purchaser Contract Administrator when determining whether to extend this Contract.
- 4.6. Vendor agrees all the Prices, terms, warranties, and benefits provided in this Contract are comparable to or better than the terms presently being offered by Vendor to any other governmental entity purchasing the same quantity under similar terms. If during the term of this Contract Vendor shall enter into contracts with any other governmental entity providing greater benefits or more favorable terms than those provided by this Contract, Vendor shall be obligated to provide the same to Purchaser for subsequent purchases.

5. Advance Payment Prohibited

No advance payment shall be made for the Products and Services furnished by Vendor pursuant to this Contract. Notwithstanding the above, maintenance payments, if any, may be made on a quarterly basis at the beginning of each quarter.”

6. Taxes

- 6.1. Purchaser will pay sales and use taxes, if any, imposed on the Products and Services acquired hereunder. Vendor must pay all other taxes including, but not limited to, Washington Business and Occupation Tax, other taxes based on Vendor’s income or gross receipts, or personal property taxes levied or assessed on Vendor’s personal property. Purchaser, as an agency of Washington State government, is exempt from property tax.
- 6.2. Vendor shall complete registration with the Washington State Department of Revenue and be responsible for payment of all taxes due on payments made under this Contract.

7. Invoice and Payment

- 7.1. Vendor will submit properly itemized invoices to the Purchaser’s System Manager. Invoices shall provide and itemize, as applicable:
- a) Purchaser Contract number _____.
 - b) Vendor name, address, phone number, and Federal Tax Identification Number;
 - c) Description of Products, including quantity ordered, model and serial numbers;
 - d) Date(s) of delivery and/or date(s) of installation and set up;
 - e) Price for each item, or Vendor’s list Price for each item and applicable discounts;
 - f) Maintenance charges;
 - g) Net invoice Price for each item;
 - h) Applicable taxes;
 - i) Shipping costs;
 - j) Other applicable charges;
 - k) Total invoice Price; and
 - l) Payment terms including any available prompt payment discounts.
 - m) All invoices shall be sequentially numbered regardless of purpose beginning with one (1).
 - n) Invoices are sent to the address listed in Appendix A.

- 7.2. Payments shall be due and payable within thirty (30) calendar days after receipt and Acceptance of Products or Services or thirty (30) calendar days after receipt of properly prepared invoices, whichever is later.
- 7.3. Purchaser shall pay maintenance and support charges on a quarterly basis, in advance. Payment of maintenance service/support of less than one (1) month's duration shall be prorated at 1/30th of the basic monthly maintenance charges for each calendar day.
- 7.4. Incorrect or incomplete invoices will be returned by Purchaser to Vendor for correction and reissue.
- 7.5. The Purchaser Contract number _____ must appear on all bills of lading, packages, and correspondence relating to this Contract.
- 7.6. Purchaser shall not honor drafts, nor accept goods on a sight draft basis.
- 7.7. If Purchaser fails to make timely payment, Vendor may invoice Purchaser one percent (1%) per month on the amount overdue or a minimum of one dollar (\$1). Payment will not be considered late if payment is deposited electronically in Vendor's bank account or if a check or warrant is postmarked within thirty (30) calendar days of Acceptance of the Equipment or receipt of Vendor's properly prepared invoice, whichever is later.

8. Overpayments to Vendor

Vendor shall refund to Purchaser the full amount of any erroneous payment or overpayment under this Contract within thirty (30) days' written notice. If Vendor fails to make timely refund, Purchaser may charge Vendor one percent (1%) per month on the amount due, until paid in full.

Vendor's Responsibilities

9. Statement of Work

- 9.1. All Services shall be performed pursuant to the terms of this Contract and shall be documented in a Statement of Work (SOW) established between Purchaser and Vendor. The SOW shall at a minimum:
- a) Reference this Contract number _____;
 - b) Define project or task objectives;
 - c) Describe the scope of Services or work to be performed;
 - d) Identify deliverables;
 - e) Specify a timeline and period of performance;
 - f) Specify compensation and payment, e.g., the hourly rate and total Vendor hours to be provided or the fixed price for a deliverable (whichever is applicable), total cost of the project, and reimbursable Vendor expenses;
 - g) Describe Vendor's roles and responsibilities and identify specific Vendor staff;
 - h) Describe Purchaser's roles and responsibilities;
 - i) Identify the acceptance criteria for the deliverables;
 - j) Provide signature block for both parties.
- 9.2. The first SOW will address the discovery phase in which the Contractor will examine a number of application, architecture, and security requirements associated with the project and make recommendations for the final future ACCESS environment. The Contractor will also produce an initial project work plan and schedule depicting tasks from initiation through completion of the project. This document shall serve as the

basis for subsequent work orders. There is no guarantee that future SOWs will be issued beyond the initial discovery phase.

9.3. Subsequent SOWs shall govern, at a minimum, production of the following deliverables:

- a) System Design document
- b) Data Conversion Plan document (if necessary)
- c) Test Plan document
- d) Implementation Plan document
- e) Training Plan document
- f) All application software to implement the system as designed
- g) All system software necessary to implement the system as designed
- h) All hardware components necessary to implement the system as designed
- i) Installation and configuration of all hardware and system software to implement the system as designed
- j) Configuration of application software to implement the system as designed
- k) Provide training to WSP staff as identified in the Training Plan
- l) System documentation
- m) Data conversion as identified in the Data Conversion Plan (if necessary)
- n) System test support
- o) Production cut-over support
- p) Maintenance and support

9.4. The terms and conditions of any SOW cannot conflict with the terms and conditions of this Contract. In the event of any conflict, the Contract shall prevail.

10. Commencement of Work

No work shall be performed by Vendor until an SOW is executed by Vendor and Purchaser and is received by Vendor.

11. Ownership/Rights in Data

- 11.1. Purchaser and Vendor agree that all data and work products (collectively called "Work Product") produced pursuant to this Contract shall be considered work made for hire under the U.S. Copyright Act, 17 U.S.C. §101 *et seq*, and shall be owned by Purchaser. Vendor is hereby commissioned to create the Work Product. Work Product includes, but is not limited to, discoveries, formulae, ideas, improvements, inventions, methods, models, processes, techniques, findings, conclusions, recommendations, reports, designs, plans, diagrams, drawings, Software, databases, documents, pamphlets, advertisements, books, magazines, surveys, studies, computer programs, films, tapes, and/or sound reproductions, to the extent provided by law. Ownership includes the right to copyright, patent, register and the ability to transfer these rights and all information used to formulate such Work Product.
- 11.2. If for any reason the Work Product would not be considered a work made for hire under applicable law, Vendor assigns and transfers to Purchaser the entire right, title and interest in and to all rights in the Work Product and any registrations and copyright applications relating thereto and any renewals and extensions thereof.
- 11.3. Vendor shall execute all documents and perform such other proper acts as Purchaser may deem necessary to secure for Purchaser the rights pursuant to this section.
- 11.4. Vendor shall not use or in any manner disseminate any Work Product to any third party, or represent in any way Vendor ownership in any Work Product, without the prior

written permission of Purchaser. Vendor shall take all reasonable steps necessary to ensure that its agents, employees, or Subcontractors shall not copy or disclose, transmit or perform any Work Product or any portion thereof, in any form, to any third party.

- 11.5. Material that is delivered under this Contract, but that does not originate therefrom ("Preexisting Material"), shall be transferred to Purchaser with a nonexclusive, royalty-free, irrevocable license to publish, translate, reproduce, deliver, perform, display, and dispose of such Preexisting Material, and to authorize others to do so except that such license shall be limited to the extent to which Vendor has a right to grant such a license. Vendor shall exert all reasonable effort to advise Purchaser at the time of delivery of Preexisting Material furnished under this Contract, of all known or potential infringements of publicity, privacy or of intellectual property contained therein and of any portion of such document which was not produced in the performance of this Contract. Vendor agrees to obtain, at its own expense, express written consent of the copyright holder for the inclusion of Preexisting Material. Purchaser shall receive prompt written notice of each notice or claim of copyright infringement or infringement of other intellectual property right worldwide received by Vendor with respect to any Preexisting Material delivered under this Contract. Purchaser shall have the right to modify or remove any restrictive markings placed upon the Preexisting Material by Vendor.

12. Title to Equipment

Upon successful completion of Acceptance Testing and receipt of Purchaser's letter of Acceptance and receipt of payment by Vendor, Vendor shall convey to Purchaser good title to the Equipment free and clear of all liens, pledges, mortgages, encumbrances, or other security interests.

Transfer of title to the Equipment shall include an irrevocable, fully paid-up, perpetual license to use the internal code (embedded software) in the Equipment. If Purchaser subsequently transfers title to the Equipment to another entity, Purchaser shall have the right to transfer the license to use the internal code with the transfer of Equipment title. A subsequent transfer of this software license shall be at no additional cost or charge to either Purchaser or Purchaser's transferee.

13. Shipping and Risk of Loss

Vendor shall ship all Products purchased pursuant to this Contract, freight prepaid, FOB Purchaser's destination. The method of shipment shall be consistent with the nature of the Products and hazards of transportation. Regardless of FOB point, Vendor agrees to bear all risks of loss, damage, or destruction of the Products ordered hereunder that occurs prior to Delivery except loss or damage attributable to Purchaser's fault or negligence; and such loss, damage, or destruction shall not release Vendor from any obligation hereunder. After Delivery the risk of loss or damage shall be borne by Purchaser, except loss or damage attributable to Vendor's fault or negligence.

14. Equipment Compatibility/Specifications/Configurations

- 14.1. Vendor shall notify Purchaser of the existence of any compatibility issues between Vendor's Equipment and Purchaser's already existing or planned for hardware, software, and cabling. Purchaser will provide Vendor timely access to necessary areas and Equipment sites and shall provide Vendor with a list of any existing or planned for hardware, software, and cabling, as necessary.
- 14.2. Vendor warrants that each item of Equipment delivered hereunder will conform to that item's detailed Specifications in all respects including, but not limited to: physical characteristics, operating characteristics, space requirements, power requirements,

maintenance or warranty characteristics, modularity, compatibility, and the like, as may be modified in writing and agreed to by the parties.

- 14.3. For the purpose of delivery and performance under this Contract, Equipment purchased hereunder shall be grouped together in one or more Equipment, firmware, and/or software configurations as set forth in Vendor's Response. Any such configuration shall be deemed incomplete and undelivered if any item of Equipment within that configuration has not been delivered, or if delivered, not installed or operational in accordance with this Contract's **Delivery** and **Installation and Set-Up** sections.
- 14.4. Purchaser shall have the right to connect the Equipment purchased hereunder to any equipment manufactured or supplied by others including other computers, peripheral equipment, terminal devices, communications equipment, software and the like that interface with the Equipment purchased hereunder.
- 14.5. If requested by Purchaser, Vendor agrees to identify, on all items of Equipment supplied under this Contract, all appropriate test points for connecting commercially available equipment monitors designed to measure system capacity, performance, or activity.

15. Delivery

- 15.1. Vendor shall deliver the Products ordered pursuant to this Contract on or before the Delivery Date(s) identified in the Statements of Work. For any exception to this Delivery Date, Vendor must notify Purchaser and obtain prior approval in writing. Time is of the essence with respect to delivery and Vendor may be subject to liquidated damages and/or termination of an Order or of this Contract and/or other damages available under law for failure to deliver on time. Purchaser has the right to extend the Delivery Date of a Statement of Work at its own discretion.
- 15.2. All deliveries made pursuant to this Contract must be complete. Unless Vendor has obtained prior written approval from Purchaser, which shall not be withheld unreasonably, incomplete deliveries or backorders will not be accepted. All packages must be accompanied by a packing slip that identifies all items included with the shipment and the Purchaser's Order Document number. Vendor's delivery receipt must be signed by an authorized representative of Purchaser for all deliveries made hereunder.

16. Site Security

While on Purchaser's premises, Vendor, its agents, employees, or Subcontractors shall conform in all respects with physical, fire, or other security regulations.

17. Equipment Installation and Set-up

- 17.1. Purchaser shall prepare the environment to house the Equipment based upon written requirements provided by Vendor in its Response, as modified in writing and agreed to by the parties. Vendor's specialists shall be available to provide required consultation related to environment preparation at no extra cost to Purchaser apart from the costs presented in Vendor's Response. Any requirements for the environment not disclosed in Vendor's Response will be completed by Vendor at no additional cost to Purchaser.
- 17.2. Vendor is hereby notified that fiber optic, communications, control systems, and other types of cable (collectively called "cabling") may be located within Purchaser's grounds and facilities.

- 17.3. Before beginning work on or about Purchaser's premises, Vendor shall contact the Purchaser to determine if Purchaser's cabling systems will be impacted and to make necessary arrangements. Prior to the commencement of any work that may impact underground utilities not owned by Purchaser, Vendor agrees to notify affected owners under the requirements of chapter 19.22 RCW, Underground Utilities.
- 17.4. Purchaser hereby permits Vendor to interface with such cabling and design engineering systems in support of the delivery of the Products and Services ordered under this Contract.
- 17.5. Vendor shall install the Equipment, ready for Acceptance Testing, on or before the Installation Date(s) specified in Statements of Work. Failure to meet the Installation Date(s) may subject Vendor to liquidated damages and/or termination of an Order or of this Contract and other damages available under law, unless such failure is caused by acts or omissions of Purchaser.
- 17.6. After installing the Equipment, Vendor shall provide Purchaser with documentation of a successful system audit, performed at Purchaser's installation site using Vendor's diagnostic routines, as approved by Purchaser, that demonstrates that the Equipment meets or exceeds the Specifications. Vendor shall certify to Purchaser in writing that the Equipment is ready for Acceptance Testing. If after reviewing such documentation Purchaser agrees that the Equipment is ready for Acceptance Testing, Purchaser shall begin Acceptance Testing, as set forth in the section titled **Standard of Performance and Acceptance**.

18. Software Installation

Vendor shall install the Software on Purchaser's designated equipment in accordance with applicable industry standards.

19. Standard of Performance and Acceptance

- 19.1. The Purchaser and the Vendor shall negotiate an Acceptance Test Plan that shall be incorporated into this Contract as Schedule B through a mutually agreed upon amendment to this Contract. The Standard of Performance stated in the Acceptance Test Plan is also applicable to any additional, replacement, or substitute Product and any Product that is modified by or with the written approval of Vendor after having been Accepted.
- 19.2. The Effectiveness Level for a Product is the percentage of time in a month that the Product is functioning properly in accordance with its Specifications. The Effectiveness Level is determined by dividing the Operational Use Time of the Product by the sum of the Operational Use Time plus the Product Failure downtime, all of which shall be measured in hours and whole minutes. Operational Use Time for a Product is defined as the total time the Product would normally be used. Product Failure downtime is defined as the accumulated time during Operational Use time when work cannot be processed or accurately completed because of a Product Failure. Product Failure is defined as a malfunction in the Equipment or Software that prevents the accomplishment of the intended function(s) of the Product.
- 19.3. Downtime for each incident shall start from the time that Vendor knew or reasonably should have known of the Product Failure, or Purchaser makes a bona fide attempt to contact Vendor's designated representative at the prearranged contact point, whichever occurs earlier, until the Product is returned to fully operational status in conformance with its Specifications. During periods of Product Failure downtime, Purchaser may use operable Products when such action does not interfere with repair of the inoperable Product.

- 19.4. No Product shall be accepted and no charges shall be paid until this Standard of Performance is met. The date of Acceptance shall be the first Purchaser Business Day following the successful Acceptance Testing period and shall be formalized in a notice of Acceptance from Purchaser to Vendor.
- 19.5. Final Acceptance. Final acceptance of the vendor product consists of functional testing and performance testing. Functional acceptance testing will validate that the vendor product successfully performs all functions as identified in the System Design document which will be developed during the design phase of the project. Functional acceptance criteria and testing procedures will be identified in a mutually agreed upon System Test Plan.
- Performance testing will be conducted for 30 calendar days after production cutover when all live production transactions are being processed by the replacement system. Performance acceptance testing will validate that the vendor product processes production-level volumes of transactions at agreed upon response times and that system reliability meets the 99.999% up-time level required in the RFP. System functionality will also be monitored during this time. Performance acceptance criteria and testing procedures will be identified in a mutually agreed upon System Test Plan.
- WSP shall retain a minimum of 20% of onetime costs for payment upon final acceptance excluding Equipment.
- 19.6. Monthly Performance Monitoring. Throughout the warranty period and the initial and subsequent maintenance terms of this Contract, Purchaser shall monitor the Product to ensure that it conforms to the Standard of Performance established in the Acceptance Test Plan. Should the Product fail to operate in conformance with the Standard of Performance for any thirty (30) calendar days period, Vendor shall take corrective action as directed by Purchaser and, if the Product is Equipment, credit Purchaser a portion of the maintenance fees paid as provided in the **Equipment Maintenance** and **Software Maintenance and Support** sections.

20. Equipment Warranty

- 20.1. Vendor warrants that the Equipment shall be in good operating condition and shall conform to the Specifications for a period of one (1) year, the Equipment Warranty Period, commencing upon the first day after delivery.
- 20.2. During the Equipment Warranty Period, Vendor shall adjust, repair, or replace all Equipment that is defective or not performing in conformance with the Specifications. All costs for such adjustments, repairs, or replacements, including all costs for replacing parts or units and their installation and any transportation and delivery fees, shall be at Vendor's expense. Any defective Equipment shall be repaired or replaced for Purchaser so that it conforms to the Specifications.
- 20.3. Vendor agrees that all warranty service provided hereunder shall be performed by manufacturer-trained, certified, and authorized technicians. Vendor further agrees to act as the sole point of contact for warranty service. Vendor warrants that it has or will obtain and pass through to Purchaser any and all warranties obtained or available from the Original Equipment Manufacturer (OEM), including any replacement, upgraded, or additional Equipment warranties.
- 20.4. Vendor shall provide Help Desk Services for reporting warranty issues and for troubleshooting problems. Vendor's Help Desk Services shall be accessible via e-mail or via one or more toll-free telephone lines.

- 20.5. Vendor shall provide escalation procedures to ensure that the proper level of attention and resources are directed towards resolution of Products and Services problems in a timely manner. The escalation procedures shall indicate the steps to be taken in response to a problem report, the contact information and title of Vendor's employee(s) responding at each level and the elapsed time before the next level of response is invoked. In addition, Vendor shall provide a copy of its disaster recovery plan for managing crisis situations in order to help avoid or reduce the potential adverse affects of catastrophic events (e.g., floods, fires, earthquakes, fuel/gas leaks rendering a building unuseable, etc.).
- 20.6. Purchaser agrees that Vendor will not be liable for any damages caused by the Purchaser's actions or failure of Purchaser to fulfill any of its responsibilities for site installation.
- 20.7. THE WARRANTIES IN THIS CONTRACT REPLACE ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING ANY WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE.

21. Software Warranty

Vendor warrants that the Software shall be in good operating condition and shall conform to the Specifications for a period of one (1) year, the Software Warranty Period. The Software Warranty Period begins the first day after the Acceptance Date. Vendor shall replace all Software that is defective or not performing in accordance with the Specifications, at Vendor's sole expense.

22. Equipment Maintenance

At the expiration of the Warranty Period set forth in the section titled **Equipment Warranty**, Vendor shall provide maintenance services for the Equipment as described herein, at the Prices set forth on Schedule A.

- 22.1. Vendor shall keep the Equipment in good operating condition or restore it to good working order in accordance with the Specifications or, upon Purchaser's prior written approval, to current standards.
- 22.2. Vendor shall provide contracted maintenance support twenty-four (24) hours per day, seven (7) days per week, every day of the year /including all Purchaser and Vendor recognized holidays.
- 22.3. Purchaser shall provide Vendor physical access to the Equipment to perform maintenance service. Remote access will be provided in accordance with security policies, standards, and guidelines of WSP and the State of Washington. WSP will pay for equipment and/or services to other provisioning vendors needed in Washington.
- 22.4. Preventive Maintenance. Vendor shall specify in writing the number of hours each Equipment item requires per month for preventive maintenance and the frequency and duration of such preventive maintenance. From this Vendor-supplied information Purchaser shall develop and provide to Vendor in writing the schedule within which Vendor shall provide preventive maintenance. This schedule may be modified as agreed in writing. In addition, preventive maintenance may be performed at a time convenient to Purchaser within or contiguous with remedial maintenance.
- 22.5. Remedial maintenance. On site remedial maintenance shall be performed within four (4) hours after notification that Equipment is malfunctioning or inoperative. Vendor shall provide Purchaser with a designated point of contact and shall provide Help Desk services as set forth in the section titled **Equipment Warranty**.

- 22.6. Upon completion of each maintenance call, Vendor shall furnish a maintenance activity report to Purchaser, which shall include, as a minimum, the following:
- a) Date and time notified;
 - b) Date and time of arrival;
 - c) Type and serial number(s) of machine(s);
 - d) Time spent for repair;
 - e) Description of malfunction;
 - f) List of parts replaced; and
 - g) Additional charges, if applicable.
- 22.7. There shall be no additional maintenance charges for:
- a) Replacement parts;
 - b) Preventive maintenance, regardless of when performed;
 - c) Remedial maintenance required within a forty-eight (48) hour period due to recurrence of the same malfunction;
 - d) Time spent by maintenance personnel after arrival at the site awaiting the arrival of additional maintenance personnel and/or delivery of parts, tools or other required material; or
 - e) Remedial maintenance required when the scheduled preventive maintenance preceding the malfunction has not been performed.
- 22.8. Malfunctioning Equipment must be repaired or a replacement spare installed by Vendor's qualified field engineer no later than the close of business on the Business Day following notification of Equipment malfunction. Failure of Vendor to comply with this requirement shall be a Failure to Perform.
- 22.9. Guaranteed Response Time
- a) For the term of maintenance service contracted for herein, Vendor shall provide Purchaser with a guaranteed four (4) hour maintenance response time for the Equipment purchased hereunder. Within four (4) hours after notification by Purchaser that Purchaser is experiencing Equipment problem(s), Vendor's qualified field engineer shall arrive at Purchaser's location to correct such problem. This guaranteed four (4) hour response service shall be available to Purchaser twenty-four (24) hours per day, seven (7) days per week, every day of the year including all Purchaser and Vendor recognized holidays.
 - b) If Vendor's maintenance personnel fail to arrive at Purchaser's installation site within four (4) hours, Vendor shall be assessed liquidated damages, as set forth in the subsection of this Contract titled **Liquidated Damages – Specific**, for each "late" hour or part thereof (prorated in whole minutes) beginning with the time of notification and ending with the time of arrival.
- 22.10. Local Support
- For project phases prior to Final Acceptance, the Vendor will provide personnel onsite as necessary or mutually agreed upon. Following Final Acceptance, the Vendor will provide at least one person for field maintenance support from the Thurston County area.

23. Software Upgrades and Enhancements

Vendor shall:

- 23.1. Supply, under a current Software and Hardware maintenance agreement, updated versions of the Software to operate on upgraded versions of operating systems, upgraded versions of firmware, or upgraded versions of hardware pending Vendor certification;
- 23.2. Supply at no additional cost updated versions of the Software that encompass improvements, extensions, maintenance updates, error corrections, or other changes that are logical improvements or extensions of the original Software supplied to Purchaser; and
- 23.3. Supply at no additional cost interface modules that are developed by Vendor for interfacing the Software to other Software products as specified in the RFP and RFP responses. Any interface not listed will be negotiated as a new statement of work with its own fee and time schedule.

24. Equipment and Maintenance Documentation

Vendor shall provide two (2) complete sets of documentation for each Equipment Order, including technical, electrical, maintenance, and installation information and will provide updated documentation for the term of this Contract. There shall be no additional charge for this documentation or the updates, in whatever form provided. Vendor's Equipment documentation shall be comprehensive, well-structured, and indexed for easy reference. If Vendor maintains its technical, electrical, maintenance and installation documentation on a web site, Vendor may fulfill the obligations set forth in this section by providing Purchaser access to its web-based documentation information. Vendor may also provide such information on CD-ROM. Vendor grants Purchaser the right to make derivative works, update, modify, copy or otherwise reproduce the documentation furnished pursuant to this section at no additional charge excluding other party software.

25. Software Maintenance and Support Services

As a deliverable under a current maintenance contract, Vendor shall provide a replacement copy or correction service at no additional cost to Purchaser for any error, malfunction, or defect in Software that, when used as delivered, fails to perform in accordance with the Specifications and that Purchaser shall bring to Vendor's attention. Vendor shall undertake such correction service as set forth below and shall use its best efforts to make corrections in a manner that is mutually beneficial. Vendor shall disclose all known defects and their detours or workarounds to Purchaser.

In addition, Vendor shall provide the following Services:

- 25.1. Help Desk Services. Vendor shall provide Help Desk Services for reporting errors and malfunctions and trouble shooting problems. Vendor's Help Desk Services shall be web-based and accessible by toll-free telephone lines and/or via e-mail. Vendor's Help Desk Services shall include but are not limited to the following Services:
 - a) Assistance related to questions on the use of the subject Software;
 - b) Assistance in identifying and determining the causes of suspected errors or malfunctions in the Software;
 - c) Advice on detours or workarounds for identified errors or malfunctions, where reasonably available;
 - d) Information on errors previously identified by Purchaser and reported to Vendor and detours to these where available; and
 - e) Advice on the completion and authorization for submission of the required form(s) reporting identified problems in the Software to Vendor.

- 25.2. On-line Support. Vendor may execute on-line diagnostics from a remote Vendor location solely to assist in the identification and isolation of suspected Software errors or malfunctions.
- 25.3. Error and Malfunction Service. Within two (2) Business Days of receiving oral or written notification by Purchaser of identified errors or malfunctions in the Software, Vendor will either:
- a) Provide Purchaser with detour or code correction to the Software error or malfunctions. Each detour or code correction will be made available in the form of either a written correction notice or machine-readable media and will be accompanied by a level of documentation adequate to inform Purchaser of the problem resolved and any significant operational differences resulting from the correction that is known by Vendor, or
 - b) Provide Purchaser with a written response describing Vendor's then-existing diagnosis of the error or malfunction and generally outlining Vendor's then-existing plan and timetable, subject to Purchaser's approval, for correcting or working around the error or malfunction.
- 25.4. On-Call Support. If a problem occurs following Final Acceptance and with current maintenance Contract which significantly impacts Purchaser's usage of the Software and remains unidentified or unresolved after Purchaser has utilized the detour or code correction prescribed by Vendor pursuant to subsection 25.1 or 25.3 above, Vendor will dispatch a qualified representative to the system location during Business Days and Hours. The representative must arrive within four (4) Business Hours. This representative shall have the qualifications necessary to provide:
- a) Advice and assistance in diagnosis and identification of Software errors or malfunctions.
 - b) On-site consultation on correction or detour of identified errors or malfunctions.
- 25.5. When Vendor performs Services pursuant to this Contract that require the use of Purchaser's equipment, Purchaser agrees to make the equipment available at reasonable times and in reasonable time increments, and in no event will Purchaser charge Vendor for such use.
- 25.6. Maintenance Release Services. Vendor will provide error corrections and maintenance releases to the Software that have been developed by Vendor at no additional cost to Purchaser assuming a current maintenance contract. Such releases shall be licensed to Purchaser pursuant to the terms and conditions of this Contract. Each maintenance release will consist of a set of programs and files made available in the form of machine-readable media and will be accompanied by a level of documentation adequate to inform Purchaser of the problems resolved including any significant differences resulting from the release that are known by Vendor. Vendor agrees that each maintenance release of Software will be compatible with the then-current unaltered release of Software applicable to the computer system.

26. Spare Parts for Equipment

Vendor shall make available OEM replacement parts, or Purchaser-approved equivalent based upon availability from third party equipment providers, for a minimum of five (5) years from the date of the initial delivery to Purchaser. Vendor and Purchaser must stay aware and knowledgeable regarding equipment parts availability because a lack may indicate that equipment needs replacement.

27. Vendor Commitments, Warranties and Representations

Any written commitment by Vendor within the scope of this Contract shall be binding upon Vendor. Failure of Vendor to fulfill such a commitment may constitute breach and shall render Vendor liable for damages under the terms of this Contract. For purposes of this section, a commitment by Vendor includes: (i) Prices, discounts, and options committed to remain in force over a specified period of time; and (ii) any warranty or representation made by Vendor in its Response or contained in any Vendor or manufacturer publications, written materials, schedules, charts, diagrams, tables, descriptions, other written representations, and any other communication medium accompanying or referred to in its Response or used to effect the sale to Purchaser.

28. Compliance with Standards

Vendor represents that all Equipment, Software, and elements thereof, including but not limited to documentation and source code, shall meet and be maintained by Vendor to conform to applicable industry standards.

29. Training

Vendor agrees to provide training that is substantively the same as contained in the Vendor's Proposal as negotiated in a Statement of Work. A fee may be charged for training, as set forth in Schedule A.

The starting dates of the training will be as agreed by the parties in the Statement(s) of Work. The training fee, whether separately stated under the pricing provisions of this Contract or included in the cost of the Equipment and Software, shall cover all costs of training. Purchaser shall not be responsible for any additional manufacturer's costs for training required pursuant to this section.

Purchaser shall have the right, so long as the Equipment and/or Software purchased hereunder is in use by Purchaser, to give instruction to Purchaser's personnel in all courses described above and all revisions thereto without charge, using materials supplied by Vendor. Such use by Purchaser of Vendor's materials shall include the right to reproduce the same solely for the permitted use, which use and reproduction shall not be a violation of or infringement upon any patent, copyright, or other proprietary right of Vendor. Vendor grants to Purchaser the right to make derivative works, update, modify, copy, or otherwise reproduce the documentation furnished pursuant to this section at no additional charge.

30. Minority and Women's Business Enterprise (MWBE) Participation

With each invoice for payment and within thirty (30) days of Purchaser Contract Administrator's request, Vendor shall state that its Subcontractor(s) still maintain(s) its/their MWBE certification(s) and specify the amounts paid to each certified MWBE Subcontractor under this Contract. Vendor shall maintain records supporting these statements in accordance with this Contract's **Review of Vendor's Records** section.

31. Protection of Purchaser's Confidential Information

31.1. Vendor acknowledges that some of the material and information that may come into its possession or knowledge in connection with this Contract or its performance may consist of information that is exempt from disclosure to the public or other unauthorized persons under either chapter 42.56 RCW or other state or federal statutes ("Confidential Information"). Confidential Information includes, but is not limited to, names, addresses, Social Security numbers, e-mail addresses, telephone numbers, financial profiles, credit card information, driver's license numbers, medical data, law enforcement records,

agency source code or object code, agency security data, or information identifiable to an individual that relates to any of these types of information. Vendor agrees to hold Confidential Information in strictest confidence and not to make use of Confidential Information for any purpose other than the performance of this Contract, to release it only to authorized employees or Subcontractors requiring such information for the purposes of carrying out this Contract, and not to release, divulge, publish, transfer, sell, disclose, or otherwise make the information known to any other party without Purchaser's express written consent or as provided by law. Vendor agrees to implement physical, electronic, and managerial safeguards to prevent unauthorized access to Confidential Information.

- 31.2. Vendor agrees to release Confidential Information or material only to employees or Subcontractors who have passed a fingerprint-based criminal history background check and signed Schedule D, Nondisclosure Agreement. Purchaser approval of Vendor staff is contingent on this Subsection. The cost of fingerprint-based criminal history background checks shall be the responsibility of the Purchaser.
- 31.3. Immediately upon expiration or termination of this Contract, Vendor shall, at Purchaser's option: (i) certify to Purchaser that Vendor has destroyed all Confidential Information; or (ii) return all Confidential Information to Purchaser; or (iii) take whatever other steps Purchaser requires of Vendor to protect Purchaser's Confidential Information.
- 31.4. Purchaser reserves the right to monitor, audit, or investigate the use of Confidential Information collected, used, or acquired by Vendor through this Contract. The monitoring, auditing, or investigating may include, but is not limited to, salting databases.
- 31.5. Violation of this section by Vendor or its Subcontractors may result in termination of this Contract and demand for return of all Confidential Information, monetary damages, or penalties.

Software License

32. License Grant

- 32.1. Vendor grants to Purchaser a non-exclusive, perpetual license to use the Software pursuant to the XXX Software License Agreement and related documentation according to the terms and conditions of this Contract
- 32.2. Purchaser may modify any Vendor Software and may combine such with other programs or materials to form a derivative work, provided that upon discontinuance or termination of the license, Vendor Software will be removed from the derivative work and, at Purchaser's option, either destroyed or returned to Vendor. In such situations, Purchaser retains a license only to use the Software in the derivative work.
- 32.3. Purchaser will not decompile or disassemble any Software provided under this Contract or modify Software that bears a copyright notice of any third party without the prior written consent of Vendor or Software owner.
- 32.4. Purchaser may copy each item of Software to multiple hard drives or networks excluding backups to the specific number of software licenses acquired as a result of this contract.
- 32.5. Purchaser will make and maintain no more than one archival copy of each item of Software, and each copy will contain all legends and notices and will be subject to the same conditions and restrictions as the original. Purchaser may also make copies of the Software in the course of routine backups of hard drive(s) for the purpose of recovery of hard drive contents. Purchaser may use backup or archival copies of the Software, without reinstallation or interruption of production copy(ies), for disaster recovery

exercises at its disaster recovery site(s), without additional charge [within the scope of the software license purchased]. Purchaser may make these backup or archival copies available to the disaster recovery site employees who require use of the Software in order to assist Purchaser with disaster recovery exercises [within the scope of the software licenses purchased]. Purchaser agrees that production use of the Software at the disaster recovery site(s) shall be limited to the scope of the software licenses purchased and times when Purchaser's facilities, or any portion thereof, are inoperable due to emergency situations.

- 32.6. Business or Support Termination Rights. In the event that Vendor shall, for any reason, cease to conduct business, or cease to support the Software licensed under this Contract, Purchaser shall have a right to convert the Software licenses into perpetual licenses, with rights of quiet enjoyment, but subject to payment obligations not to exceed the Contract Prices.
- 32.7. Freedom of Use. Vendor understands that Purchaser may provide information processing services to other users that are agencies of state government and other tax supported entities. Vendor further understands that Purchaser or other users that are agencies of state government and other tax-supported entities may provide services to the public through Internet applications. Software delivered hereunder may be used in the delivery of these services. Vendor acknowledges and agrees that such use of Software products is acceptable under the licensing agreements contained herein.
- 32.8. Purchaser may move Software from one device to another provided such Software is completely removed from the first device after a reasonable testing period on the new device.

33. Software Ownership

Vendor shall maintain all title, copyright, and other proprietary rights in the Software. Purchaser does not acquire any rights, express or implied, in the Software, other than those specified in this Contract. Vendor hereby warrants and represents to Purchaser that Vendor is the owner of the Software licensed hereunder or otherwise has the right to grant to Purchaser the licensed rights to the Software provided by Vendor through this Contract without violating any rights of any third party worldwide. Vendor represents and warrants that Vendor has the right to license the Software to Purchaser as provided in this Contract; and that Purchaser's use of the Software and documentation within the terms of this Contract will not infringe upon any copyright, patent trademark or other intellectual property right worldwide or violate any third party's trade secret, contract or confidentiality rights worldwide. Vendor represents and warrants that: (i) Vendor is not aware of any claim, investigation, litigation, action, suit or administrative or judicial proceeding pending or threatened based on claims that the Software infringes any patents, copyrights, or trade secrets of any third party, and (ii) that Vendor has no actual knowledge that the Software infringes upon any patents, copyrights, or trade secrets of any third party.

34. Software Code Escrow

- 34.1. Source Code Escrow Package Definition. The term "Source Code Escrow Package" shall mean:
- a) A complete copy in machine-readable form of the source code and executable code of the licensed Software;
 - b) A complete copy of any existing design documentation and user documentation; and/or

- c) Complete instructions for compiling and linking every part of the source code into executable code for purposes of enabling verification of the completeness of the source code as provided below. Such instructions shall include precise identification of all compilers, library packages, and linkers used to generate executable code.
- 34.2. Delivery of Source Code into Escrow. Vendor shall deliver a Source Code Escrow Package to Escrow Agent, provided that Vendor, Purchaser, and Escrow Agent shall first enter into a supplementary escrow agreement substantially the same as attached as Schedule C – *Sample Software Escrow Agreement*. Vendor and Purchaser shall use best efforts to enter into such an Escrow Agreement as soon as possible after the Effective Date of this Contract, but not later than sixty (60) days after the Effective Date of this Contract.
- 34.3. Delivery of New Source Code into Escrow. If during the term of this Contract, term of license, or term of maintenance and support, Vendor provides Purchaser with a maintenance release or upgrade version of the licensed Software, Vendor shall within ten (10) Business Days deposit with Escrow Agent a Source Code Escrow Package for the maintenance release or upgrade version and give Purchaser notice of such delivery.
- 34.4. Verification of Source Code Escrow Package. At its option and expense, Purchaser may request that the completeness and accuracy of any Source Code Escrow Package be verified.
- a) Such verification may be requested once per Source Code Escrow Package.
 - b) Such verification will be conducted by Escrow Agent or, upon at least ten (10) Business Days' prior notice to Vendor, by another party ("Verifier") acceptable to Vendor, after full disclosure to Vendor of information reasonably requested by Vendor about Verifier.
 - c) Prior to conducting the verification, Verifier shall first execute a confidentiality agreement prepared by Vendor that precludes Verifier from disclosing any information to Purchaser about the Source Code Escrow Package other than whether the Source Code Escrow Package was found to be complete and accurate.
 - d) Unless otherwise agreed at the time by Vendor and Purchaser, verification will be performed on-site at Vendor's premises, utilizing Vendor's equipment and software, at a time reasonably acceptable to Vendor. Vendor shall make technical and support personnel available as reasonably necessary for the verification.
 - e) At its discretion, Vendor may designate a representative to accompany the Source Code Escrow Package at all times, and to be present at the verification. Verifier will be Purchaser's sole representative at the verification.
 - f) Verifier is solely responsible for the completeness and accuracy of the verification. Neither the Escrow Agent, if different from the Verifier, nor Vendor shall have any responsibility or liability to Purchaser for any incompleteness or inaccuracy of any verification.
- 34.5. Escrow Fees. All fees and expenses charged by Escrow Agent will be borne by Vendor.
- 34.6. Release Events for Source Code Escrow Packages. The Source Code Escrow Package may be released from escrow to Purchaser, temporarily or permanently, solely upon the occurrence of one or more of the following "Escrow Release Events:"
- a) Vendor becomes insolvent, makes a general assignment for the benefit of creditors, files a voluntary petition of bankruptcy, suffers or permits the appointment of a receiver for business or assets, or becomes subject to any proceeding under any bankruptcy or insolvency law, whether domestic or foreign;

- b) Vendor has wound up or liquidated its business voluntarily or otherwise and Purchaser has compelling reasons to believe that such events will cause Vendor to fail to meet its warranties and maintenance obligations in the foreseeable future; or
- c) Vendor has voluntarily or otherwise discontinued support of the Software or fails to support the Software in accordance with its warranties and maintenance obligations.

34.7. Release Event Procedures. If Purchaser desires to obtain the Source Code Escrow Package from Escrow Agent:

- a) Purchaser shall comply with the procedures set forth in the Escrow Agreement to document the occurrence of the Release Event;
- b) Purchaser shall maintain all materials and information comprising the Source Code Escrow Package in confidence in accordance with the Contract section titled Vendor's Proprietary Information;
- c) If the release is temporary, Purchaser shall promptly return all released materials to Vendor when the circumstances leading to the release are no longer in effect; and
- d) Purchaser shall promptly, fully, and completely respond to any and all requests for information from Vendor concerning Purchaser's use or contemplated use of the Source Code Escrow Package.

35. Software Specifications

All Software will conform to its Specifications. Vendor warrants that Products delivered hereunder shall perform in accordance with these Specifications.

36. Compliance with Standards

Vendor represents that all Software and elements thereof, including but not limited to, documentation and source code, shall meet and be maintained by Vendor to conform to the standards set forth in RFP No. _____.

37. Date Warranty

Vendor warrants that all Products provided under this Contract: (i) do not have a life expectancy limited by date or time format; (ii) will correctly record, store, process, and present calendar dates; (iii) will lose no functionality, data integrity, or performance with respect to any date; and (iv) will be interoperable with other software used by Purchaser that may deliver date records from the Products, or interact with date records of the Products ("Date Warranty"). In the event a Date Warranty problem is reported to Vendor by Purchaser and such problem remains unresolved after three (3) calendar days, at Purchaser's discretion, Vendor shall send, at Vendor's sole expense, at least one (1) qualified and knowledgeable representative to Purchaser's premises. This representative will continue to address and work to remedy the failure, malfunction, defect, or nonconformity on Purchaser's premises. This Date Warranty shall last perpetually. In the event of a breach of any of these representations and warranties, Vendor shall indemnify and hold harmless Purchaser from and against any and all harm, injury, damages, costs, and expenses incurred by Purchaser arising out of said breach.

38. Physical Media Warranty

38.1. Vendor warrants to Purchaser that each licensed copy of the Software provided by Vendor is and will be free from physical defects in the media that tangibly embodies the copy (the "Physical Media Warranty"). The Physical Media Warranty does not apply to defects discovered more than thirty (30) calendar days after the date of Acceptance of the Software copy by Purchaser.

- 38.2. Vendor shall replace, at Vendor's expense including shipping and handling costs, any Software copy provided by Vendor that does not comply with this warranty.

39. No Surreptitious Code Warranty

- 39.1. Vendor warrants to Purchaser that no licensed copy of the Software provided to Purchaser contains or will contain any Self-Help Code nor any Unauthorized Code as defined below. Vendor further warrants Vendor will not introduce, via modem or otherwise, any code or mechanism that electronically notifies Vendor of any fact or event, or any key, node, lock, time-out or other function, implemented by any type of means or under any circumstances, which may restrict Purchaser's use of or access to any program, data or equipment based on any type of limiting criteria, including frequency or duration of use for any copy of the Software provided to Purchaser under this Contract. This warranty is referred to in this Contract as the "No Surreptitious Code Warranty."
- 39.2. As used in this Contract, "Self-Help Code" means any back door, time bomb, drop dead device, or other software routine designed to disable a computer program automatically with the passage of time or under the positive control of a person other than a licensee of the Software. Self-Help Code does not include software routines in a computer program, if any, designed to permit an owner of the computer program (or other person acting by authority of the owner) to obtain access to a licensee's computer system(s) (e.g., remote access via modem) solely for purposes of maintenance or technical support.
- 39.3. As used in this Contract, "Unauthorized Code" means any virus, Trojan horse, worm or other software routines or Equipment components designed to permit unauthorized access to disable, erase, or otherwise harm software, Equipment, or data; or to perform any other such actions. The term Unauthorized Code does not include Self-Help Code.
- 39.4. Vendor will defend Purchaser against any claim, and indemnify Purchaser against any loss or expense arising out of any breach of the No Surreptitious Code Warranty. No limitation of liability, whether contractual or statutory, shall apply to a breach of this warranty.

40. Reauthorization Code

Vendor's Software shall not require a reauthorization code in order for the Software to remain functional upon Purchaser's movement of the Software to another computer system.

41. Software Documentation

Vendor shall provide two (2) complete sets of documentation for each Software Order, including technical, maintenance, and installation information. Vendor shall also provide two (2) complete sets of documentation for each updated version of Software Vendor provides pursuant to the **Software Upgrades and Enhancements** section. Vendor shall provide the documentation on or before the date Vendor delivers its respective Software. There shall be no additional charge for this documentation or the updates, in whatever form provided. Vendor's Software documentation shall be comprehensive, well structured, and indexed for easy reference. If Vendor maintains its technical, maintenance and installation documentation on a web site, Vendor may fulfill the obligations set forth in this section by providing Purchaser access to its web-based documentation information. Vendor may also provide such information on CD-ROM. Vendor grants Purchaser the right to make derivative works, update, modify, copy or otherwise reproduce the documentation furnished pursuant to this section at no additional charge.

Contract Administration

42. Legal Notices

- 42.1. Any notice or demand or other communication required or permitted to be given under this Contract or applicable law (except notice of malfunctioning Equipment) shall be effective only if it is in writing and signed by the applicable party, properly addressed, and either delivered in person, or by a recognized courier service, or deposited with the United States Postal Service as first-class mail, postage prepaid, or via facsimile to the parties at the addresses and fax numbers provided in this section.

To Vendor at:

XXX

Attn: Contracts Administration

XXX

XXX

Phone: XXX

Fax: XXX

E-mail: XXX

To Purchaser at:

Washington State Patrol

Budget and Fiscal Services

Attn: Contracts Manager

PO Box 42602

210 – 11th Ave SW, Room 116

Olympia WA 98504-2602

Phone: (360) 596-4052

Fax: (360) 596-4078

E-mail: jeff.hugdahl@wsp.wa.gov

- 42.2. Notices shall be effective upon receipt or four (4) Business Days after mailing, whichever is earlier. The notice address as provided herein may be changed by written notice given as provided above.
- 42.3. In the event that a subpoena or other legal process commenced by a third party in any way concerning the Equipment or Services provided pursuant to this Contract is served upon Vendor or Purchaser, such party agrees to notify the other party in the most expeditious fashion possible following receipt of such subpoena or other legal process. Vendor and Purchaser further agree to cooperate with the other party in any lawful effort by the other party to contest the legal validity of such subpoena or other legal process commenced by a third party.

43. Vendor Contract Administration

43.1. Vendor Account Manager

Vendor shall appoint an Account Manager for Purchaser's account after Acceptance under this Contract who will provide oversight of Vendor activities conducted hereunder. Vendor's Account Manager will be the principal point of contact for Purchaser concerning Vendor's performance under this Contract. Vendor shall notify Purchaser Contract Administrator and Purchaser System Manager, in writing, when there is a new Vendor Account Manager assigned to this Contract. The Vendor Account Manager information is cited in Appendix A.

43.2. Vendor Project Manager

Vendor shall appoint a Project manager for Purchaser's account under this Contract who will provide oversight of Vendor activities conducted hereunder through Final Acceptance. The Vendor's Project Manager will be the principal point of contact for Purchaser concerning Vendor's performance under this Contract through Final Acceptance. Vendor shall notify Purchaser Contract Administrator in writing when there is a new Vendor Project Manager assigned to this Contract. The Vendor Project Manager is cited in Appendix A.

44. WSP Contract Administration

44.1. WSP System Manager

Purchaser shall appoint a SystemManager for this Contract to provide oversight of activities conducted hereunder. The Purchaser Manager will be the principal contact for Vendor concerning business activities under this Contract. Purchaser shall notify Vendor, in writing, when there is a new Purchaser System Manager assigned to this Contract.

44.2. WSP Contracts Manager

The WSP Contracts Manager reviews and coordinates administration of all WSP contracts. This person has responsibility that all contracting laws and regulations are met and complied with. Vendor can and should contact this person when none of the persons above can be reached. This person should be included as part of any official notice being sent by electronic mail with or without a Licensed Certificate. WSP shall notify the Vendor within five (5) business days when a new WSP Contract Manager is assigned.

45. Notification of Change to Personnel

When either the Vendor or Purchaser changes one of the Manager assignments, notification will be made in writing to all persons with assignments as listed in Appendix A.

46. Section Headings, Incorporated Documents and Order of Precedence

- 46.1. The headings used herein are inserted for convenience only and shall not control or affect the meaning or construction of any of the sections.
- 46.2. Each of the documents listed below is, by this reference, incorporated into this Contract as though fully set forth herein.
 - a) Schedule A
 - b) Statements of Work issued under this Contract;
 - c) Purchaser RFP _____;
 - d) Vendor's Response to Purchaser RFP _____;
 - e) The terms and conditions contained on Purchaser's Order Documents, if used; and
 - f) All Vendor or manufacturer publications, written materials and schedules, charts, diagrams, tables, descriptions, other written representations and any other supporting materials Vendor made available to Purchaser and used to effect the sale of the Product to Purchaser.
 - g) The cooperatively produced technical design specification for the WSP ACCESS environment.
- 46.3. In the event of any inconsistency in this Contract, the inconsistency shall be resolved in the following order of precedence:
 - a) Applicable federal and state statutes, laws, and regulations;
 - b) Sections of this Contract;
 - c) Statements of Work issued under this Contract;
 - d) Schedule A
 - e) Purchaser RFP _____;
 - f) Vendor's Response to Purchaser RFP _____;
 - g) The terms and conditions contained on Purchaser's Order Documents, if used; and

- h) All Vendor or manufacturer publications, written materials and schedules, charts, diagrams, tables, descriptions, other written representations and any other supporting materials Vendor made available to Purchaser and used to effect the sale of the Product to Purchaser.

47. Entire Agreement

This Contract sets forth the entire agreement between the parties with respect to the subject matter hereof and except as provided in the section titled **Vendor Commitments, Warranties and Representations**, understandings, agreements, representations, or warranties not contained in this Contract or a written amendment hereto shall not be binding on either party. Except as provided herein, no alteration of any of the terms, conditions, delivery, Price, quality, or Specifications of this Contract will be effective without the written consent of both parties.

48. Authority for Modifications and Amendments

No modification, amendment, alteration, addition, or waiver of any section or condition of this Contract shall be effective or binding unless it is in writing and signed by Purchaser and Vendor Contracting Officers. Only Purchaser Contracting Officer shall have the express, implied, or apparent authority to alter, amend, modify, add, or waive any section or condition of this Contract on behalf of Purchaser.

49. Independent Status of Vendor

In the performance of this Contract, the parties will be acting in their individual, corporate or governmental capacities and not as agents, employees, partners, joint venturers, or associates of one another. The parties intend that an independent contractor relationship will be created by this Contract. The employees or agents of one party shall not be deemed or construed to be the employees or agents of the other party for any purpose whatsoever. Vendor shall not make any claim of right, privilege or benefit which would accrue to an employee under chapter 41.06 RCW, or Title 51 RCW.

50. Governing Law

This Contract shall be governed in all respects by the law and statutes of the state of Washington, without reference to conflict of law principles. However, if the Uniform Computer Information Transactions Act (UCITA) or any substantially similar law is enacted as part of the law of the state of Washington, said statute will not govern any aspect of this Contract or any license granted hereunder, and instead the law as it existed prior to such enactment will govern. The jurisdiction for any action hereunder shall be exclusively in the Superior Court for the state of Washington. The venue of any action hereunder shall be in the Superior Court for Thurston County, Washington.

51. Subcontractors

Vendor may, with prior written permission from Purchaser Contracting Officer, which consent shall not be unreasonably withheld, enter into subcontracts with third parties for its performance of any part of Vendor's duties and obligations. In no event shall the existence of a subcontract operate to release or reduce the liability of Vendor to Purchaser for any breach in the performance of Vendor's duties. For purposes of this Contract, Vendor agrees that all Subcontractors shall be held to be agents of Vendor. Vendor shall be liable for any loss or damage to Purchaser, including but not limited to personal injury, physical loss, harassment of Purchaser employees, or violations of the **Patent and Copyright Indemnification, Protection of Purchaser's Confidential Information, Ownership/Rights in Data, and Software Ownership** sections of this Contract occasioned by the acts or omissions of Vendor's Subcontractors, their agents or employees. The **Patent and Copyright Indemnification, Protection of Purchaser's Confidential Information, Ownership/Rights in**

Data, Software Ownership, Publicity and Review of Vendor's Records sections of this Contract shall apply to all Subcontractors.

52. Assignment

- 52.1. With the prior written consent of Purchaser Contracting Officer, which consent shall be at Purchaser's sole option, Vendor may assign this Contract including the proceeds hereof, provided that such assignment shall not operate to relieve Vendor of any of its duties and obligations hereunder, nor shall such assignment affect any remedies available to Purchaser that may arise from any breach of the sections of this Contract, or warranties made herein including but not limited to, rights of setoff.
- 52.2. Purchaser may assign this Contract to any public agency, commission, board, or the like, within the political boundaries of the state of Washington, provided that such assignment shall not operate to relieve Purchaser of any of its duties and obligations hereunder.

53. Publicity

- 53.1. The award of this Contract to Vendor is not in any way an endorsement of Vendor or Vendor's products by Purchaser and shall not be so construed by Vendor in any advertising or other publicity materials.
- 53.2. Vendor agrees to submit to Purchaser, all advertising, sales promotion, and other publicity materials relating to this Contract or any Product furnished by Vendor wherein Purchaser's name is mentioned, language is used, or Internet links are provided from which the connection of Purchaser's name therewith may, in Purchaser's judgment, be inferred or implied. Vendor further agrees not to publish or use such advertising, sales promotion materials, publicity or the like through print, voice, the World Wide Web, and other communication media in existence or hereinafter developed without the express written consent of Purchaser *prior* to such use.

54. Review of Vendor's Records

- 54.1. Vendor and its Subcontractors shall maintain books, records, documents and other evidence relating to this Contract, including but not limited to Minority and Women's Business Enterprise participation, protection and use of Purchaser's Confidential Information, and accounting procedures and practices which sufficiently and properly reflect all direct and indirect costs of any nature invoiced in the performance of this Contract. Vendor shall retain all such records for six (6) years after the expiration or termination of this Contract. Records involving matters in litigation related to this Contract shall be kept for either one (1) year following the termination of litigation, including all appeals, or six (6) years from the date of expiration or termination of this Contract, whichever is later.
- 54.2. All such records shall be subject at reasonable times and upon prior notice to examination, inspection, copying, or audit by personnel so authorized by the Purchaser's Contract Administrator and/or the Office of the State Auditor and federal officials so authorized by law, rule, regulation or contract, when applicable, at no additional cost to the State. During this Contract's term, Vendor shall provide access to these items within Thurston County. Vendor shall be responsible for any audit exceptions or disallowed costs incurred by Vendor or any of its Subcontractors.
- 54.3. Vendor shall incorporate in its subcontracts this section's records retention and review requirements.
- 54.4. It is agreed that books, records, documents, and other evidence of accounting procedures and practices related to Vendor's cost structure, including overhead, general and administrative

expenses, and profit factors shall be excluded from Purchaser's review unless the cost or any other material issue under this Contract is calculated or derived from these factors.

55. Right of Inspection

Vendor shall provide right of access to its facilities to Purchaser, or any of Purchaser's officers, or to any other authorized agent or official of the state of Washington or the federal government, at all reasonable times, in order to monitor and evaluate performance, compliance, and/or quality assurance under this Contract.

56. Participation in Purchaser's Quality Assurance Monitoring Programs

The WSP has engaged a separate firm to provide independent quality assurance (QA) services. That firm is responsible for monitoring and evaluating project progress and key project artifacts prepared by the Vendor. The Vendor will provide the QA firm as well as any state oversight entity with timely access to Vendor management personnel, methods, documentation, project content, management documentation, and other project and system artifacts needed to evaluate and assess project status, risks and issues over the life of the project.

57. Updating and Maintaining the Application Product

During the term of this Contract problems may be discovered or it may be determined that changes or enhancements are needed to the vendor product. Either WSP or the Vendor may propose to modify products as described in the System Design or individual Statements of Work. Development and/or coding activities will not begin on a request until a technical design update is jointly approved by authorized representatives of WSP and Vendor. Any technical design modification is subject to equitable compensation in accordance with Schedule E, Problem Report/Change Request Process.

The WSP System Manager and Vendor Account Manager can clarify the procedures in Schedule E, Problem Report/Change Request Process, with notice to other WSP and Vendor contacts, without amending the Contract providing there is not a cost or schedule impact. The limits and rates must be changed by amendment to the Contract.

The level of work effort and cost thresholds will determine whether the changes are handled as a simple change request or a more detailed Statement of Work (SOW).

57.1. Change Requests

Change Requests may be issued on a time and materials basis according to the limits set in Schedule E. Each change request will establish the work to be performed and deliverables to be produced with acceptance criteria for each deliverable, a timeline and period of performance, and a Not-To-Exceed (NTE) price.

The Vendor will make a good faith effort to complete the Services and Deliverables within the estimated NTE price as set forth in the agreed to Change Request, but does not guarantee that the Services or the Deliverables can be completed within the NTE for time and material estimates. The Vendor will make WSP aware as soon as it is known or suspected that the estimate needs to change.

57.2. Statements of Work

Statements of Work are used to develop large tasks with deliverables and acceptance criteria, delivery dates, specific terms and conditions for the SOW, and a Firm Fixed Price with a compensation and payment plan. WSP understands that the process may take longer and cost more because the Vendor takes on more risk than if done using a "time and materials"

approach. Vendor understands deliverables and Firm Fixed Price fits the State funding model more appropriately in accordance with Schedule E.

Schedule E Problem Report/Change Request Process describes the procedures to be used for development of each SOW. Any task regardless of work size may become a SOW depending upon complexity, risk, deliverables, cost, or designation by WSP.

57.3. Reporting and Status

Vendor and WSP shall communicate regularly about SOW status, problem reports, change requests, general issues, and related matters at least monthly or more often as needed. Such reports shall be made through the WSP System Manager and the Vendor Account Manager.

Each party shall respond to the other within two business days on any query, issue, or request with

- Status;
- Expected time of answer if not given; and
- Possible course(s) of action.

General Provisions

58. Patent and Copyright Indemnification

58.1. Vendor, at its expense, shall defend, indemnify, and save Purchaser harmless from and against any claims against Purchaser that any Product supplied hereunder, or Purchaser's use of the Product within the terms of this Contract, infringes any patent, copyright, utility model, industrial design, mask work, trade secret, trademark, or other similar proprietary right of a third party worldwide. Vendor shall pay all costs of such defense and settlement and any penalties, costs, damages and attorneys' fees awarded by a court or incurred by Purchaser provided that Purchaser:

- a) Promptly notifies Vendor in writing of the claim, but Purchaser's failure to provide timely notice shall only relieve Vendor from its indemnification obligations if and to the extent such late notice prejudiced the defense or resulted in increased expense or loss to Vendor; and
- b) Cooperates with and agrees to use its best efforts to encourage the Office of the Attorney General of Washington to grant Vendor sole control of the defense and all related settlement negotiations.

58.2. If such claim has occurred, or in Vendor's opinion is likely to occur, Purchaser agrees to permit Vendor, at its option and expense, either to procure for Purchaser the right to continue using the Product or to replace or modify the same so that they become noninfringing and functionally equivalent. If use of the Product is enjoined by a court and Vendor determines that none of these alternatives is reasonably available, Vendor, at its risk and expense, will take back the Product and provide Purchaser a refund. In the case of Product, Vendor shall refund to Purchaser its depreciated value. No termination charges will be payable on such returned Product, and the Purchaser will pay only those charges that were payable prior to the date of such return. Depreciated value shall be calculated on the basis of a useful life of four (4) years commencing on the date of purchase and shall be an equal amount per year over said useful life. The depreciation for fractional parts of a year shall be prorated on the basis of three hundred sixty-

five (365) days per year. In the event the Product has been installed less than one (1) year, all costs associated with the initial installation paid by Purchaser shall be refunded by Vendor.

58.3. Vendor has no liability for any claim of infringement arising solely from:

- a) Vendor's compliance with any designs, specifications or instructions of Purchaser;
- b) Modification of the Product by Purchaser or a third party without the prior knowledge and approval of Vendor;
- c) Use of the Product in a way not specified by Vendor; or,
- d) Use of the Product with equipment not supplied by Vendor;

unless the claim arose against Vendor's Product independently of any of these specified actions.

59. Save Harmless

Vendor shall defend, indemnify, and save Purchaser harmless from and against any claims, including reasonable attorneys' fees resulting from such claims, by third parties for any or all injuries to persons or damage to property of such third parties arising from intentional, willful or negligent acts or omissions of Vendor, its officers, employees, or agents, or Subcontractors, their officers, employees, or agents. Vendor's obligation to defend, indemnify, and save Purchaser harmless shall not be eliminated or reduced by any alleged concurrent Purchaser negligence.

60. Insurance

60.1. Vendor shall, during the term of this Contract, maintain in full force and effect, the insurance described in this section. Vendor shall acquire such insurance from an insurance carrier or carriers licensed to conduct business in the state of Washington and having a rating of A-, Class VII or better, in the most recently published edition of *Best's Reports*. In the event of cancellation, non-renewal, revocation or other termination of any insurance coverage required by this Contract, Vendor shall provide written notice of such to Purchaser within one (1) Business Day of Vendor's receipt of such notice. Failure to buy and maintain the required insurance may, at Purchaser's sole option, result in this Contract's termination.

60.2. The minimum acceptable limits shall be as indicated below:

- a) Commercial General Liability covering the risks of bodily injury (including death), property damage and personal injury, including coverage for contractual liability, with a limit of not less than \$1 million per occurrence/\$2 million general aggregate;
- b) Business Automobile Liability (owned, hired, or non-owned) covering the risks of bodily injury (including death) and property damage, including coverage for contractual liability, with a limit of not less than \$1 million per accident;
- c) Employers Liability insurance covering the risks of Vendor's employees' bodily injury by accident or disease with limits of not less than \$1 million per accident for bodily injury by accident and \$1 million per employee for bodily injury by disease;
- d) Umbrella policy providing excess limits over the primary policies in an amount not less than \$3 million;
- e) Professional Liability Errors and Omissions, with a deductible not to exceed \$100,000, conditioned upon subsection 60.3 below, and coverage of not less than \$1 million per occurrence/\$2 million general aggregate; and
- f) Crime Coverage with a deductible not to exceed \$1 million, conditioned upon subsection 60.3 below, and coverage of not less than \$5 million single limit per occurrence and \$10 million in the aggregate, which shall at a minimum cover occurrences falling in the

following categories: Computer Fraud; Forgery; Money and Securities; and Employee Dishonesty.

- 60.3. For Professional Liability Errors and Omissions coverage and Crime Coverage, Vendor shall continue such coverage for two (2) years beyond the expiration or termination of this Contract, naming Purchaser as an additional insured and providing Purchaser with certificates of insurance on an annual basis;
- 60.4. Vendor shall pay premiums on all insurance policies. Such insurance policies shall name Purchaser as an additional insured on all general liability, automobile liability, and umbrella policies. Such policies shall also reference this Contract number _____ and shall have a condition that they not be revoked by the insurer until forty-five (45) calendar days after notice of intended revocation thereof shall have been given to Purchaser by the insurer.
- 60.5. All insurance provided by Vendor shall be primary as to any other insurance or self-insurance programs afforded to or maintained by the State and shall include a severability of interests (cross-liability) provision.
- 60.6. Vendor shall furnish separate certificates of insurance and endorsements for each Subcontractor. Subcontractor(s) shall comply fully with all insurance requirements stated herein. Failure of Subcontractor(s) to comply with insurance requirements does not limit Vendor's liability or responsibility.
- 60.7. Vendor shall furnish to Purchaser copies of certificates of all required insurance within thirty (30) calendar days of this Contract's Effective Date and copies of renewal certificates of all required insurance within thirty (30) days after the renewal date. These certificates of insurance must expressly indicate compliance with each and every insurance requirement specified in this section. Failure to provide evidence of coverage may, at Purchaser's sole option, result in this Contract's termination.
- 60.8. By requiring insurance herein, Purchaser does not represent that coverage and limits will be adequate to protect Vendor. Such coverage and limits shall not limit Vendor's liability under the indemnities and reimbursements granted to Purchaser in this Contract.

61. Industrial Insurance Coverage

Prior to performing work under this Contract, Vendor shall provide or purchase industrial insurance coverage for its employees, as may be required of an "employer" as defined in Title 51 RCW, and shall maintain full compliance with Title 51 RCW during the course of this Contract. Purchaser will not be responsible for payment of industrial insurance premiums or for any other claim or benefit for Vendor, or any Subcontractor or employee of Vendor, which might arise under the industrial insurance laws during the performance of duties and services under this Contract.

62. Licensing Standards

Vendor shall comply with all applicable local, state, and federal licensing, accreditation and registration requirements and standards necessary in the performance of this Contract. (See, for example, chapter 19.02 RCW for state licensing requirements and definitions.)

63. OSHA/WISHA

Vendor represents and warrants that its Products, when shipped, are designed and manufactured to meet then current federal and state safety and health regulations. Vendor agrees to indemnify and hold Purchaser harmless from all damages assessed against Purchaser as a result of the failure of the Products furnished under this Contract to so comply.

64. Uniform Commercial Code (UCC) Applicability

- 64.1. Except to the extent the sections of this Contract are clearly inconsistent, this Contract shall be governed by any applicable sections of the Uniform Commercial Code (UCC) as set forth in Title 62A RCW.
- 64.2. To the extent this Contract entails delivery or performance of services, such services shall be deemed “goods” within the meaning of the UCC, except when to do so would result in an absurdity.
- 64.3. In the event of any clear inconsistency or contradiction between this Contract and the UCC, the terms and conditions of this Contract take precedence and shall prevail unless otherwise provided by law.

65. Antitrust Violations

Vendor and Purchaser recognize that in actual economic practice overcharges resulting from antitrust violations are usually borne by Purchaser. Therefore, Vendor hereby assigns to Purchaser any and all claims for such overcharges as to goods and services purchased in connection with this Contract, except as to overcharges not passed on to Purchaser resulting from antitrust violations commencing after the date of the bid, quotation, or other event establishing the Price under this Contract.

66. Compliance with Civil Rights Laws

During the performance of this Contract, Vendor shall comply with all federal and applicable state nondiscrimination laws, including but not limited to: Title VII of the Civil Rights Act, 42 U.S.C. §12101 *et seq.*; the Americans with Disabilities Act (ADA); and Title 49.60 RCW, Washington Law Against Discrimination. In the event of Vendor’s noncompliance or refusal to comply with any nondiscrimination law, regulation or policy, this Contract may be rescinded, canceled, or terminated in whole or in part under the **Termination for Default** sections, and Vendor may be declared ineligible for further contracts with Purchaser.

67. Severability

If any term or condition of this Contract or the application thereof is held invalid, such invalidity shall not affect other terms, conditions, or applications which can be given effect without the invalid term, condition, or application; to this end the terms and conditions of this Contract are declared severable.

68. Waiver

Waiver of any breach of any term or condition of this Contract shall not be deemed a waiver of any prior or subsequent breach. No term or condition of this Contract shall be held to be waived, modified, or deleted except by a written instrument signed by the parties.

69. Treatment of Assets

- 69.1. Title to all property furnished by Purchaser shall remain in Purchaser. Title to all property furnished by Vendor, for which Vendor is entitled to reimbursement, other than rental payments, under this Contract, shall pass to and vest in Purchaser pursuant to the **Title to Equipment** section. As used in this section **Treatment of Assets**, if the “property” is Vendor’s proprietary, copyrighted, patented, or trademarked works, only the applicable license, not title, is passed to and vested in Purchaser.
- 69.2. Any Purchaser property furnished to Vendor shall, unless otherwise provided herein or approved by Purchaser, be used only for the performance of this Contract.

- 69.3. Vendor shall be responsible for any loss of or damage to property of Purchaser that results from Vendor's negligence or that results from Vendor's failure to maintain and administer that property in accordance with sound management practices.
- 69.4. Upon loss or destruction of, or damage to any Purchaser property, Vendor shall notify Purchaser thereof and shall take all reasonable steps to protect that property from further damage.
- 69.5. Vendor shall surrender to Purchaser all Purchaser property prior to completion, termination, or cancellation of this Contract.
- 69.6. All reference to Vendor under this section shall also include Vendor's employees, agents, or Subcontractors.

70. Vendor's Proprietary Information

Vendor acknowledges that Purchaser is subject to chapter 42.56 RCW and that this Contract shall be a public record as defined in chapter 42.56 RCW. Any specific information that is claimed by Vendor to be Proprietary Information, must be clearly identified as such by Vendor. To the extent consistent with chapter 42.56 RCW, Purchaser shall maintain the confidentiality of all such information marked Proprietary Information. If a public disclosure request is made to view Vendor's Proprietary Information, Purchaser will notify Vendor of the request and of the date that such records will be released to the requester unless Vendor obtains a court order from a court of competent jurisdiction enjoining that disclosure. If Vendor fails to obtain the court order enjoining disclosure, Purchaser will release the requested information on the date specified.

Disputes and Remedies

71. Disputes

- 71.1. In the event a bona fide dispute concerning a question of fact arises between Vendor and Purchaser and it cannot be resolved between the parties, either party may initiate the dispute resolution procedure provided herein.
- 71.2. The initiating party shall reduce its description of the dispute to writing and deliver it to the responding party. The responding party shall respond in writing within three (3) Business Days. The initiating party shall have three (3) Business Days to review the response. If after this review a resolution cannot be reached, both parties shall have three (3) Business Days to negotiate in good faith to resolve the dispute.
 - a) If the dispute cannot be resolved after three (3) Business Days, a Dispute Resolution Panel may be requested in writing by either party who shall also identify the first panel member. Within three (3) Business Days of receipt of the request, the other party will designate a panel member. Those two panel members will appoint a third individual to the dispute resolution panel within the next three (3) Business Days.
 - b) The Dispute Resolution Panel will review the written descriptions of the dispute, gather additional information as needed, and render a decision on the dispute in the shortest practical time.
 - c) Each party shall bear the cost for its panel member and share equally the cost of the third panel member.
- 71.3. Both parties agree to be bound by the determination of the Dispute Resolution Panel.
- 71.4. Both parties agree to exercise good faith in dispute resolution and to settle disputes prior to using a Dispute Resolution Panel whenever possible.

- 71.5. Purchaser and Vendor agree that, the existence of a dispute notwithstanding, they will continue without delay to carry out all their respective responsibilities under this Contract that are not affected by the dispute.
- 71.6. If the subject of the dispute is the amount due and payable by Purchaser for Services being provided by Vendor, Vendor shall continue providing Services pending resolution of the dispute provided Purchaser pays Vendor the amount Purchaser, in good faith, believes is due and payable, and places in escrow the difference between such amount and the amount Vendor, in good faith, believes is due and payable.

72. Attorneys' Fees and Costs

- 72.1. If any litigation is brought to enforce any term, condition, or section of this Contract, or as a result of this Contract in any way, the prevailing party shall be awarded its reasonable attorneys' fees together with expenses and costs incurred with such litigation, including necessary fees, costs, and expenses for services rendered at both trial and appellate levels, as well as subsequent to judgment in obtaining execution thereof.
- 72.2. In the event that the parties engage in arbitration, mediation or any other alternative dispute resolution forum to resolve a dispute in lieu of litigation, both parties shall share equally in the cost of the alternative dispute resolution method, including cost of mediator or arbitrator. In addition, each party shall be responsible for its own attorneys' fees incurred as a result of the alternative dispute resolution method.

73. Non-Exclusive Remedies

The remedies provided for in this Contract shall not be exclusive but are in addition to all other remedies available under law.

74. Liquidated Damages

- 74.1. Liquidated Damages – General
- a) Any delay by Vendor in meeting the Delivery Date(s), Installation Date(s), and, maintenance or repair dates set forth in this Contract will interfere with the proper implementation of Purchaser's programs and will result in loss and damage to Purchaser.
 - b) As it would be impracticable to fix the actual damage sustained in the event of any such failure(s) to perform, Purchaser and Vendor agree that in the event of any such failure(s) to perform, the amount of damage which will be sustained will be the amount set forth in the following subsections and the parties agree that Vendor shall pay such amounts as liquidated damages and not as a penalty.
 - c) Liquidated damages provided under the terms of this Contract are subject to the same limitations as provided in the section titled **Limitation of Liability**.
- 74.2. Liquidated Damages – Specific
- a) If Vendor does not have the Equipment and Software installed by the Installation Date, agreed upon between Purchaser and Vendor, then Vendor shall provide a revised Installation Date and pay to Purchaser as fixed and agreed liquidated damages, in lieu of all other damages due to such delay, for each calendar day between the specified Installation Date and the date that Vendor actually installs the Equipment and Software, and the Equipment and Software is operational in accordance with the **Standard of Performance and Acceptance** section an amount of 1% of total cost (purchase price plus applicable tax and shipping) of the delinquent Equipment and/or Software per day.

- b) If the revised Installation Date is more than thirty (30) calendar days from the original Installation Date, then by written notice to Vendor, Purchaser may immediately terminate the right of Vendor to deliver the Equipment and/or Software and Purchaser may obtain substitute Equipment and/or Software from another vendor. In this event, Vendor shall be liable for fixed and agreed-upon liquidated damages, in lieu of all other damages due to such delay, in the amount specified above, until substitute Equipment and/or Software is installed, or a maximum of thirty (30) calendar days from the original delivery date, whichever occurs first.
- c) If Vendor's maintenance personnel fail to arrive at Purchaser's site within four (4) hours after notification by Purchaser that maintenance is required, Vendor shall pay to Purchaser as fixed and agreed liquidated damages, in lieu of all other damages due to such non-responsiveness, for each hour between the agreed four (4) hour response time and the actual response time an amount of one-hundred dollars (\$100) per hour for each "late" hour or part thereof (prorated) beginning with the time of notification by Purchaser and ending with the time that Vendor's maintenance personnel arrive at Purchaser's Equipment site. This response time applies to the Final Acceptance period as well as post Final Acceptance.

75. Failure to Perform

If Vendor fails to perform any substantial obligation under this Contract, Purchaser shall give Vendor written notice of such Failure to Perform. If after thirty (30) calendar days from the date of the written notice Vendor still has not performed, then Purchaser may withhold all monies due and payable to Vendor, without penalty to Purchaser, until such Failure to Perform is cured or otherwise resolved.

76. Limitation of Liability

- 76.1. The parties agree that neither Vendor nor Purchaser shall be liable to each other, regardless of the form of action, for consequential, incidental, indirect, or special damages except a claim related to bodily injury or death, or a claim or demand based on a Date Warranty or No Surreptitious Code Warranty issue or patent, copyright, or other intellectual property right infringement, in which case liability shall be as set forth elsewhere in this Contract. This section does not modify any sections regarding liquidated damages or any other conditions as are elsewhere agreed to herein between the parties. The damages specified in the sections titled **OSHA/WISHA**, **Termination for Default**, and **Review of Vendor's Records** are not consequential, incidental, indirect, or special damages as that term is used in this section.
- 76.2. Neither Vendor nor Purchaser shall be liable for damages arising from causes beyond the reasonable control and without the fault or negligence of either Vendor or Purchaser. Such causes may include, but are not restricted to, acts of God or of the public enemy, acts of a governmental body other than Purchaser acting in either its sovereign or contractual capacity, war, explosions, fires, floods, earthquakes, epidemics, quarantine restrictions, strikes, freight embargoes, and unusually severe weather; but in every case the delays must be beyond the reasonable control and without fault or negligence of Vendor, Purchaser, or their respective Subcontractors.
- 76.3. If delays are caused by a Subcontractor without its fault or negligence, Vendor shall not be liable for damages for such delays, unless the Services to be performed were obtainable on comparable terms from other sources in sufficient time to permit Vendor to meet its required performance schedule.
- 76.4. Neither party shall be liable for personal injury to the other party or damage to the other party's property except personal injury or damage to property proximately caused by such party's respective fault or negligence.

Contract Termination

77. Termination for Default

- 77.1. If either Purchaser or Vendor violates any material term or condition of this Contract or fails to fulfill in a timely and proper manner its obligations under this Contract, then the aggrieved party shall give the other party written notice of such failure or violation. The responsible party will correct the violation or failure within thirty (30) calendar days or as otherwise mutually agreed in writing. If the failure or violation is not corrected, this Contract may be terminated immediately by written notice from the aggrieved party to the other party. The option to terminate shall be at the sole discretion of the aggrieved party. Purchaser reserves the right to suspend all or part of the Contract, withhold further payments, or prohibit Vendor from incurring additional obligations of funds during investigation of any alleged Vendor compliance breach and pending corrective action by Vendor or a decision by Purchaser to terminate the Contract.
- 77.2. In the event of termination of this Contract by Purchaser, Purchaser shall have the right to procure the Products and Services that are the subject of this Contract on the open market and Vendor shall be liable for all damages, including, but not limited to: (i) the cost difference between the original Contract price for the Products and Services and the replacement costs of such Products and Services acquired from another Vendor; (ii) if applicable, all administrative costs directly related to the replacement of this Contract, such as costs of competitive bidding, mailing, advertising, applicable fees, charges or penalties, staff time costs; and, (iii) any other costs to Purchaser resulting from Vendor's breach. Purchaser shall have the right to deduct from any monies due to Vendor, or that thereafter become due, an amount for damages that Vendor will owe Purchaser for Vendor's default.
- 77.3. If the Failure to Perform is without the defaulting party's control, fault, or negligence, the termination shall be deemed to be a **Termination for Convenience**.
- 77.4. This section shall not apply to any failure(s) to perform that results from the willful or negligent acts or omissions of the aggrieved party.

78. Termination for Convenience

When, at the sole discretion of Purchaser, it is in the best interest of the State, Purchaser Contracting Officer may terminate this Contract, in whole or in part, by 30 (thirty) calendar days' written notice to Vendor. If this Contract is so terminated, Purchaser is liable only for payments required by the terms of this Contract for Products and Services received and Accepted by Purchaser prior to the effective date of termination.

79. Termination for Withdrawal of Authority

In the event that Purchaser's authority to perform any of its duties is withdrawn, reduced, or limited in any way after the commencement of this Contract and prior to normal completion, Purchaser may terminate this Contract by seven (7) calendar days' written notice to Vendor. No penalty shall accrue to Purchaser in the event this section shall be exercised. This section shall not be construed to permit Purchaser to terminate this Contract in order to acquire similar products or services from a third party.

80. Termination for Non-Allocation of Funds

If funds are not allocated to Purchaser to continue this Contract in any future period, Purchaser may terminate this Contract by seven (7) calendar days' written notice to Vendor or work with Vendor to arrive at a mutually acceptable resolution of the situation. Purchaser will not be obligated to pay any further charges for Services including the net remainder of agreed to consecutive periodic payments

remaining unpaid beyond the end of the then current period. Purchaser agrees to notify Vendor in writing of such non-allocation at the earliest possible time. No penalty shall accrue to Purchaser in the event this section shall be exercised. This section shall not be construed to permit Purchaser to terminate this Contract in order to acquire similar products or services from a third party.

81. Termination for Conflict of Interest

Purchaser may terminate this Contract by written notice to Vendor if Purchaser determines, after due notice and examination, that any party has violated chapter 42.52 RCW, Ethics in Public Service or any other laws regarding ethics in public acquisitions and procurement and performance of contracts. In the event this Contract is so terminated, Purchaser shall be entitled to pursue the same remedies against Vendor as it could pursue in the event Vendor breaches this Contract.

82. Termination Procedure

- 82.1. In addition to the procedures set forth below, if Purchaser terminates this Contract, Vendor shall follow any procedures Purchaser specifies in Purchaser's notice of termination.
- 82.2. Upon termination of this Contract, Purchaser, in addition to any other rights provided in this Contract, may require Vendor to deliver to Purchaser any property, Products, or Work Products specifically produced or acquired for the performance of such part of this Contract as has been terminated. The section titled **Treatment of Assets** shall apply in such property transfer.
- 82.3. Unless otherwise provided herein, Purchaser shall pay to Vendor the agreed-upon price, if separately stated, for the Products or Services received and accepted by Purchaser, provided that in no event shall Purchaser pay to Vendor an amount greater than Vendor would have been entitled to if this Contract had not been terminated. Failure to agree with such determination shall be a dispute within the meaning of the **Disputes** section of this Contract. Purchaser may withhold from any amounts due Vendor such sum as Purchaser determines to be necessary to protect Purchaser from potential loss or liability.
- 82.4. Vendor shall pay amounts due Purchaser as the result of termination within thirty (30) calendar days of notice of amounts due. If Vendor fails to make timely payment, Purchaser may charge interest on the amounts due at one percent (1%) per month until paid in full.

83. Covenant Against Contingent Fees

- 83.1. Vendor warrants that no person or selling agency has been employed or retained to solicit or secure this Contract upon any agreement or understanding for a commission, percentage, brokerage, or contingent fee, *except* bona fide employees or a bona fide established commercial or selling agency of Vendor.
- 83.2. In the event Vendor breaches this section, Purchaser shall have the right to either annul this Contract without liability to Purchaser, or, in Purchaser's discretion, deduct from payments due to Vendor, or otherwise recover from Vendor, the full amount of such commission, percentage, brokerage, or contingent fee.

Contract Execution

84. Authority to Bind

The signatories to this Contract represent that they have the authority to bind their respective organizations to this Contract.

85. Counterparts

This Contract may be executed in counterparts or in duplicate originals. Each counterpart or each duplicate shall be deemed an original copy of this Contract signed by each party, for all purposes.

In Witness Whereof, the parties hereto, having read this Contract in its entirety, including all attachments, do agree in each and every particular and have thus set their hands hereunto.

This Contract is effective this ____ day of _____, 2____.

Approved

State of Washington
Washington State Patrol

Approved

XXX

Signature

Signature

Print or Type Name Date

Print or Type Name Date

Title

Title

Approved as to Form

State of Washington
Office of the Attorney General

Signature

Print or Type Name

Assistant Attorney General

Title Date

Appendix A

Contact Information for Vendor and Purchaser

Vendor Account Manager

Name:

Address:

Phone:

Fax:

E-mail:

Vendor Project Manager

Name:

Address:

Phone:

Fax:

E-mail:

Purchaser SystemManager

Name: Mr. Steven Cole

WSP

Address: 403 Cleveland Ave SE

Suite C

Tumwater, WA 98501

Phone: 360 705 5131

Fax: 360 705 5784

E-mail: steven.cole@wsp.wa.gov

Purchaser Contracts Manager

Name: Mr. Jeff Hugdahl

WSP

Address: PO Box 42602

Olympia, WA 98504-2602

Phone: 360 596 4052
Fax: 360 596 4078
E-mail: jeff.hugdahl@wsp.wa.gov

Invoices

Name: ITD Fiscal Unit

WSP

Address: 403 Cleveland Ave SE
Suite C
Tumwater, WA 98501

Phone: 360 705 5183
Fax: 360 705 5784

Schedule A
Authorized Product and Price List
for
Contract Number _____
with
(Vendor Name)

Schedule B
Product Acceptance Plan
for
Contract Number _____
with
(Vendor Name)

To be incorporated into this Contract through a mutually agreed upon amendment.

Schedule C
Sample Software Escrow Agreement
for
Contract Number _____

This Escrow Contract (hereinafter referred to as "Contract") is entered into by and between the State of Washington, Washington State Patrol, hereinafter referred to as "Purchaser;" and the XXX Inc., hereinafter referred to as "Vendor,"

WHEREAS, the Vendor and the Purchaser have entered into Purchaser Contract No. _____ to which this Contract is appended hereto and made a part hereof, pursuant to which the Vendor has licensed to the Purchaser certain computer Software product(s), including updates, improvements, and enhancements thereof from time to time developed by the Vendor, and such additional computer program changes as the Purchaser may order from the Vendor from time to time, all documentation therefor developed by the Vendor (hereinafter collectively referred to as the "Product"); and

WHEREAS, it is the policy of the Vendor not to disclose the Source Code(s) and related documentation (hereinafter collectively referred to as the ("Source Code Escrow Package")) for the Product(s) to its customers except as provided in an applicable Escrow Contract; and

WHEREAS Vendor and the Purchaser agree that upon occurrence of certain events described in Section 3(a) hereof, the Purchaser shall be able to obtain the Source Code Escrow Package and all revisions thereof;

ACCORDINGLY, the Vendor agrees to deliver the Source Code Escrow Package to the Escrow Agent upon the effective date of this Escrow Contract, which shall be as soon as practicable after the execution date of the Software License Contract between Vendor and the Purchaser.

NOW THEREFORE, in consideration of the mutual covenants exchanged herein and for other valuable consideration, the adequacy and receipt of which are hereby acknowledged, the Vendor, the Purchaser and the Escrow Agent hereby act and agree as follows:

1. DEPOSITS

The Escrow Agent, as a safekeeping (escrow) agent, agrees to accept from the Vendor the Source Code Escrow Package. "Source Code Escrow Package" shall mean the following:

- a) A complete copy in machine-readable form of the Source Code and Executable Code of the Licensed Software;
- b) A complete copy of any existing Design Documentation and User Documentation;
- c) Complete instructions for compiling and linking every part of the Source Code into Executable Code for purposes of enabling verification of the completeness of the Source Code as provided below. Such instructions shall include precise identification of all compilers, library packages, and linkers used to generate Executable Code.

The Escrow Agent will issue to the Vendor and Purchaser a receipt for the Source Code Escrow Package upon delivery. The Source Code Escrow Package held by the Escrow Agent shall remain the exclusive property of the Vendor, and the Escrow Agent shall not use the Source Code Escrow Package or disclose the same to any third party except as specifically provided for herein. The Escrow Agent will hold the Source Code Escrow Package in safekeeping at its office listed in Section 9 titled Notices below unless and until the Escrow Agent is to deliver the Source Code Escrow Package to Vendor or the Purchaser, in which case, the Escrow Agent shall deliver the Source Code Escrow Package to the party identified therein, subject, however, to the sections of this Escrow Contract.

2. REPRESENTATIONS OF VENDOR TO PURCHASER

Vendor represents and warrants to Purchaser that:

- a. The materials described in this Contract as Software applications products hereto constitutes the Source Code Escrow Package and documentation for the Product licensed to the Purchaser pursuant to the Software license and service Contract therein.
- b. The Source Code Escrow Package delivered to the Escrow Agent are in a form suitable for reproduction by computer and photocopy equipment, and consists of full source language statement of the computer program or programs comprising the Software and complete computer program maintenance documentation, including all flow charts, schematics and annotations which comprise the precoding detailed design specifications, and all other material necessary to allow a reasonably skilled third party programmer or analyst to maintain or enhance the Product without the help of any other person or reference to any other material; such Source Code Escrow Package to be in the mode machine readable by the then operating Purchaser equipment and produced and copied on 1600 bpi magnetic tape.
- c. The Vendor will promptly supplement the Source Code delivered hereunder with all revisions, corrections, enhancements or other changes so that the Source Code Escrow Package constitutes a human readable computer program for the current release of the Product. This supplementation shall be made in machine readable format by the then operating Purchaser equipment and produced and copied on 1600 bpi magnetic tape, along with specifications of sections a. and b. herein, every six (6) months or within ten (10) Business Days of delivery of any modification, enhancement, or upgrade to the Purchaser or any other customer of the Vendor, whichever occurs first.

3. NOTICE OF DEFAULT

- a. The Vendor shall be deemed to be in default of its responsibilities to the Purchaser if:
 - i. The Vendor becomes insolvent, makes a general assignment for the benefit of creditors, files a voluntary petition of bankruptcy, suffers or permits the appointment of a receiver for its business or assets, becomes subject to any proceeding under any bankruptcy or insolvency law, whether domestic or foreign;
 - ii. The Vendor has wound up or liquidated its business voluntarily or otherwise and the Purchaser has compelling reasons to believe that such events will cause the Vendor to fail to meet its warranties and maintenance obligations in the foreseeable future; or
 - iii. The Vendor voluntarily or otherwise discontinues support of the provided products or fails to support the products in accordance with its warranties and maintenance obligations.
- b. The Purchaser shall give written notice ("Notice of Default") to the Escrow Agent of any default by the Vendor. The Notice of Default shall, at the minimum:
 - i. Be labeled "Notice of Default";
 - ii. Identify the Software License Contracts and any other relevant agreement, contained therein and this Escrow Contract;
 - iii. Specify the nature of the default(s);
 - iv. Identify the Source Code Escrow Package with specificity; and
 - v. Demand the delivery of the Source Code Escrow Package to the Purchaser.
- c. Upon receipt of the Notice of Default, the Escrow Agent shall send a copy thereof to the Vendor by certified or registered mail, postage prepaid, return receipt requested. The Escrow Agent shall

automatically be authorized and directed to deliver the Source Code Escrow Package to the Purchaser in accordance with this Escrow Contract within ten (10) Business Days.

4. NOTICE OF TERMINATION

Upon the termination of the applicable Software License Contracts, the Vendor may obtain the return of the applicable Source Code Escrow Package to terminated Software applications products by furnishing written notice of the termination, agreed to by authorized and notarized signature of the Purchaser.

5. DISPUTES

The Escrow Agent shall not release the Source Code Escrow Package to either party except in accordance with the completion of any of the sections in Section 3 above, or upon receipt of an agreement with authorized and notarized signatures of both Vendor and the Purchaser, authorizing the release of the Source Code Escrow Package to one of the parties hereto.

6. PAYMENT OF ESCROW

As payment for its Services hereunder, the Escrow Agent shall receive a fee of _____ from the Vendor.

7. TERMINATION

Unless terminated sooner, this Escrow Contract shall terminate on the delivery of the Source Code Escrow Package of Software applications products to Vendor or Purchaser as provided herein.

8. WAIVER, AMENDMENT OR MODIFICATION; SEVERABILITY

This Escrow Contract shall not be waived, amended, or modified except by the written agreement of all the parties hereto. Any invalidity, in whole or in part, of any section of this Escrow Contract shall not affect the validity of any other of its sections.

9. NOTICES

All notices required to be given hereunder shall be in writing and shall be given by certified or registered mail, return receipt requested, to the parties at their respective addresses as follows:

to **Vendor** at: *[Vendor Name]*
 Attention: [Name]
 [Street Address]
 [City]
 [State]
 [phone and fax numbers]

to Purchaser at: Washington State Patrol
 Attention: Budget and Fiscal Services
 PO Box 42602
 Olympia, WA 98504-2602
 Phone: (360)596-4052; Fax (360) 596-4078

to Escrow Agent at: *[Escrow Agent's Name]*
 Attention: [Name]
 [Street Address]
 [City]
 [State]
 [phone and fax numbers]

10. LIMITATION ON ESCROW AGENT'S RESPONSIBILITY AND LIABILITY

- a. The Escrow Agent shall not be obligated or required to examine or inspect the Source Code Escrow Package, or any of the Additions. The Escrow Agent's obligation for safekeeping shall be limited to providing the same degree of care for the Source Code Escrow Package as it maintains for its valuable documents and those of its customers lodged in the same location with appropriate atmospheric or other safeguards. However, the parties agree and acknowledge that the Escrow Agent shall not be responsible for any loss or damage to any of the Source Code Escrow Package due to changes in such atmospheric conditions, unless such changes are proximately caused by the gross negligence or malfeasance of the Escrow Agent.
- b. The Escrow Agent shall be protected in acting upon any written notice, request, waiver, consent, receipt or other paper or document furnished to it, not only in assuming its due execution but also the validity and effectiveness of its information therein contained, which it in good faith believes to be genuine and what it purports to be.
- c. In no event shall the Escrow Agent be liable for any act or failure to act under the sections of the Escrow Contract except where its acts are the result of gross negligence or malfeasance. The Escrow Agent shall have no duties except those which are expressly set forth herein, and it shall not be bound by any notice of a claim, or demand, termination or rescission of the Escrow Contract, unless received in writing , and, if its duties herein are affected, unless it shall have given its prior written consent thereto.
- d. The parties to this Contract hereby jointly and severally indemnify the Escrow Agent against any loss, liability or damage (other than any caused by the gross negligence or malfeasance of the Escrow Agent), including reasonable costs of litigation and counsel fees, arising from and in connection with the performance of its duties under this Contract.

11. GOVERNING LAWS

This Contract shall be governed in all respects by the law and statutes of the state of Washington. The venue of any action hereunder shall in the Superior Court for Thurston County, Washington.

12. AUTHORITY TO BIND

The signatories to this Contract represent that they have the authority to bind their respective organizations to this Contract.

IN WITNESS WHEREOF, the parties hereto have caused this Escrow Contract to be duly executed in

triplicate originals and each triplicate shall be deemed an original copy of this Contract signed by each party, for all purposes, as of the year and date last written below.

FOR THE WASHINGTON STATE PATROL

[Vendor's Name]

By: _____

By: _____

Its: _____

Its: _____

Date: _____

Date: _____

ESCROW AGENT

By: _____

Its: _____

Date: _____

Schedule D
Nondisclosure Agreement
for
Contract Number _____

As an employee, agent or Subcontractor of the XXX, I acknowledge that some of the material and information that may come into my possession or knowledge in connection with Washington State Patrol Contract Number _____ (Contract) or its performance may consist of information that is exempt from disclosure to the public or other unauthorized persons under either chapter 42.56 RCW or other state or federal statutes ("Confidential Information").

Confidential Information includes, but is not limited to, names, addresses, Social Security numbers, e-mail addresses, telephone numbers, financial profiles, credit card information, driver's license numbers, medical data, law enforcement records, agency source code or object code, agency security data, or information identifiable to an individual that relates to any of these types of information.

I agree to hold Confidential Information in strictest confidence and not to make use of Confidential Information for any purpose other than the performance of this Contract, to release it only to authorized employees or Subcontractors requiring such information for the purposes of carrying out this Contract, and not to release, divulge, publish, transfer, sell, disclose, or otherwise make it known to any other party without the Washington State Patrol's express written consent or as provided by law.

I agree to release such information or material only to employees or Subcontractors who have signed a Nondisclosure Agreement substantially the same as this Nondisclosure Agreement. I also agree to implement physical, electronic, and managerial safeguards to prevent unauthorized access to Confidential Information.

Immediately upon expiration or termination of this Contract, my employment with the XXX, or the contractual relationship with the XXX if I am a subcontractor, I shall surrender any and all Confidential Information in my possession to the XXX for its disposition according to the terms of the Contract.

I understand that I am subject to all applicable state and federal laws, rules, and regulations, including RCW 10.97, violation of which may result in criminal prosecution.

Signature of Employee or Subcontractor

Printed Name and Title

Date

SCHEDULE E

Problem Report/Change Request Process

- A. The WSP System Manager can initiate and approve Problem Reports, Change Requests, or Statements of Work (SOW) that remain within the scope defined herein.
- B. The party requesting the change or submitting the problem report ("Requester") will forward to the other party ("Recipient") a form by electronic mail. A form template is shown below. The form includes at a minimum:
- Task name
Requester's name and title
Date of the Report/Request
Description of the proposed change (problem correction)
Reason for the proposed change
Priority of the proposed change
Log number
- C. The Recipient may assign a tracking number as well.
- D. Each Problem Report/Change Request is categorized by the Requester as "Mission Critical", "High", "Medium", or "Low".
- E. The Vendor analyses the impact of the Problem Report/Change Request as to number of hours, travel, process to implement for Mission Critical and High Change Requests. Other Problem Report/Change Requests are investigated upon specific request by the WSP System Manager and/or WSP Contract Administrator.
- F. A progress report shall be made on each assigned investigation every ten (10) Business Days after submittal. If the analysis takes longer than twenty (20) Business Days or two (2) reporting cycles, a Statement of Work may be initiated. If the investigation shows that analysis requires more than 75 hours, a Statement of Work should be initiated. If the investigation shows that analysis, design, development, installation, testing, and implementation will require more than four hundred hours, a Statement of Work is initiated.
- G. Generally, WSP shall use the following guides when classifying tasks as either a Statement of Work or a Change Request:
- Tasks with an estimate over \$75,000 or 400 hours become a Statement of Work.
 - Tasks with an estimate over \$20,000 or 150 hours may be either depending on other material
 - Tasks with an estimate under \$20,000 and 150 hours generally will be a Change Request
- H. Upon completion of the investigation, Vendor sends the Technical Design modifications for WSP review. WSP modifies the Technical Design or approves it through the WSP System Manager.

I. Change Request

- (1) Upon acceptance of Technical Design changes, WSP directs Vendor to proceed with work
- (2) The Vendor performs task work and reports hour consumption versus earlier estimates and current hours to complete. If consumed hours and to-complete hours total more than estimated hours by more than 20%, Vendor and WSP must discuss next steps including the possibility of conversion to a Statement of Work .
- (3) WSP shall reimburse Vendor for Time and Materials hours worked according to Schedule A Price List, PROVIDED all requirements contained in the Change Request are corrected or met.

J. Statement of Work

- (1) WSP prepares more complete specification of task to be accomplished.
- (2) Vendor prepares draft technical design, project plan with deliverables, schedule, and cost including travel, and a preliminary estimate price revision to the Maintenance Contract. The final price revision is provided after completion of the Statement of Work development.
- (3) WSP reviews draft technical design, project plan, schedule, and costs.
- (4) WSP can request changes to design and plan.
- (5) Vendor reviews design, plan, schedule, and costs after changes.
- (6) Vendor goes through approval procedures for fixed cost agreement and returns to WSP.
- (7) WSP agrees by submitting for approval as personal services contract amendment.
- (8) Upon approval, WSP signs and sends to Vendor.
- (9) Work commences
- (10) Payment is made as deliverables are completed and accepted

This template can be used for problem reports, change requests, order of magnitude requests, and Statement of Work initiation. Elements of the form template can be modified by mutual agreement of the WSP System Manager and the Vendor Project Manager.

WSP Identifier:	Date of Report:	Reported by:		
Date of Problem:	Problem Was Found In:		Problem Reported By:	
Description				
Desired Solution:				
Priority (check one):	Mission Critical	High	Medium	Low



Appendix J

Certifications and Assurances

Appendix J – Certifications and Assurances

CERTIFICATIONS AND ASSURANCES

I/we make the following certifications and assurances as a required element of the proposal to which it is attached, understanding that the truthfulness of the facts affirmed here and the continuing compliance with these requirements are conditions precedent to the award or continuation of the related contract(s):

1. I/we declare that all answers and statements made in the proposal are true and correct.
2. The prices and/or cost data have been determined independently, without consultation, communication, or agreement with others for the purpose of restricting competition. However, I/we may freely join with other persons or organizations for the purpose of presenting a single proposal.
3. The attached proposal is a firm offer for a period of 180 days following receipt, and it may be accepted by WSP without further negotiation (except where obviously required by lack of certainty in key terms) at any time within the 180-day period.
4. In preparing this proposal, I/we have not been assisted by any current or former employee of the state of Washington whose duties relate (or did relate) to this proposal or prospective contract, and who was assisting in other than his or her official, public capacity. (Any exceptions to these assurances are described in full detail on a separate page and attached to this document.)
5. I/we understand that WSP will not reimburse me/us for any costs incurred in the preparation of this proposal. All proposals become the property of WSP, and I/we claim no proprietary right to the ideas, writings, items, or samples, unless so stated in this proposal.
6. Unless otherwise required by law, the prices and/or cost data which have been submitted have not been knowingly disclosed by the Proposer and will not knowingly be disclosed by him/her prior to opening, directly or indirectly to any other Proposer or to any competitor.
7. I/we agree that submission of the attached proposal constitutes acceptance of the solicitation contents and the attached Personal Service Contract General Terms and Conditions. If there are any exceptions to these terms, I/we have described those exceptions in detail on a page attached to this document.
8. No attempt has been made or will be made by the Proposer to induce any other person or firm to submit or not to submit a proposal for the purpose of restricting competition.

Signature of Proposer

Title

Date



Appendix K Glossary

Appendix K – Glossary

The following definitions will assist the reader in understanding the meaning of unique terms or words used in this RFP:

Term	Definition
ACCESS	A Central Computerized Enforcement Service System. A computer message switching system operated by the Washington State Patrol.
Access Control	The process that limits and controls access to resources of a computer system; a logical or physical control designed to protect against unauthorized entry or use.
Access Rights	Also called permissions or privileges, these are the rights granted to users by the administrator or supervisor. Access rights determine the actions users can perform (e.g., read, write, execute, create and delete).
Antivirus Software	Applications that detect, prevent and possibly remove all known viruses from files located in a microcomputer hard drive.
Authentication	The act of verifying the identity of a user and the user's eligibility to access computerized information. Authentication is designed to protect against fraudulent logon activity. It also can refer to the verification of the correctness of a piece of data.
CCH	Computerized Criminal History.
CJIS	The FBI's Criminal Justice Information Services.
COTS	Commercial off The Shelf. A product that is generally available and that will operate with little or no modification in the desired environment. These product types by definition are already fully developed.
CSA	Criminal Justice Information Systems Agency.
CSO	Criminal Justice Information Systems Officer.
CSC	Computer Sciences Corporation.
Data Security	Those controls that seek to maintain confidentiality, integrity and availability of information.
DIS	Department of Information Services.
Encryption	A technique used to protect the plaintext, by coding the data so it is unintelligible to the reader.
Ethernet	A communications methodology commonly used to connect workstations on a Local Area Network. Provides protocols to ensure that data is sent to the correct workstation, and to handle any temporary error situations. May operate at speeds up to 10 Mbits per second.

Term	Definition
Fault Tolerant	A computer architecture in which a catastrophic failure of a component (e.g., a CPU failure) does not affect the operation of the system as a whole. Program execution is unimpeded by the failure. This architecture requires that each component be duplicated and that all operations occur on a mirrored basis to allow continuous operation.
Firewall	A device that enforces security policies for traffic traversing to and from different network segments. A firewall no longer only protects an organization from the Internet, but also protects sensitive segments within organizations.
GJXDM	Global Justice XML Data Model. http://www.it.ojp.gov/jxdm/ .
Hit	In the context of the ACCESS project a "hit" on a Subject record occurs when an inquirer requests contact information related to the Subject record. The inquirer would have previously elected to view the subject record as a result of a query. In a broader context, a "hit" occurs when a search of the database finds a record which meets pre-described thresholds in matching the search criteria.
Hot File	Database file containing information about wanted persons, stolen vehicles, etc., that is of interest to state and national authorities. Must be maintained very accurately to avoid wrongful detention of subjects. Must also allow for very quick query access.
III	Interstate Identification Index. An index that keeps track of the detail records for subjects with criminal histories. The index is currently located in Washington, D.C., and is maintained by the US Department of Justice, Federal Bureau of Investigation, and Criminal Justice Information Systems.
Intelligent	An end user terminal that can perform some local processing and can store some terminal processing commands.
IGN	Intergovernmental Network.
ISB	Information Services Board.
LAN	Local Area Network. A combined hardware/software technology that permits workstations to communicate with each other and share database files and processing. LAN's are probably the dominant future architecture for the Law Enforcement environment.
LCJA	Local Criminal Justice Agency.
Level 1 User	Users who have authority to enter inquiry transaction records into the system
Level 2 User	Users who have authority to enter, modify, and delete departmental records.

Term	Definition
MDC	Mobile Data Computer. An end user device (often installed in an automotive patrol car environment) that has intelligent processing, image display and expansion into extended functions such as image capture. Functionally similar to an end user PC device. Contrast with MDT.
MDT	Mobile Data Terminal. An end user device (often installed in an automotive patrol car environment) that has little or no intelligent processing, and cannot be expanded. Functionally similar to a "Fixed Function Terminal."
MFC	Message Field Code. A string of data, usually three characters followed by a slash (/) that defines the purpose of the following characters, which are the contents of a data element. This data (e.g., "SER/") is provided by a requester in the input message. For example, to define a data element for a serial number of a gun to be "123456789", the string of "SER/123456789" would be entered.
MSS	Message Switching System.
NCIC	National Crime Information Center. A data center operated by the US Department of Justice, Federal Bureau of Investigation. NCIC is a repository for wanted persons, stolen vehicles, etc., of interest to state and national personnel. NCIC provides "hot file" access nationwide, although the data entered actually belongs to the agency that entered it.
NCIC III	A colloquial term for the III files maintained and accessed via NCIC. III files are accessed via NCIC, but are actually on a different computer system.
NCIC-2000	A federal initiative to upgrade the NCIC system and to extend the services provided. First portion scheduled for implementation in March 1995, with all States required to convert to the NCIC-2000 standards by March 1998.
NIEM	National Information Exchange Mode.
NLETS	The International Justice and Public Safety Information Sharing Network. This is a non-profit corporation that provides a computerized message switching interconnection among all states and other external agencies. Used for all interstate communication traffic.
NOAA	National Oceanographic and Atmospheric Administration.
NWWS	NOAA Weather Wire Service.
Operating System	A master control program that runs the computer and acts as a scheduler and traffic controller. It is the first program copied into the computer's memory after the computer is turned on and must reside in memory at all times. It sets the standards for the applications programs that run in it.

Term	Definition
Record Owner	System user who has entered a Subject record into the ACCESS database. The record owner is responsible for maintaining the record, and is the point of contact for supporting documentation.
Record Supervisor	Responsible for overseeing all subject records and record owners belonging to the agency/organization. There is only one record supervisor per agency or organization. The record supervisor has authority to make changes to any record belonging to the organization.
RISS.net	Regional Information Sharing Systems Nationwide Network. RISS.net is a secure intranet composed of <i>six regional centers</i> that share intelligence and coordinate efforts against criminal networks that operate in many locations across jurisdictional lines. Typical targets of RISS activities are drug trafficking, terrorism, violent crime, cyber crime, gang activity, and organized criminal activities. Each of the centers, however, selects its own target crimes and the range of services provided to member agencies.
SGN	State Government Network.
SOR	Sex Offender Registry.
System Administrator	Person who has authority to permit access to the system and perform all other administrative functions for the system.
TAC	Technical Agency Coordinator.
TCP/IP	Transmission Control Protocol/Internet Protocol. Two related communications protocols that permit logical connections between disparate computing systems. TCP/IP is notable as it is non proprietary and can use various different physical transmission media, and provides a rich set of services.
Virus	Malicious programs designed to spread and replicate from computer to computer through telecommunications links or through sharing of computer diskettes and files.
WACIC	Washington State Crime Information Center. A data center operated by the Washington State Patrol. WACIC is a repository for wanted persons, stolen vehicles, etc., of interest to state and national personnel.
WASIS	Washington State Identification System. A data center operated by the Washington State Patrol. WASIS is a repository of Criminal History information for state and national personnel.
WebMSS	Web-enabled message switch system user interface to ACCESS.
WSP	Washington State Patrol.
XML	Extensible Markup Language – A markup language is a mechanism to identify structures in a document. The XML specification defines a standard way to add markup to documents.