Caliber Public Safety

CALIBER
Public Safety

Washington Association of Sheriffs & Police Chiefs

NIBRS State Repository Replacement

RFP CJIS-2016-01

Due Date: April 22, 2016

Caliber Public Safety, a business unit of Harris Systems USA, Inc.

2429 Military Road, Suite 300 | Niagara Falls | NY | 14304

Phone: 716.297.8005 | Fax: 716.297.4499 | www.caliberpublicsafety.com

CALIBER Public Safety

Table of Contents

In accordance with *1.14 Number of Proposals* in the RFP instructions, only one copy of the Appendix reports/materials needs to be submitted. Therefore, only the binder marked "ORIGINAL" will contain these documents.

CALIBER
Public Safety

April 20, 2016

Ms. Joan L. Smith, CJIS Manager
WASPC
3060 Willamette Drive NE
Lacey, WA 98516

RE: NIBRS Project RFP CJIS-2016-01

Dear Selection Committee:

Caliber Public Safety[1] (CPS) is excited to submit the attached proposal in response to the Washington Association of Sheriffs & Police Chiefs (WASPC) RFP for a National Incident-Based Reporting System (NIBRS) State Repository. We have thoroughly reviewed the RFP requirements, understand the scope of the work to be performed, and accept the requirements as stated. We are confident in our ability to meet or exceed your expectations.

We have proposed the Caliber NIBRS State Repository. Our solution integrates seamlessly into the state's infrastructure and is configurable to meet each unique data requirement. No other vendor can offer you comparable product capabilities and competency with their NIBRS repository system, as we will show you in this proposal.

Harris Systems USA, Inc. will execute all legal documents pertaining to this RFP or any subsequent documents. This proposal is valid for 120 days from the proposal due date of April 22, 2016. By affixing my signature below, I attest that all information provided in response to this RFP is true and accurate and that I am authorized to obligate Harris Systems USA, Inc. contractually and negotiate the contract on their behalf.

If you have any questions or need further information, please feel free to contact Terri Somers, Regional Sales Executive, at 925-876-8074 or tsomers@caliberpublicsafety.com. We look forward to the opportunity to talk with you more about the proposed solution and how we can help you achieve your goals.

CPS acknowledges receipt of Vendor Questions and WASPC answers dated April 1, 2016.

Sincerely,

James Simak
Senior Executive Vice President
Harris Systems USA, Inc.
314-802-5158 ext. 76100

---

[1] Caliber Public Safety is a business unit of one of Constellation Software Inc.'s (TSX:CSU) operating groups. Harris Systems USA, Inc. is a subsidiary of Constellation and is one of the legal entities that markets and distributes software products and services under the Caliber Public Safety ("Caliber") platform.

Appendix B: Nondisclosure Agreement

Nondisclosure Agreement

NOTE: This should be considered an example agreement; WASPC may modify this agreement before or during contract negotiations.

In consideration of the Washington Association of Sheriffs and Police Chiefs (WASPC) retaining the services of CALIBER PUBLIC SAFETY, a business unit of HARRIS SYSTEMS USA, INC., (Vendor) and because of the sensitivity of certain information which may come under the care and control of Vendor, both parties agree that all information regarding WASPC or the National Incident-Based Reporting System (NIBRS); or gathered, produced, or derived from or accessed as a result of the Contract (hereinafter "Confidential Information") must remain confidential, subject to release only by written permission of WASPC, and more specifically agree as follows:

1. The Confidential Information may only be used by Vendor to assist Vendor in its Contract with WASPC.
2. Vendor will not, at any time, use the Confidential Information in any fashion, form, or manner except in its capacity as a Vendor to WASPC.
3. Vendor agrees to maintain the confidentiality of any and all deliverables resulting from the Contract in the same manner that it protects the confidentiality of its own proprietary products.
4. The Confidential Information may not be copied or reproduced without WASPC's written consent.
5. All Confidential materials made available to Vendor, including copies thereof, must be returned to WASPC upon the first to occur of; (a) completion of the project, or (b) request by WASPC.
6. The foregoing does not prohibit or limit Vendor's use of the information including, but not limited to, ideas, concepts, know-how, techniques and methodologies (a) previously known to it, (b) independently developed by it, (c) acquired by it from a third party, or (d) which is or becomes part of the public domain through no breach of this agreement by Vendor.

7. This agreement becomes effective as of the date Confidential Information is first made available to Vendor and survives the Contract and is a continuing requirement.

8. Breach of this Nondisclosure Agreement by Vendor shall entitle WASPC to immediately terminate the Contract upon written notice to Contractor for such breach. The parties acknowledge the measure of damages in the event of a breach of this Nondisclosure Agreement may be difficult or impossible to calculate, depending on the nature of the breach. WASPC does not waive any right to seek additional relief, either equitable or otherwise, concerning any breach of this Agreement.

[Signature and Printed Name of Vendor required]

By: _____

James Simak

Title: Senior Executive Vice President

Date: April 20, 2016

Section 1 – Proposal Executive Summary

Look to Caliber Public Safety for your Next Generation NIBRS State Repository

Caliber Public Safety (CPS) is your trusted partner with the experience, expertise, and forward-looking initiatives to ensure federal reporting compliance. Recognized nationally as NIBRS subject matter experts, CPS stays current with NIBRS issues by not only maintaining regular contact with the FBI database management team involved with building and servicing the national system, our representatives also sit on the IJIS CPAC subcommittee where they work closely with other experts to examine and update the NIBRS standards. We are motivated to lead the way in providing a Next Generation NIBRS Repository.

Experience

Over 15 years of State Repository Experience:

- Successful implementations, generally completed in less than six months, are what set CPS apart.
- With the lowest NIBRS error rate, CPS can be counted on to tackle your most difficult challenge and do so with a reliable, affordable solution.
- CPS offers the ability to provide a hosted solution at Nlets, the nation's largest interstate justice and public safety network, a strategic partner since 2008.
- WASPC legacy system expertise – as the current incumbent vendor as a result of our acquisition of TAC.10, CPS has deep subject matter expertise on the WASPC legacy system and current submission formats and business rules. Combining the in depth level of knowledge on the current system with the best practices of the CPS project management and client services organizations makes CPS uniquely qualified to ensure both a successful implementation and long term customer satisfaction.

We look to leverage our experience as the leader in deploying cloud solutions to deliver a turnkey hosted solution for all our UCR/NIBRS clients.

Technology

An Industry Leader:

- Our solution is built upon a proven .NET browser-based software architecture leveraging the latest technologies to provide a state of the art platform.
- Nlets hosting option. CPS is an Nlets strategic partner and has been hosting public safety agency customers for over 8 years from the Nlets data center. We have built a state of the art infrastructure platform at Nlets and have proven experience hosting customers efficiently, securely, and cost effectively.
- Our solution is 100% web-based so all users access the system using a standard web browser. No client application is needed on the workstations for WASPC agency users or for users from the local law enforcement agencies, simplifying administration and improving accessibility.
- N-DEx Compatible. CPS provides for the capability for your agency to submit N-DEx data directly to the FBI from your NIBRS Repository.
- Small Agency Records Management Solution. Provides smaller agencies the ability to record their full incident and arrest information. The forms engine allows for data collection form set-up with the ability to customize reports in very little time.

We have significant investment planned to advance our platform further, thus continuing to solidify our position as the premier UCR/NIBRS reporting solution on the market.

Value

Caliber's Overriding Objective – Deliver Maximum Value:

- Built with an open architecture design to integrate seamlessly into the state's infrastructure.
- Structured for dual error checking at both the state and federal level.
- Based upon modular components, configurable to meet the unique needs of the state.
- Ad hoc query and reporting built directly into the application and controlled by our security.
- Easy to learn and use while offering powerful tools for data analysis.
- Nlets hosting option – provides a very cost effective turnkey platform with >99.99% uptime and CJIS level security.

Our State Repository solution includes all data elements from the Federal NIBRS Volume I Data Collection Guidelines. The NIBRS Verification Module is compliant with the Federal NIBRS Volume IV Error Message Manual. State-specific data is input and validated according to each state's individual guidelines. The Data Extraction Module uses the Federal NIBRS Volume II Data Submission Specifications.

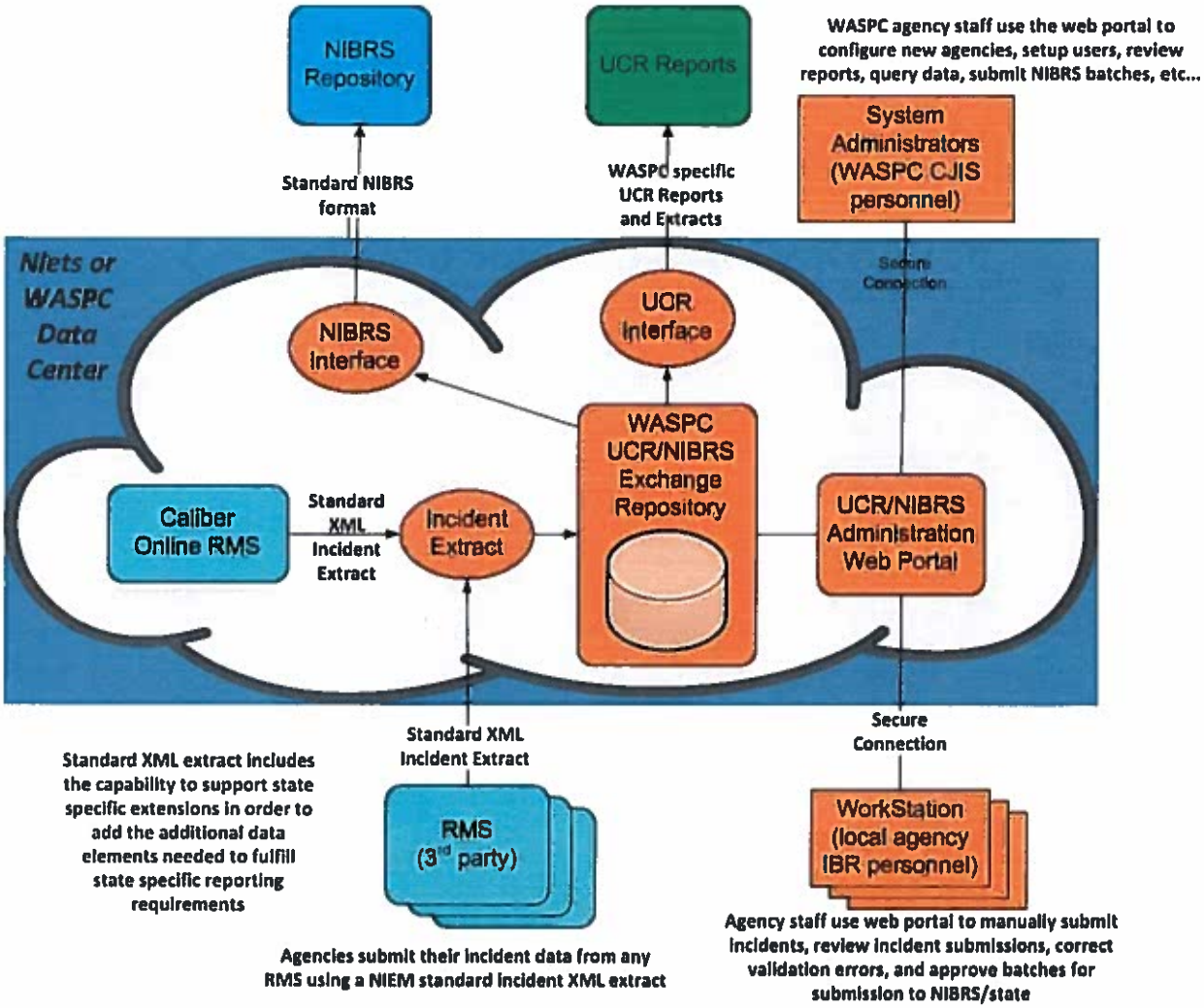
Not current manuals

Section 2 – Technical Solution and Description

Solution Overview

CPS proposes to deliver a complete solution for WASPC that will provide a 100% web-based interface for both WASPC agency personnel and the NIBRS/UCR personnel from all local and state law enforcement agencies. The UCR/NIBRS repository may be hosted by WASPC in a state operated data center or, as an option, it may be hosted in our CJIS secure data center operated by our Nlets strategic partner. The proposed system will support both UCR summary reporting and NIBRS incident based reporting.

The following diagram provides a high level overview of the system components:



2.1 Basic Requirements

The proposed system shall conform to the National Incident-Based Reporting System (NIBRS) requirements as defined by the FBI in the current versions (as of the signed contract date) of the NIBRS Technical Specification and NIBRS User Manual available at https://www.fbi.gov/about-us/cjis/ucr/ucr-program-data-collections#National. (If the current Technical Specification on the FBI website is Version 2.1, refer to list of errors Appendix D of the RFP.)

It is mandatory that the state repository system shall provide the following functional capabilities related to NIBRS:

1. The system must provide the capability to capture and preserve all required NIBRS data elements as defined in the FBI NIBRS User Manual and as detailed in the FBI NIBRS Technical Specification (available https://www.fbi.gov/about-us/cjis/ucr/ucr-program-data-collections#National).

   CPS Response: We comply with this requirement.

2. The system must allow for the entry of the standard values for each data element in accordance with the values prescribed in the FBI NIBRS User Manual and as further addressed in the current version (as of the signed contract date) of the FBI NIBRS Technical Specification. (If the current Technical Specification on the FBI website is Version 2.1, refer to list of errors Appendix D of the RFP.)

   CPS Response: We comply with this requirement. We are aware of the errors in the 2.1 version of the specification. We are actively involved in the NIBRS standard and its ongoing evolution through membership on the IJIS CPAC committee.

3. The system must meet any additional Incident-Based Reporting (IBR) data collection requirements that are specific to the State of Washington. Appendix C of this RFP provides a detailed listing of all additional segments and/or data elements that the State of Washington requires.

   CPS Response: We comply with this requirement.

4. The proposed system must perform the editing and validation of data in accordance with the data quality rules prescribed in the FBI NIBRS Technical Specification, including all conditional validations as defined therein.

   CPS Response: We comply with this requirement.

5. The system must provide the capability for the submission of NIBRS reports in the form and format as prescribed in the current version (as of the signed contract date) of the FBI NIBRS Technical Specification and in accordance with any requirements specific to the State of Washington. (If the current Technical Specification on the FBI website is Version 2.1, refer to list of errors Appendix D of the RFP.)

   CPS Response: We comply with this requirement and will comply with any FBI changes to the NIBRS specification. CPS will maintain NIBRS compliance as part of our standard maintenance agreement.

6. Prior to final acceptance, the system-generated NIBRS reports must achieve State and FBI certification in accordance with the definitions provided in the FBI NIBRS Technical Specification and the criteria provided in the FBI NIBRS User Manual.

CPS Response: Our repository is NIBRS compliant and we will actively support all testing requirements to achieve state and FBI certification.

2.2 Preferences

A. Administrators and Users
   1. Local System Administrator and Users
      a. Levels of user privileges: administrator, power user, report generator.
      b. Local users should receive immediate notification when a file uploaded successfully or if there is a file upload error.
      c. A file upload error should indicate the reason for the error; i.e., naming convention, incorrect file format, incidents already on file, etc.
      d. If the file is a duplicate, the system should allow the user to cancel the upload.

CPS Response: We comply with these requirements A.1(a-d)

   2. State System Administrators
      a. A desired system feature includes a contacts database for State System Administrators (SSAs) to send messages, updates, and alerts (similar to a listserv); the contacts database should include such data elements as employee names, e-mail addresses, jurisdiction population, full-time employee counts, jail statistics (average daily population, average length of stay, bed rate), etc.

CPS Response: Our Agency forms can be enabled with these fields. Our inbox system can also be enabled which will allow for this functionality.

      b. The SSAs should receive notifications when file uploads stop, fail, or the file is a duplicate upload; the unprocessed file notification sent to local administrator should be sent as a "cc" to SSAs.

CPS Response: We comply. This feature will be enabled after the notification service is set up with an smtp email account. Our technicians will work with your agency to complete this set up.

      c. The SSAs must have the ability to produce standard, ad hoc, and crime mapping reports, charts, and graphs.

CPS Response: We comply. Charts and graphs are generated through Excel after the data is exported from our ad hoc report generator.

d. The SSAs must be able to monitor the system through a utilities function, including reviewing a system journal for incident activity, file uploads, file processing status (such as in queue, percentage completed, completed, and location in queue), and table updates, modifications, or deletions; it is desirable that SSAs have the ability to update data tables.

CPS Response: We comply. The application provides both a dashboard and an administrative user panel to provide SSAs with excellent visibility to repository operations and the ability to update configuration table settings.

e. The SSAs must be able to manage local user accounts, including the set-up or disabling of user profiles and re-setting passwords.

CPS Response: We comply with this requirement.

B. Data Entry and File Upload

1. Options for submission to state repository must include batch file upload and individual incident entry (IIE).

CPS Response: We comply with this requirement.

2. The individual incident entry (IIE) must have data validation on each data field.
   a. Data entry should be user friendly with drop-down tables relevant to either the incident or arrest data being entered.
   b. Missing mandatory fields or invalid data entry errors should highlight during IIE.
   c. The mandatory fields should highlight according to the offense.
   d. The user should not be able advance to next screen without completing mandatory fields.
   e. When the IIE is complete, the NIBRS check should list errors and return the user to screen and highlight the error(s).
   f. Any field with a date entry should allow the option to type the date or use a calendar.
   g. It is desirable that hot keys be available to facilitate data entry.

CPS Response: We comply with all of these requirements B.2(a-g). The system will highlight fields in a red box and take the user to the error on the Incident or Arrest. Mandatory fields are marked with a red label. Cntrl S saves a record from any location, Cntrl N will create a new record for the record type the user is currently on. Also, tab and shift tab navigate forward and back.

3. The sequence of IIE screens should be:
   a. Administrative; time entry must have a pop-up explaining "00" rule.
   b. Offense; with the ability to immediately enter Property associated with the offense.
   c. Victim; the Domestic Violence indicator should be associated with the Victim.
   d. Offender.
   e. Property.
   f. Arrestee.

CPS Response: We comply with all of these requirements B.3(a-f). Requirement B.3(a) will be developed for the project. All the other screens are already available and can be sequenced in any order as an agency configuration setting.

C. Data Reports

1. The system must provide report writing capability; the repository must include standard reports and the functionality to allow the user to create ad-hoc reports. The Vendor should elaborate on types of reports to be expected. Report samples will be appreciated.

   CPS Response: We comply with this requirement.

2. The system must output data to Microsoft Access, Excel, Word, and PDF in both report form and data form.

   CPS Response: We comply with this requirement.

3. Law Enforcement Agencies must have the ability to access other law enforcement agency data for report extraction.

   CPS Response: We comply with this requirement. This is controlled by permissions set up by SSA users.

4. The data reports should include but are not limited to:
   a. Ad hoc; a desirable feature would be user ability to design the report lay-out.
   b. Crime Mapping.
   c. Data Quality; these reports are for use by the SSAs and local agency contributors to audit data quality.
   d. Standard Reports; including Summary of Offenses, Summary of Offenses - Domestic Violence, Offenses by Location, Arrests by Offense and Age Category, Hate Crime, Activity Log (ability to choose by month or year), Outstanding Errors and Incidents/Arrest Not Checked.
   e. Static report (snapshot) of the database for the *Crime in Washington* (annual crime report); including a "Save As" function with ability to change dates/ranges for the *CIW* or other specialty reports.

   CPS Response: We comply with these requirements C.4(a-e). In addition to the standard reports, the application includes both an ad hoc reporting tool and a master search and reporting feature. The product also features a batch data report and a dashboard that allows SSAs to view admin stats on recent submissions, late submitters, submission errors, and data quality. CPS will provide a static snapshot of the database to WASPC annually to support the annual crime report.

D. Data Validation and Error Notification
   1. The system must meet all FBI and Washington State data validation edits, perform thorough error-checking, and automatically send electronic error reports back to the submitting agency.
      a. The State System must perform data validations and locate errors before the file goes to the FBI.
      b. In addition to the batch error upload report being sent automatically to the submitting agency, it should be available for retrieval by a Local or State System Administrator.
   2. Incidents with errors should be included in Ad Hoc and Summary Reports (do not exclude or omit incidents with errors from the data reports).
   3. There should be an ability to easily edit the FBI error messages to make them more user-friendly and understandable; error messages must be clearly stated.
   4. There should not be a Time Windows error.
   5. The Error Report list:
      a. Should not include "outside of base date" comment (unable to correct, so don't display).
      b. Should not include errors without case number (unable to access, so don't display).

CPS Response: We comply with all of these requirements (D.1-5). Requirement D.3 will be developed for the project and added to the admin tools section.

E. State System
   1. The system must authenticate access with differing levels of users as defined by WASPC; access must be based on user profiles (user names and passwords).
   2. The system must provide the State System Administrators (SSAs) the ability to designate roles and responsibilities for other administrators and users.
   3. The system must allow the SSAs the ability to enter and update system data directly through the application.
   4. There must be at least two (2) databases available:
      a. Training database; a duplicate of the Production database with data field descriptions available when hovering.
      b. When files, incidents, or arrests are uploaded or entered to the Training database for certification or test purposes, the SSAs should have the ability to transfer the files, incidents, or arrests to the Production database.
      c. Production database; with permanent statistical archive ability.

CPS Response: We comply with all of these requirements (E.1-4). Our application supports both role base security and the ability to assign users to separate organizational units. Requirement E.4(a) for data field descriptions available when hovering will be developed for the project.

F. System Features
   1. The system must automatically discover NIBRS batch submissions; the schedule is State user-defined.
   2. The system must provide batch submissions or individual incident entry to state repository via a web browser.
   3. The data must be available for data reports after State Repository acceptance of the file.

   a. Once data are entered, uploaded, modified, or deleted, it should be immediately available for reports (regardless of whether the FBI Error Data Set [EDS] has been received and processed).
4. The Domestic Violence (DV) indicator is mandatory, relevant to all offenses, and should be associated with the Victim.
   a. It is desirable that the DV indicator default based on certain victim relationships to offender, for example, "Spouse".
   b. If a default is triggered, a desirable feature for users would be a pop-up window asking, "Are you sure ...?"
5. The Gang Involvement indicator is mandatory.
6. All related cases should be displayed for the Multiple Clearance indicator; the user should have the ability to delete a case number if necessary.
7. It is desirable that any data value that is not applicable to Washington State or utilized by the FBI be "greyed-out" or eliminated; for example, "Common Law Spouse" is not applicable in Washington State and Property Type "99" is not used by the FBI. These data values to be determined during system implementation.
8. For data entered via the IIE, a system journal should be available for State System Administrators (SSAs) in order to track when and who entered, updated, or deleted an incident.
9. A desirable feature for users would be a pop-up window asking, "Are you sure ...?"
10. The system must store and provide a journal of agency information, error rates, and agency submission status; these data must be available to the SSAs via a Utilities or Maintenance menu.
11. The Zero Report function:
    a. Should allow an agency to enter a Zero Report even if the file contains a correction or update from a previous month's case.
    b. Should allow an agency to override a Zero Report month if an incident is now available for that month.
12. A desirable system feature is the ability to convert NIBRS data to Summary data for comparison during the NIBRS certification process; the system should produce Summary data from the submitted NIBRS data by agency, month, and year.

CPS Response: We comply with all of these requirements (F.1-12). Our system has a full audit history with an audit wizard available to show all activity relating to a record in the system. Our system has the ability to generate summary data and counts from NIBRS records.

G. Vendor Responsibilities
1. The Vendor must have a state repository system that is FBI certified in at least one state at time of Vendor's RFP response.

   CPS Response: We comply with this requirement. Our platform is currently FBI certified in four states.

2. The Vendor's system must be FBI submission-capable.

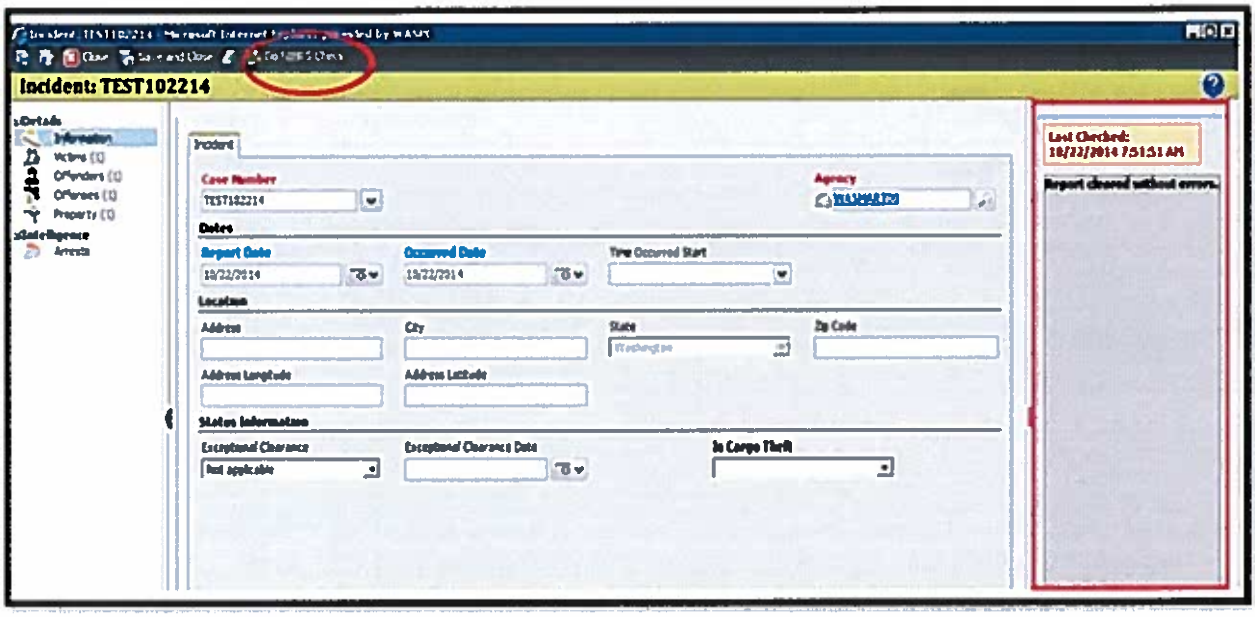
   CPS Response: We comply with this requirement.

3. The Vendor must have minimum of two years' experience with NIBRS repository development.

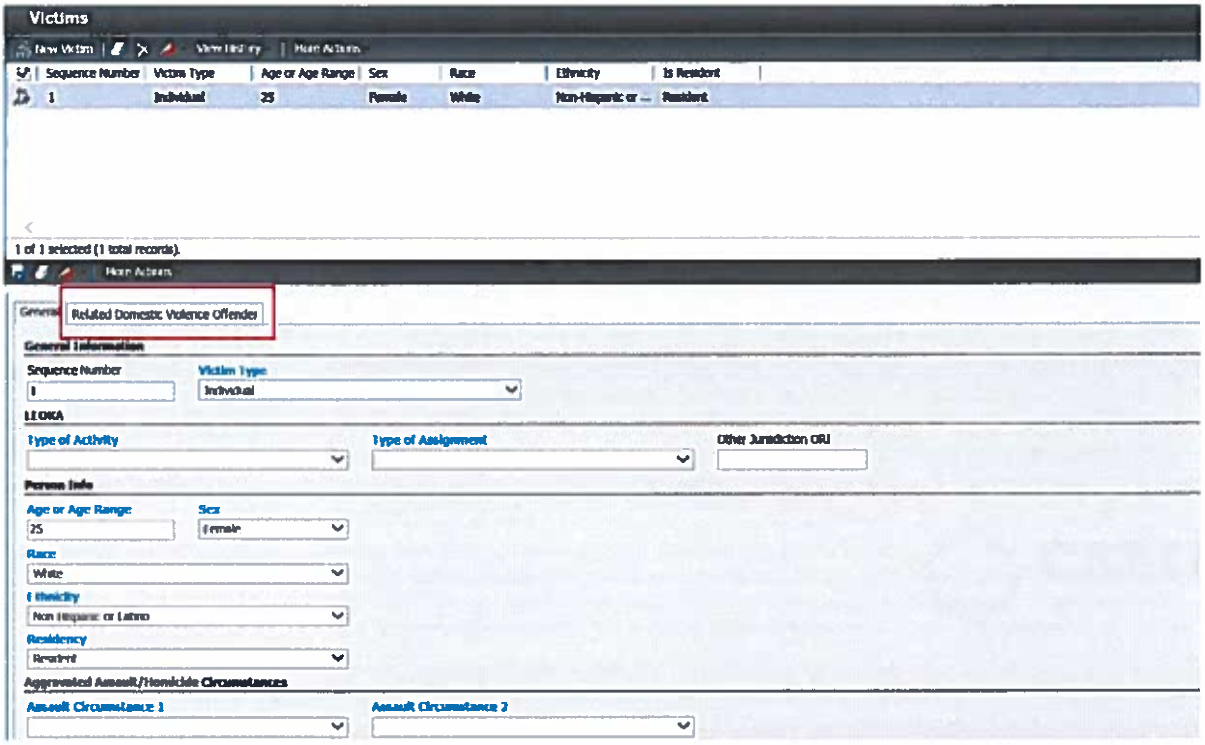
   CPS Response: We comply with this requirement. We have over 15 years of NIBRS repository experience.

4. The Vendor is encouraged to present logical solutions and proposed record layouts for additional Washington State data values.

   CPS Response: We will create a template layout for Washington State data values. Utilizing our forms engine, any adjustments can be performed directly on the installed system by SSAs. The following screenshots depict state specific fields. The application forms engine will allow adjustments to be made to meet WASPC requirements.



Here, we inline the location fields into the incident form that Washington collects.



The Domestic Violence Code will be moved from the offense to the Offense/Victim relationship. Users can add offender relationships to the victim from the tab and the system will mark those relationships as domestic violence.

5. The Vendor must include their Record Layout and Report Samples in the technical section.

   CPS Response: The record and report samples may be referenced at the following link: http://acic.org/crimeStatistics/Pages/default.aspx. Any additional information will be provided upon request.

6. The Vendor must have Customer Service availability: Monday through Friday, 8am-4pm, Pacific Time.
   a. Customer Service includes a process for Work Order Number assignment.
   b. It is desirable that the State System Administrators have the ability to check the status of a work order via an on-line tracking system.

   CPS Response: We comply with these requirements. Customer Service is available 24x7x365. CPS utilizes a ticket tracking system to record all support requests and work orders. A customer self-service portal is available for checking the status of open tickets.

7. The Vendor must be able to edit the system as the national UCR Program requires without additional cost to the State of Washington.
   a. The Vendor should establish a desired protocol for notification to the Vendor when there is an update of the FBI and/or State technical specifications.

   CPS Response: We comply with this requirement. When new requirements are released by the FBI, our process is to program these requirements into our platform with a new feature activation flag. We will schedule a meeting with WASPC to review the new requirements and new system functionality and, together, work out a plan for deploying to both the testing and production servers. Our normal sequence is to activate the feature in testing first so that it may be tested and verified by WASPC and then schedule a date for activating the feature in production.

8. The Vendor must update the repository software or tables in timely manner or allow State System Administrators to update tables.

   CPS Response: We comply with this requirement using the process described above for G.7.

9. The Vendor must provide user-friendly electronic manuals, error messages, and pop-up windows.

   CPS Response: We comply with this requirement.

10. The Vendor must provide comprehensive user and technical personnel training.

    CPS Response: We comply with this requirement. Our proposal includes the following training classes:
    - Administrator training for WASPC personnel.
    - Train-the-trainer classes for WASPC trainers responsible for training local agency UCR/NIBRS personnel.
    - Technical training for WASPC technical staff responsible for managing the technology platform. (Note: This class is not required if EASPC chooses the Nlets hosting option.)

11. Vendors are responsible for specifying each hardware component necessary to satisfy the requirements of this RFP; however, all required hardware and system software will be procured by WASPC. Specifications are to be detailed enough to allow WASPC to provide the necessary equipment.
    a. Server storage capacity should be estimated for five years of use.
    b. The server operating system must be compatible with Windows Server 2008 or higher.
    c. The server database software must be compatible with Windows SQL Server 2010 or higher.

    CPS Response: We comply with these requirements. Our current standard versions are Windows Server 2012 and SQL Server 2012 but the system is compatible with Windows Server 2008 and SQL Server 2008. The recommended hardware specifications are listed below and include sufficient storage capacity for at least 5 years of use.

Database Server		Web Server		Application Server	
Minimum	*Preferred*	*Minimum*	*Preferred*	*Minimum*	*Preferred*
Windows Server 2012/2012 R2		Windows Server 2012/2012 R2		Windows Server 2012/2012 R2	
2.4 GHz	Quad Core 2.39 GHz	2.0 GHz	Quad Core 2.39 GHz	2.0 GHz	Quad Core 2.39 GHz
8 GB	20 GB	8 GB	12 GB	8 GB	8 GB
100 GB	500 GB	100 GB	500 GB	100 GB	500 GB
100/1000 NIC		100/1000 NIC		100/1000 NIC	
SQL Server 2012/2014 Standard or Enterprise with Reporting Services		IIS 6 or greater; .NET 4.0 Framework (Full Version)			

2.3 Add-On Components

1. Web-browser: Although this is an add-on component, it is a mandatory feature. Submitting agencies must be able to submit and query their data and generate and print data reports.

   CPS Response: We comply with this requirement. All application user interfaces are provided as a web application that runs in a standard web browser so no client software installation is required. This is true for both WASPC users as well as local agency users.

2. Crime Mapping: This is not a mandatory feature. The crime mapping component should be part of the web-browser with the submitting agencies able to query their own crime maps. This needs to function on address or latitude/longitude geocodes; it may require an additional element be added to the NIBRS system. This must be priced separately from the web-browser.

   CPS Response: We will comply with this requirement. The agency has a couple of options regarding crime mapping:

   a. Utilize the existing interface to Bair RAIDSOnline. This existing interface will be provided at no additional charge.
   b. CPS has proposed an optional crime mapping component as part of our response. This will include a state branded portal that will utilize ESRI web mapping. This feature will be available to both WASPC and local agency users.

3. Data Migration - This is a mandatory feature. The system must accept the data values from the current state repository; this includes data validation and access to historical data for report compilation.

   CPS Response: We comply with this requirement. We have successfully completed multiple data migrations from our legacy repository to our new repository for other state customers.

Section 3 – Project Management Description

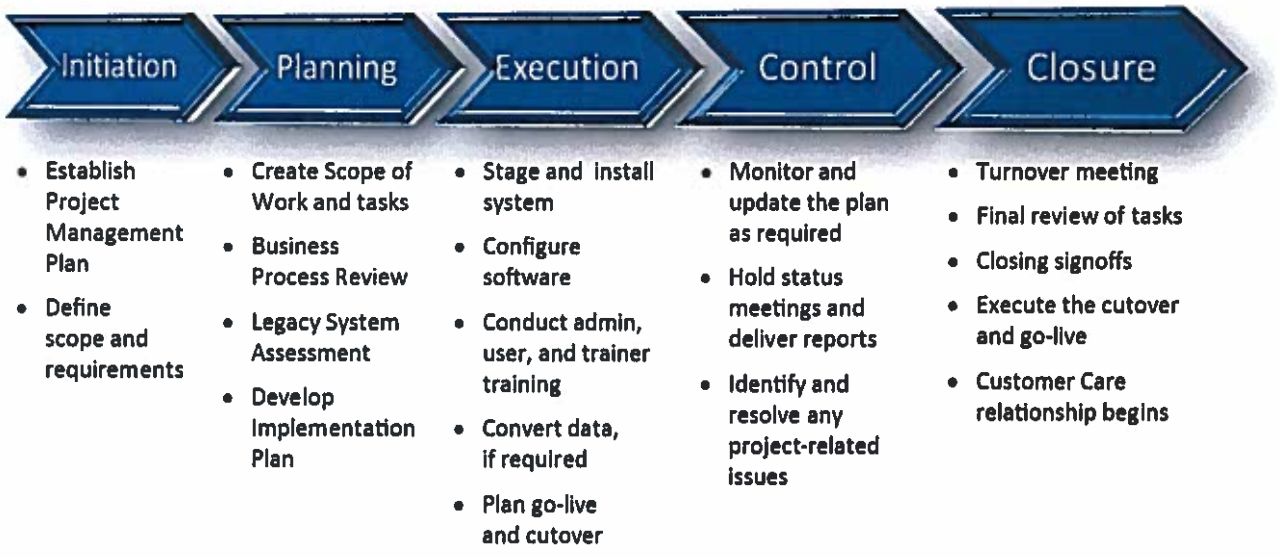
3.1 Project Plan

Vendors must include a plan for implementing the project described in this RFP. The plan must be comprehensive in scope and detail to convey the Vendor's ability to manage this project. The plan shall include project tasks, approximate dates, and time in hours required to complete each task. The ability of the Vendor to manage all aspects of this project is a critical factor.

CPS Response:

Our project methodology focuses on utilizing defined industry and program management best practices. The methods are process- and activity-based and include key roles based on the Project Management Body of Knowledge (PMBOK) and the System Development Life Cycle (SDLC). The implementation approach will follow the SDLC in concert with WASPC-specified tasks and deliverables. The following figure illustrates the proposed phased approach; each phase identifies the activities, tasks, and work products required to consistently deliver repeatable results. CPS, in collaboration with the WASPC project team, will define and follow formal quality and review procedures.

The implementation methodology consists of five phases:



Phase 1: The Project Initiation Phase

During this phase of the project goals are set, constraints are identified, and the project teams are put in place. Specific information about your agency that was learned and gathered during the sales cycle will be used as a basis for the activities during this initial and important phase as it will serve as the foundation for the remainder of the project. Specific activities include:

- Establish the project management plan
- Identify key stakeholder and project team members and their relevant roles
- Establish program governance and steering team
- Establish change management and approval process
- Establish risk and issue management process
- Establish communication process and tool
- Define Scope and Contractual Requirements
- Review project scope and contract deliverables/milestones
- Review and discuss program phasing and preliminary schedule
- Discuss internal and external dependencies and limitations
- Conduct risk assessment and develop preliminary risk profile
- Develop mitigation plan and establish critical success factors

Phase 2: The Planning Phase

During this phase, the client and our team work together to document the scope of the project and create a list of implementation tasks necessary for project success. Steps included in this phase are:

- Hold Project Kickoff Meeting
- Conduct BPR sessions to document operational requirements
- Assess legacy system and determine data migration requirements
- Collect and prepare data
- Develop blueprint for data setup and operational workflow
- Identify and define customizations, if applicable

Phase 3: The Execution Phase

- Configure three separate application environments:
  - Training
  - Testing
  - Production
- Confirm remote connectivity
- Convert data from legacy applications
- Configure software
- Implement change management processes
- Train system administrators
- Train end users

- Plan the go-live and cutover process
  - Phased approach
    - Base System: System data converted from WASPC legacy UCR/NIBRS repository. Configuration complete and reports verified.
    - Pilot Phase: Begin LEA RMS data submissions with a set of test agencies. Process submissions for both UCR and NIBRS and verify correctness of the results. Use the data submitted in this phase for the FBI certification process.
    - Full Production Phase: Continue to add new LEAs into the submission process based on training and operational readiness.

Phase 4: The Control Phase

This phase occurs in conjunction with the Execution Phase and consists of constant monitoring by the CPS Project Manager. Some specific tasks of this phase include:

- Monitor and update the project plan
- Ensure quality communication
- Conduct status meetings and provide status reports
- Identify any project-related issues and find resolutions
- Document project change requests

Phase 5: The Closing Phase

The final phase of the project occurs when all tasks are finished and the project is complete. An important element of this phase is the conclusion of services by the Implementation Team and the transition of ongoing client support to our Technical Support Team.

- Execute the cutover and go live
- Final review of tasks and verify all deliverables are met
- Turnover meeting to Technical Support
- Client services relationship begins

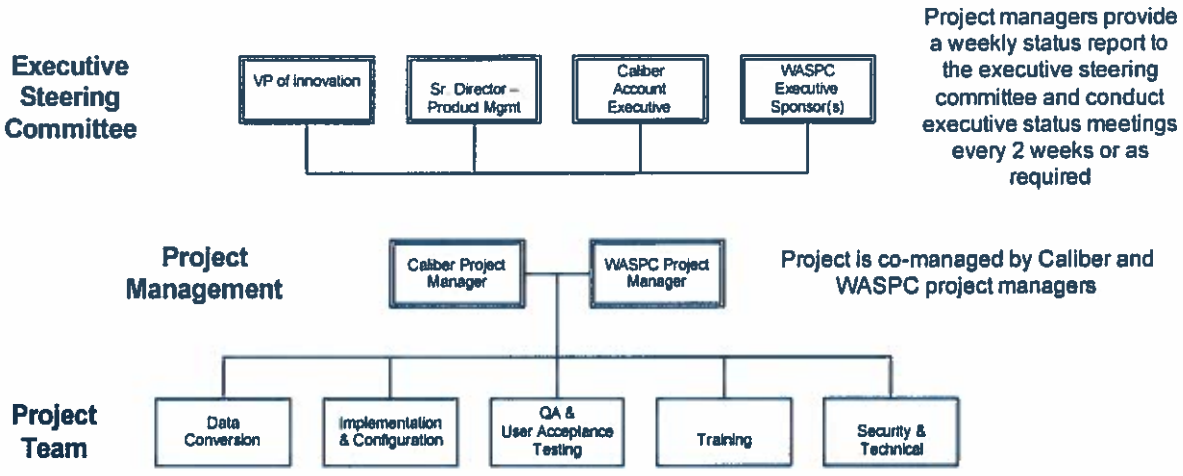
Project Team

The organization of the project team is a critical success factor for any large scale project. At CPS, we employ a collaborative project management model that pairs the CPS project manager with a client project manager in a co-management model. The project team is composed of functional groups that include both CPS and WASPC personnel as required for the specific tasks.

The project team is supported by an executive steering committee that includes CPS executive sponsors, the CPS account executive, and WASPC executive sponsor(s). The objective of the steering committee is to oversee the project to ensure a successful implementation and confirm that all contract obligations are fulfilled.

The project team will include a number of functional experts who are very experienced with delivering state repository projects successfully. In addition, the extended team will also include UCR/NIBRS subject matter experts who are active in the ongoing evolution of the NIBRS standard. One of our key strategies for 2016 is to offer our UCR/NIBRS platform as a cloud service platform hosted at the Nlets data center. As part of that initiative, Harris personnel are working directly with the FBI and BJS in support of the NCS-X program to create a cloud based UCR/NIBRS exchange that leverages economies of scale to deliver a highly capable and cost effective system for managing UCR/NIBRS reporting. All of this expertise will be available to consult with WASPC personnel to assist in making educated decisions on platform configuration and operational procedures.

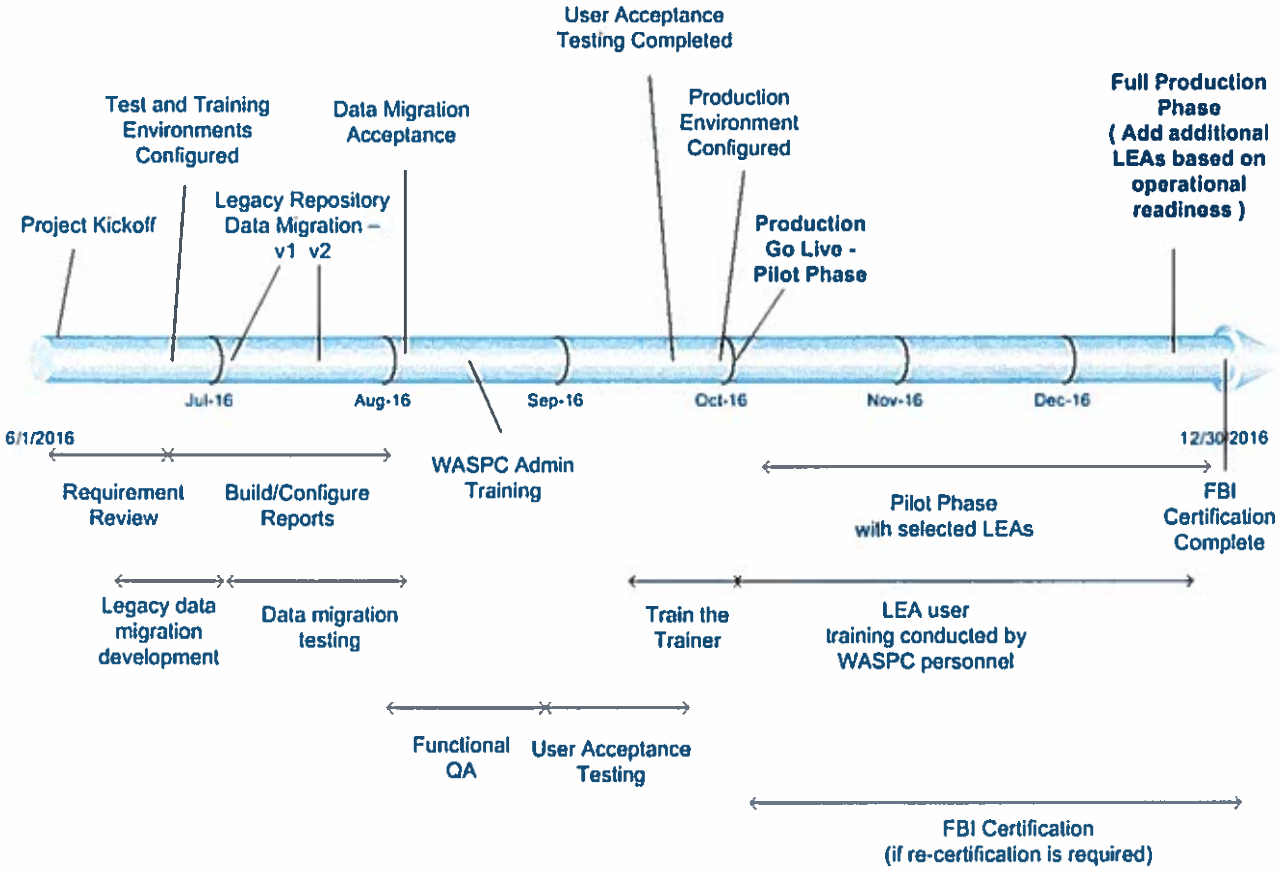
The diagram below illustrates our typical project organization.



The project is organized into functional teams that consist of Caliber and WASPC personnel working together to accomplish the assigned tasks.

3.2 Project Schedule

The approximate start date for the replacement project is June 1, 2016. The Vendor must provide an estimated schedule for complete implementation of project (required components) and re-certification with the FBI. The estimate should assume the FBI's response to data submissions is prompt.



Project Plan – Task List and Durations

	Duration	
INITIATING	2	weeks
Approve Project Agreement	1	day
Select Project Managers	1	day
Requirement Review	5	days
Create Statement of Work	2	days
Review Hardware and network requirements with agency	1	day
Agency and CPS Agree to Proceed	1	day
Hold Kick Off Meeting	1	day
EXECUTING	24	weeks
Configuration of Test Environment	5	Days
Data migration development	10	Days
Converted customer data is placed on internal staging system	1	day
Agency conducts verification of migrated data on agency staging system	15	days
CPS trainer conducts software review sessions with SSAs	3	days
Report development	20	days
CPS system testing on agency staging system	15	days
WASPC user acceptance testing	20	days
Train the trainer	2	days
Configure production environment	2	days
Production pilot phase	90	days
Local agency training	90+	days
FBI Certification (as required)	90	days
Finalize Go Live plans	3	days
Full production Go Live	1	day
CLOSING		
Project Sign-off	1	day
Develop post Go Live support plan	1	day
CLOSURE-post closure		
Transition to support		

3.3 Roles and Responsibilities

Vendors shall define the roles and responsibilities of the WASPC project team as well as those of the Vendor's project team. WASPC's project manager will work closely with the Vendor's project manager.

CPS Response:

Here is a listing of the key roles required for this project:

- Project manager – need one CPS project manager and one for WASPC
- Executive sponsors – serve as steering committee and make all contract, schedule, and change management decisions
- Data conversion team – CPS will provide data migration specialists and will execute the data conversion. WASPC requires resources to review the converted data and provide sign off on the data migration
- Application development and QA – CPS' engineering team will perform all development on functions and reports and will be responsible for QA testing.
- User Acceptance Testing – WASPC will be responsible for providing subject matter experts to develop a User Acceptance Test Plan and for performing application acceptance testing.
- Trainers – CPS will provide trainers for WASPC user training as well as technical training as required. CPS will also provide training to assist WASPC trainers develop a training program for LEA users. WASPC needs to provide the users to be trained as application users and/or LEA trainers.
- NIBRS certification – CPS and WASPC must both provide NIBRS specialists to work with the FBI to certify the repository NIBRS submissions.

3.4 Project Change Control

Vendors must describe how they handle "bug" reporting and product enhancement requests during the implementation phases of the project. This includes a Work Order Number process and whether on-line work order tracking is available.

CPS Response:

Project change management is one of the key disciplines of the CPS project management process. All system defects found during testing as well as any new requirements or enhancements are entered into our support tracking system and assigned a unique reference number. System defects are reviewed by engineering and scheduled for resolution in a specified build. Once the build is ready it is deployed to the testing environment so that the resolutions can be verified by WASPC personnel. The ticket status is updated as the issue goes through the process so that there is visibility to the status of all reported defects.

For product enhancement requests a project change control ticket is created with a unique number. The project manager will present these requests to engineering for vetting and estimation. If any additional information is required in order to prepare an estimate, the project manager will schedule meetings with the appropriate WASPC and CPS personnel. Once the requirements are fully defined, engineering will estimate the level of effort for the enhancement. The project manager will review the estimate and prepare a project change request for WASPC with the details, costs, and proposed timeline. If WASPC approves the change request, it will be added to the project scope and scheduled into the project timeline.

3.5 Testing

Vendors must describe how the products will be tested. This should include:

1. Application testing – acceptance testing of the basic functionality and operation of the application.
   a. It is desirable that WASPC project team members have access to the software for comprehensive testing of data elements and validations during RFP evaluation.
2. Acceptance testing – Upon completion of application testing, WASPC will run system for a minimum of 60-days to ensure the system meets the functional and performance requirements stated in the RFP.
3. FBI re-certification.

CPS Response:

- Data conversion is initially tested by CPS QA staff. Once the CPS QA is successfully completed, then the data conversion will be validated by WAPSC subject matter experts. Any issues that are discovered are then returned back to the data conversion specialists for resolution. This process continues in an iterative fashion until data conversion acceptance is achieved. Our objective will be to complete the data conversion prior to UAT testing so that UAT includes all the converted data being present in the test system.

- Functional testing is performed on the UCR/NIBRS repository once the WASPC-specific configuration has been completed. Since this is a COTS application which has already undergone extensive testing during initial development, the focus of the functional testing is to confirm the operation of the configured system is correct and meets the agency's business requirements. Once CPS completes the functional QA, the system is turned over to the WASPC UAT personnel to perform functional application testing.

- Input/output testing is specific functional testing that is performed to validate the operation of the external interfaces for both import of RMS data into the repository and export of NIBRS and UCR extracts from the repository. If there are multiple RMS input formats that are planned to be supported, then each type is tested. Once CPS internal QA is completed, the system is turned over to the WASPC UAT team to confirm the results.

- User Acceptance Testing – During this phase, data is loaded into the testing repository from a set of local agencies side by side with normal production operation. This parallel testing allows WASPC to verify operation with actual production data. Once the UAT is completed, WASPC can move into the production pilot phase.

- Pilot Phase – CPS recommends that a pilot production phase be planned once UAT is completed successfully. During the pilot phase, WASPC will choose a small set of LEA's to test the submission process. The pilot phase duration is typically set at 90 days to allow for 3 months of submissions to be performed. Upon completion of the pilot, the system is ready for full production operation and the onboarding process for the local agencies to come on board is initiated.

- FBI Recertification – CPS has certified the repository platform with the FBI a number of times and is very familiar with the certification process. CPS NIBRS specialists will work directly with WASPC personnel and the FBI to perform the required test submissions and achieve the necessary verification and error rates to achieve FBI NIBRS certification. Since this proposal involves an upgrade of the currently certified system, and uses the same validation engine that has already been certified, it may be possible that a full FBI re-certification may not be required. Additional discussion on this point is needed to determine the course of action. If a re-certification is determined to be necessary, CPS will fully support the process.

- New releases – CPS will provide new releases of our UCR/NIBRS platform on an ongoing basis that we will deploy on a regular maintenance schedule. These releases will be initially deployed in the testing and training environments so that the new functionality can be verified by WASPC personnel prior to scheduling the production deployment.

3.6 System Maintenance and Support

Vendors must outline a system maintenance and support plan. Support should be covered during the hours of 8am – 4pm Pacific Time, Monday through Friday.

CPS Response:

One of the strengths of the CPS proposal is the commitment we bring to customer service and support. CPS is in the process of a complete overhaul of the support processes and procedures of the acquired organizations to leverage the best practices of the proven Harris client services methodology. We are confident that with this focus on continuous improvement of the customer experience that we will provide superior customer service to repository users.

Here are some of the highlights of the CPS technical support process:

24x7x365 Coverage

CPS' annual maintenance agreement provides unlimited telephone support concerning all software questions and issues. Our commitment to providing continual technical support is one of our hallmarks and, as always, it is a toll-free call that is addressed by a trained support technician. In addition to phone support, you can reach us via email or through a secure online portal. The online customer portal is also a valuable customer research tool that can be used to search details such as the nature of an issue, the technician assigned to a ticket, corrective action taken, and length of time required to correct the issue.

Remote Assistance Saves Time and Money

If an issue arises that hinders your ability to use the proposed system, you don't want to worry about the time and cost of a technician coming to your site. CPS Technical Support utilizes advanced remote diagnostic tools to rapidly identify a problem and to correct any software-related issues.

When online intervention is used, diagnostics can be performed and file and application software may be remotely patched, replaced, or reloaded. This benefit is part of your annual maintenance agreement and is used to correct the vast majority of issues that arise.

Online Customer Service Portal

CPS provides a customer service portal for authorized users to submit trouble tickets and get updates on previously submitted issues. The portal also provides the ability to pull reports on currently open tickets.

Escalation Procedures

CPS Technical Support will classify each incoming issue according to the severity levels outlined in the IBR Service Level Agreement, as noted in the table below. Client will be notified of the existence and classification of the problem by either telephone or written notification (including e-mail) to the designated Client contact persons/numbers. Telephone notifications shall be followed as soon as reasonably possible by written notification given by CPS to Client, which shall be deemed received by Client upon completion of transmission by computer, telecopier or telefax. Problem resolution will be provided in the appropriate severity level as described in the IBR Service Level Agreement and within the time limits specified.

SEVERITY	SEVERITY DESCRIPTION	PREMIUM SUPPORT
Priority 1 Critical	▪ The problem critically impacts the Client's ability to do business (mission critical usability problems) ▪ The system is down/inaccessible ▪ Results in corruption or loss of data ▪ No known workaround or solution to the problem at the time the call is logged	**30 minute response** via Phone Submission
Priority 2 Major	▪ Prevents the use of an explicitly documented major function of the software ▪ A significant number of users are unable to use the system. ▪ EXISTING User logon issues ▪ No known workaround or solution to the problem at the time the call is logged	**2 hour response** via Phone Submission

SEVERITY	SEVERITY DESCRIPTION	
Priority 3 Medium	• It does not meet the criteria of a priority 1 or priority 2 • Product does not work as explicitly documented • Non-mission critical usability issues (e.g. printing)	8 business hour response
Priority 4 Minor	• It does not meet the criteria of previous priorities • The problem is minor and negligibly impacts the Customer's ability to do business. Routine priorities also include questions and/or general consultation. • Documentation errors • New user set-up • New instance/schema set-up • Data load (example: Citation codes) • Installation Issues/Access set-up (new user, new machine, new method)	5 business day response

3.7 Training

WASPC requires Vendor provide comprehensive training for all state user and technical personnel. All training shall include step-by-step detail that will enable personnel unfamiliar with system to use all components and functions. Training will be performed at the WASPC site.

CPS Response:

CPS trainers are professionals who are familiar with public safety operations and deliver training that supplements and enhances your standard operating procedures while providing a solid technical foundation for operators. We design our education programs to support customers during the implementation phase and beyond—collaborating with users through long-term, effective use of our systems. We understand the importance of your mission and we will make sure you are prepared.

Following are the types of training courses that we typically include as part of a UCR/NIBRS state repository project:

(1) Administrator Training

This training is targeted at WASPC system administrators and is scheduled once the system configuration has been completed and the data conversion from the legacy repository is primarily complete. The objective is to time this initial training session so that the legacy data is populated and the system is configured per the functional requirements. We configure the system to your specific requirements and train administrators to set up system procedures, user security, state-specific reports (in addition to standard Federal reports), state-specific IBR elements, and any unique workflow requirements that are required in addition to standard input forms used by other states.

(2) Technical Training

This optional training module is intended for WASPC technical personnel in the event that WASPC chooses to host the repository in a state data center. This training will provide the technical detailed information on server, database, interfaces, and software configuration in order to implement the repository system. The material will also include developing a technical maintenance plan for ongoing operation of the repository platform.

(3) Train-the-Trainer Training

Train-the-Trainer training is designed to prepare the WASPC trainers so they can provide in-house operator training to other WASPC personnel, and also so they can conduct training classes for LEA end users that are responsible for submitting their agency's incidents and resolving any validation errors. It is recommended that WASPC establish an ongoing training program to support all the individual Washington law enforcement agencies submitting NIBRS data. CPS recommends including our trainers in the first few LEA classes in order to ensure the WASPC trainers are fully prepared to deliver the training needed. In this way, the CPS trainers can continue to offer the expertise, motivation, site knowledge, agency knowledge, and resources to implement a high quality of sustained training.

(4) End User Training

At this point, CPS does not propose any end user training beyond the training programs described above. Our assumption is that WASPC personnel will be responsible for all state and local LEA end user training. If this is something that WASPC would like CPS to assist with, we can provide a proposal for performing end user training for local and state agency end users.

Training Environment

We will establish a dedicated training environment where all training will be conducted. We use a dedicated environment for training so that it is not impacted by any activities in the testing or production environment. This also allows the trainers to maintain the set of data in this environment that supports the training scenarios that have been developed.

This training environment is maintained on an ongoing basis so that it can be used for training state and local agency end users as well as for performing refresher and new hire training for WASPC personnel.

Continuing Education

CPS recognizes the Agency may have a need for continuing education, whether it is due to personnel turnover, a desire for advanced training, or staff promotions. In order to keep your staff armed with the latest information, we offer follow-up refresher training.

3.8 Documentation

Comprehensive user documentation is essential. WASPC requires that documentation is provided that covers all components and functions of the application.

CPS Response:

CPS delivers commercial, off-the-shelf (COTS) solutions; therefore, we will deliver standard user manuals and full system documentation. Documentation includes user guides, workbooks, administrator guides, and training syllabi. Most documentation, including application software documentation, is available for quick and easy access online. Many online documents are prepared specifically for system administrators and supervisors who maintain the system.

3.9 Vendor Issues and Concerns

Vendors are encouraged to comment on potential issues within the RFP. These comments may include concerns about project requirements or project requirements that were not made but should be considered.

CPS Response: No issues or concerns to be noted.

Section 4 – Vendor Section: Additional Information

4.1 Qualifications and Experience

To warrant consideration for this contract, Vendors must submit financial information, including an annual report or audited balance sheets and income statements. For purposes of this section, "audited" shall mean that a certified public accountant has reviewed the financial reports and has expressed an opinion regarding the fairness of the information reviewed.

CPS Response:
The consolidated financial statements of Constellation Software, Inc., available at http://www.csisoftware.com/category/corporate-financial, have been audited by KPMG LLP, CSI's external auditors, in accordance with Canadian generally accepted auditing standards on behalf of the shareholders. KPMG LLP has full and free access to CSI's Audit Committee.

4.2 Vendor Information

1. Full legal name.

   Harris Systems USA, Inc.

2. Year started.

   Constellation Software, Inc. was founded in 1995 and Harris Systems USA, Inc. was founded in 2011.

3. State and location of headquarters.

   Constellation Software, Inc.
   #1200 – 20 Adelaide Street East
   Toronto, ON M5C 2T6 Canada

   Harris Systems USA, Inc.
   760 North Watters Road, Suite 100
   Allen, TX 75013

   Caliber Public Safety
   2429 Military Road, Suite 300
   Niagara Falls, NY 14304

4. Tax identification number.

   Harris Systems USA, Inc. 45-4028409

5. Brief history.

   About Our Parent Company
   Constellation Software, Inc. (CSI), Caliber Public Safety's ultimate parent company, is an international provider of market-leading software and services to a select number of industries, both in the public and private sectors. Our mission is to acquire, manage and build market-leading software businesses that develop specialized, mission-critical software solutions to address the specific needs of our particular industries.

CSI was founded in 1995 to assemble a portfolio of vertical market software companies that have the potential to be leaders in their particular market. Since then, we have grown rapidly through a combination of acquisitions and organic growth, and established a strong constellation of companies with a large, diverse customer base comprised of over 30,000 customers operating in over 30 countries around the world.

CSI has six operating groups that currently service customers in over 100 different markets worldwide. We aggregate our business into two distinct segments for financial reporting purposes: (i) the public sector segment, which includes businesses focusing upon government and government-related customers, and (ii) the private sector segment, which includes businesses focusing upon commercial customers.

With headquarters in Toronto, Canada, and offices in North America, Europe, Australia, South America and Africa, CSI has over 10,000 employees generating consolidated revenues exceeding US $1.7 billion. Constellation is publicly traded on the Toronto Stock Exchange (TSX:CSU). Their Dunn & Bradstreet Number is 25-397-0487.

Caliber Public Safety is a business unit of one of Constellation Software Inc.'s operating groups. Harris Systems USA, Inc. is a subsidiary of CSI and is one of the legal entities that markets and distributes software products and services under the Caliber Public Safety platform.

6. Current number of employees.

   204 associates across 13 U.S. locations – with 75 in R&D, 65 in Client Services, 44 in Professional Services, 16 in Sales and Marketing, and 4 in Operations – provide a variety of support, engineering, administrative, and professional services to our clients served by the Caliber Public Safety business unit.

7. Type of entity.
   Corporation

8. Disclose if your company is aware of any potential claims, investigation, or is involved in any disputes or litigation where an adverse decision may result in a material change to Vendor's financial position or future viability.
   None

9. Disclose if your company has ever filed for bankruptcy protection, reorganization, or had a receiver appointed for it.
   None

10. Audited Vendor financial data for the last three years (use appendices).
    Due to the length of these documents, detailed financial statements may be obtained at:
    http://www.csisoftware.com/category/corporate-financial

11. Most recent annual report, if public (use appendices).
    Due to the length of these documents, detailed financial statements may be obtained at:
    http://www.csisoftware.com/category/corporate-financial

4.3 Current Customer Base and References

1. Total number of customers using the products being proposed for this RFP.

   CPS Response: Four (4) – Arizona, Arkansas, Oregon, and Washington

2. Vendors shall provide at least two reference agencies where the Vendor's NIBRS repositories are installed. The reference account information must be given in the format listed below:

   A. Agency name.

      Arizona Department of Public Safety

   B. Street address/city/zip code.

      2102 W Encanto Blvd., Phoenix, AZ 85009-2847

   C. Contact name.

      Melanie Veilleux and Joyce Dehnert

   D. Contact telephone number.

      Melanie Veilleus 602-223-2488 and Joyce Dehnert 602-223-2261

   E. Contact e-mail address.

      Mveilleux@azdps.gov and jdehnert@azdps.gov

   F. Summary of project

      State Repository. Prior to the implementation of the Caliber/TAC.10 system, Arizona was a UCR-only state. We achieved their requirement to become NIBRS compliant by converting data into a new system from the existing DB2 database. The solution provides the ability to submit NIBRS data to the FBI and summarize it for use by Arizona's legacy UCR system.

   G. Number of users.
      Agencies submitting NIBRS data: 9

   H. Date system implementation started.

      August 2003

   I. Date system was certified by FBI.

      August 2004

   J. Approximate cost.

      $101,000

A. Agency name.

Arkansas Crime Information Center

B. Street address/city/zip code.

322 S Main Street, Suite 615, Little Rock, AR 72201

C. Contact name.

Jay B. Winters, Sr. and Ralph N. Ward

D. Contact telephone number.

Jay B. Winters 501-682-7408 and Ralph N. Ward 501-682-8481

E. Contact e-mail address.

Jay.winters@acic.arkansas.gov and ralph.ward@acic.arkansas.gov

F. Summary of project

State Repository. Prior to implementation, Arkansas was submitting NIBRS data to the FBI via a Crisnet system. They have been submitting N-DEx data monthly since 2011, totaling 200,000 records from just 2 participating agencies. Arkansas processes files in two different formats for N-DEx, via xml 2.2 and via flat file. All 300 agencies in the state currently submit NIBRS data. The state is currently in the early stages of a system upgrade.

G. Number of users.

Agencies submitting data: 300

H. Date system implementation started.

September 2005

I. Date system was certified by FBI (N/A if not certified).

Arkansas is certified; date unknown.

J. Approximate cost.

$95,500

A. Agency name.

Oregon State Police

B. Street address/city/zip code.

255 Capitol St NE, 4th Floor, Salem, OR 97310

C. Contact name.

Tricia Whitfield and Michael Hawkins

D. Contact telephone number.

Tricia Whitfield 503-934-2305 and Michael Hawkins 503-934-2342

E. Contact e-mail address.

Patricia.whitfield@state.or.us and Michael.hawkins@state.or.us

F. Summary of project

State Repository. Oregon utilizes a complex NIBRS variant (O-NIBRS), which contains more fields than most other state NIBRS repository systems. Oregon continues to operate its OUCR system. Our solution processes records from approximately 240 submitting agencies, split between NIBRS and UCR. Further deployment of the system includes expanded submissions to N-DEx. Oregon's system processes over 200,000 O-NIBRS records and over 900,000 OUCR records annually.

G. Number of users.

Agencies submitting data: 240, of which 159 are NIBRS certified

H. Date system implementation started.

August 2007

I. Date system was certified by FBI (N/A if not certified).

Oregon is certified; date unknown.

J. Approximate cost.

$326,300

FBI Certification

CPS is not aware of any other vendor in the marketplace that has been able to achieve FBI certification faster than we have. Typically, this process takes more than a year from the beginning date of test submissions to the FBI. We have one customer who achieved certification in one year and another that achieved certification in nine months following the beginning of test submissions to the FBI. For reference, the first customer mentioned was able to supply all required data that met the FBI's scrutiny within 6 months, and the FBI took another 6 months to certify. Part of the time frame here is out of the control of either us or the certifying agency. In the meantime, the FBI accepts data submissions.

Other Non-Repository References

A. Agency name.

Nlets – The International Justice and Public Safety Network

B. Street address/city/zip code.

1918 W Whispering Wind Dr., Phoenix, AZ 85085

C. Contact name.

Bonnie Locke

D. Contact telephone number.

602-627-2715

E. Contact e-mail address.

blocke@nlets.org

F. Summary of project

Description: Hosting Environment / Strategic Partner. As proposed, Nlets would serve as the hosting environment for the Washington State Repository.

In June, 2014, CPS (under former InterAct corporate operations) announced an expansion of its strategic partnership with Nlets, the International Justice and Public Safety Network provider, to accelerate the deployment of the Public Safety Cloud. As part of this partnership expansion, we migrated the hosting of our CPS Records Management System (RMS) application to the Nlets data center. Caliber RMS is the largest RMS cloud service offering in the market and has already been proven in statewide implementations in Indiana and Maryland. Nlets also serves as the hosting environment for the State of Vermont Department of Corrections, and other hosted Computer Aided Dispatch customers.

The Harris Cloud powered by Nlets provides a reliable and trusted infrastructure to support customers with highly efficient and reliable public safety technologies which are in full compliance with FBI CJIS Security Policy. To date, the partnership has delivered groundbreaking cloud-based solutions including InterAct Mobile and the InterDEx™ national data-sharing network used by over 1,000 agencies in 39 states.

A. Agency name.

Vermont Department of Corrections

B. Street address/city/zip code.

280 State Drive, NOB 2 South, Waterbury, VT 05671-2000

C. Contact name.

Monica Weeber and Mary Jane Ainsworth

D. Contact telephone number.

Monica Weeber: 802-598-4112

Mary Jane Ainsworth: 802-828-2210

E. Contact e-mail address.

Monica.weeber@vermont.gov and Maryjane.ainsworth@vermont.gov

F. Summary of project

Description: Statewide Offender Management System (OMS) for the Vermont DOC.

The OMS is hosted at our Nlets Phoenix data center with a DR site at the Nlets data center in Louisville, KY. The OMS provides services to 9 correctional facilities, 11 Probation and Parole offices, and VT DOC administrative personnel. Total number of users is 2100. The system went live on March 17, 2014 and the uptime has been 100% since the production launch. As part of this project we created customer specific security and DR plans based on our standard policies together with the VT state policies.

Vendors are encouraged to use this section of their proposal to provide further information on the proposed product and other related ideas.

CPS Response:

1. ***Incumbent Status*** – CPS has complete subject matter expertise on the current legacy system as a result of its acquisition of TAC.10. We have successfully migrated data from this legacy system to our .NET platform for 2 other customers eliminating the risks of the data conversion. We also have in depth knowledge on WASPC operations and business processes which simplifies the project and significantly reduces the overall risk level.

2. ***Upgrade Proposal*** – CPS has positioned our RFP response as an upgrade to the current legacy platform as a result of WASPC being a current maintenance paying customer. This eliminates the software acquisition cost and allows WASPC to leverage available funding for other priorities including: system enhancements, hosting services, specific reporting requirements, professional services to assist local agencies with creating data extracts, and other agency priorities.

3. ***Nlets Hosted Option*** – CPS has extensive experience hosting public safety applications and has been a strategic partner of Nlets for over 8 years. The hosted platform allows WASPC to lower its Total Cost of Ownership (TCO) and leverage an enterprise grade infrastructure through the economies of scale of a SaaS deployment model.

4. ***NIBRS experience*** – CPS employees have over 15 years of NIBRS and repository experience. We are subject matter experts on NIBRS reporting and the NCS-X grant program. CPS is a member of the IJIS CPAC committee and is actively involved in helping to define the future evolution of the NIBRS standard. Our deep involvement in the NIBRS standard and understanding of the required processes and procedures makes us a true partner in achieving success with the state repository and gaining local agency participation.

5. ***Enhanced Incident Entry*** – CPS can provide the option to utilize our web-based NIBRS compliant RMS for local agencies in the state that need an RMS. The Caliber RMS is already pre-integrated with the state repository and supports a fully automated submission process.

Section 5 – Pricing

Caliber Public Safety will honor this pricing, even if WASPC decides to cancel the RFP and pursue this as an upgrade to the existing system.

	Software Product/Component Descriptions	Year One	Year Two	Year Three	Year Four	Year Five
1.	Annual SaaS Licensing	$44,000	$46,200	$48,510	$50,936	$53,482
2.	Software Maintenance	Included	Included	Included	Included	Included
3.		$	$	$	$	$
4.		$	$	$	$	$
5.		$	$	$	$	$
6.		$	$	$	$	$
7.		$	$	$	$	$
8.		$	$	$	$	$
9.		$	$	$	$	$
10.		$	$	$	$	$
Total Software Product/Component Cost Per Year		$44,000	$46,200	$48,510	$50,936	$53,482

OPTIONAL ITEMS

Cost Schedule Line Item Detail

	Vendor Cloud Hosting Descriptions	Year One	Year Two	Year Three	Year Four	Year Five
1.	**Nlets Cloud Hosting**	$10,000	$10,500	$11,025	$11,576	$12,155
2.	**Nlets Initial Setup**	$30,000				
3.	**Crime Mapping Interface (BAIR RAIDSOnline)**	Included	Included	Included	Included	Included
4.	**ESRI Crime Mapping/ State Portal**	$10,000	$10,500	$11,025	$11,576	$12,155
5.	**ESRI Crime Mapping/ State Portal Setup**	$25,000				

OPTIONAL ITEMS

Cost Schedule Line Item Detail

	Optional items	
1.	Enhancements – Block of 500 hours Some possible examples: • Batch upload enhancements to improve ability to monitor and track upload operations • Auditing enhancements to add key metrics to the dashboard on error rates, submission status, graphs and trends • Notification – enhance notification and workflow processes to support configurable notifications to users for various system events (e.g. submissions, EDS response files, error reports, etc.)	$90,000
2.	LEA Services – Block of 250 hours	$45,000
3.	NIBRS professional services – block of 200 hours	$36,000
4.	Enhanced incident entry	$360/user/year

Implementation/Set-Up/Training

Cost Schedule Line Item Detail

	Implementation/Set-Up/Training Descriptions	Year One
1.	Project Planning	Included
2.	Business Process and Procedures	Included
3.	Acceptance Testing	Included
4.	Training - 16 hours admin user training - 8 hours train the trainer - 4 hours technical training	$5,040
5.	Migration Services	Included
6.	Professional Services – Configuration and Implementation	Included
Total Implementation/Set-Up/Training Cost for Year One		**$5,040**

Evaluation Instructions

Phase 1 Evaluation Instructions (Four Evaluators)

1. Review each proposal based on the requirements and desirables in the WASPC Request for Proposals and score each element using the Evaluation Worksheet.

2. The total scores will be considered when the Project Team discusses the vendor products; however, a score will not be the determining factor.

3. Regardless of the total score in Phase 1, each vendor will be invited to provide a presentation, remote access to their software, or both.

4. Pricing is not the determining factor in choosing a vendor; however, the cost of the software must be within the NCS-X grant allocation. A vendor's proposal that requires any changes to the WASPC information technology infrastructure will be added as a cost to that vendor's proposal; for example: additional server hardware or software.

Phase 2 Evaluation Instructions (Two Evaluators)

1. Review vendor software based on the requirements and desirables in the WASPC Request for Proposals and score each element using the Evaluation Worksheet.

2. In addition to the requirements and desirables, the evaluators will consider ease of use, the user interface lay-out, report functions, and software flexibility. The Phase 2 evaluations will determine which vendors are the two finalists.

3. The two finalists may be asked additional clarifying questions regarding their proposals and software functionality.

Final Analysis

1. Based on the recommendations of the two Phase 2 evaluators, the Project Team will decide which vendor software best meets the needs of the new Washington State NIBRS Repository.

2. The final recommendation for vendor choice will be forwarded to the WASPC Chief of Staff for review and approval with the Executive Director.

Phase 1 Evaluation

Evaluation 1 (Phase 1)

NIBRS RFP Evaluation Total Score

Score 700

Vendor Name: **Caliber Public Safety**

	Point Value	Points Given	Comments (Use additional page if necessary)
I Preliminary Evaluation	300	200	
II Technical Solution	100	100	
III Project Management	100	100	
IV Proposal Format	100	~~90~~ 100	
V Technical Specifications - Basic Requirements	100	100	
VI Technical Specifications - Preferences	100	100	
VII Add-On Components	100	100	
VIII Management Requirements	100	100	
Sub-Total I - VIII	1,000	~~930~~	
References:			
Reference 1	100		
Reference 2	100		
Oral Presentation	200		
Price / Value	500	200	

Total Points Possible 1,900

Vendor: **Caliber Public Safety**

A. Technical Solution		
1. Fulfillment of the requirements as stated in this RFP	20	20
2. Understanding of the work to be performed	20	20
3. Technical approach and methodology to accomplish the work	20	20
4. Completeness and competence in addressing the scope of work	20	20
5. Demonstrated and reliable technology with previous use and success	20	20
	100	100

B. Project Management		
1. Completeness and responsiveness of project management plans	15	15
2. Project Team assigned	15	15
3. Experience in development and implementing similar systems	15	15
4. Familiarity with NIBRS terminology and requirements	20	20
5. Ability to meet deadlines	15	15
6. Special consideration for detailed project plan	20	20
	100	100

C. Proposal Format		
Cover letter	10	10
Section 1 Proposal executive summary	10	10
Section 2 Technical solution and description	10	10
Section 3 Project management description	10	10
Section 4 Vendor section for additional information	10	10
Section 5 Pricing section - to include product and maintenance/support pricing	10	10
Appendix A Supplemental and Collateral Material	10	10
Appendix B Vendor financial qualifications and annual reports	10	10
Appendix C Vendor purchase contract	10	10
Appendix D Vendor software license agreements	10	10
	100	~~100~~ 100

D. Technical Specifications - Basic Requirements		
1. Ability to capture and preserve NIBRS data pursuant to current FBI Tech Spec	20	20
2. System allows entry of standard values for each data element	20	20
3. System meets additional WA State IBR data collection requirements	20	20
4. System performs editing and validation of data	20	20
5. System provides capability for submission of NIBRS data	20	20
	100	100

E. Technical Specifications - Preferences		
A. Administrators and Users		
1. Levels of user privileges: administrator, power user, report generator	2	2
2. User receives immediate notification when upload successful or failed	2	2
3. User receives reason in message if a file upload error occurs	2	2
4. System allows user to cancel duplicate file upload	1	1
5. State system administrators (SSAs) have access to a contact database	1	1
6. SSAs receive notifications when file uploads stop, fail, or duplicate	2	2
7. SSAs have access to standard, ad hoc, crime mapping reports	2	2
8. SSAs are able to monitor system through utilities function	2	2
9. SSAs are able to manage local user accounts	1	1
Sub-Total	15	15
B. Data Entry and File Upload		
1. Submission options include both batch file upload and individual incident entry	2	2
2. Individual incident entry (IIE) has data validation on each field	2	2
3. IIE is user friendly	1	1

4. IIE has drop down menus	2	2
5. IIE mandatory or invalid fields are highlighted	1	1
6. IIE cannot advance without completing mandatory fields	1	1
7. IIE mandatory fields highlight per offense	1	1
8. When IIE complete, NIBRS check lists errors and returns user to screen	1	1
9. IIE entry of date or calendar option	1	1
10. IIE hot key options are available	1	1
11. IIE entry sequence: Admin, Offense, Victim, Offender, Property, Arrestee	1	1
12. IIE of domestic violence: DV is associated with the Victim	2	2
13. IIE entry of property: ability to enter immediately with the offense	1	1
14. IIE entry of time: pop-up explaining "00" rule	1	1
Sub-Total	18	18
C. Data Reports		
1. System provides report writing capability; includes standard and ad hoc reports	2	2
2. System allows data output in MS Access, Excel, Word, PDF in report & data form	2	2
3. LEAs have access to other LEA data for report extraction	1	1
4. Data report extraction includes ad hoc, crime mapping, and data quality	2	2
5. Standard reports include:		
a. Summary of offenses	1	1
b. Summary of offenses - Domestic Violence	1	1
c. Offenses by location	1	1
d. Arrests by Offense and Age Category	1	1
e. Hate Crime	1	1
f. Activity Log (by month or year)	1	1
g. Outstanding Errors and Incidents/Arrests Not Checked	1	1
h. Static report (snapshot) of database	1	1
Sub-Total	15	15
D. Data Validation and Error Notification		
1. System meets all FBI and WA State data validation edits and error checks	2	2
2. System sends electronic error reports back to submitting agency	2	2
3. System performs data validations/error checks before FBI file submission	2	2
4. Local and State SA are able to access batch error upload report	2	2
5. Incidents with errors are included in the ad hoc and summary reports	2	2
6. The FBI error messages can be easily edited to make them user friendly	1	1
7. There is no Time-Window Base Date Calculation	2	2
8. The error list does not include errors without a case number	1	1
Sub-Total	14	14
E. State System		
1. The system authenticates access with levels of users	2	2
2. The state system administrators (SSAs) designate roles for local users	2	2
3. The SSAs are able to enter and update data directly through the application	2	2
4. There are two databases: training and production	2	2
a. The training database displays data field descriptions when hovering	1	1
b. SSAs can transfer files from training to production	1	1
c. Production database has permanent archive ability	2	2
Sub-Total	12	12
F. System Features		
1. System discovers NIBRS batch submissions automatically	2	2
2. System provides batch submissions and IIE to repository via web browser	2	2
3. Data are immediately available for reports after State system acceptance	2	2
4. Domestic Violence (DV) indicator is associated with Victim	1	1
a. DV default is set for based on certain relationships, i.e. Spouse		
b. If default is triggered, a pop-up question asks, "Are you sure?"		
5. Gang Involvement indicator is set as mandatory	1	1

6. All related cases for Multiple Clearance indicator are displayed	1	1
a. User is able to delete a case number on the list		
7. Data values not relevant to WA State or utilized by FBI can be "greyed out"	1	1
8. System journal is available for SSAs to track IIE data entry and updates	1	1
9. Pop-up windows asking "Are you sure?" are available		
10. Journal is available in Utilities for SSAs to track agency information, error rates, and agency	1	1
11. Zero Report can be entered even if the file contains a correction from previous month	1	1
12. Agency can override Zero Report month if an incident is now available for the month	1	1
13. NIBRS data can be converted to Summary format for certification purposes		
Sub-Total	14	14
G. Vendor Responsibilities		
1. Vendor has FBI certified state repository in at least one other state	1	1
2. Vendor has system that is FBI submission-capable	2	2
3. Vendor has a minimum of two years' experience with NIBRS repository development	1	1
4. Vendor presents logical solutions and proposed record layouts	1	1
5. Vendor included record layouts and report samples in the technical section	1	1
6. Vendor has customer service available Monday through Friday, 8am-4pm, Pacific Time	1	1
a. Vendor has process for Work Order Number assignment		
b. SSAs are able to check status of work order via on-line tracking system		
7. Vendor will update system per FBI requirements at no additional cost	1	1
8. Vendor will update tables or allow SSAs to update tables in timely manner	1	1
9. Vendor provides user-friendly electronic manuals, error messages, pop-up windows	1	1
10. Vendor provides comprehensive user and technical personnel training	1	1
11. Vendor specified hardware components necessary for proposed repository	1	1
Sub-Total	12	12
Total for Section E. Technical Specifications - Preferences	100	100

Add-On Components		
1. Mandatory Web-Browser is available	40	40
2. Crime Mapping (not mandatory) is available	20	20
3. Mandatory Data Migration	40	40
	100	100

Management Requirements		
1. Project Plan:		
a. Comprehensive in scope and detail	10	10
b. Plan includes project tasks, approximate dates, and time in hours	10	10
2. Project Schedule: required components and recertification with FBI	10	10
3. Roles and Responsibilities Defined	10	10
4. Project Change Control:		
a. Bug reporting	10	10
b. Product enhancement	10	10
c. Work order number process	10	10
5. Testing:		
a. WASPC project team has access to software for application testing	10	10
b. Minimum 60-day acceptance testing	10	10
c. FBI recertification plan	10	10
	100	100

Evaluation 2 (Phase 1)

NIBRS RFP Evaluation Total Score

Score 580

Vendor Name: **Caliber Public Safety**

	Point Value	Points Given	Comments (Use additional page if necessary)
I Preliminary Evaluation	300	200	
II Technical Solution	100	70	
III Project Management	100	75	
IV Proposal Format	100	57	
V Technical Specifications - Basic Requirements	100	100	
VI Technical Specifications - Preferences	100	93	
VII Add-On Components	100	100	
VIII Management Requirements	100	85	
Sub-Total I - VIII	1,000	780	
References:			
Reference 1	100	0	
Reference 2	100	0	
Oral Presentation	200	200	
Price / Value	500	450	
Total Points Possible	1,900		

5% increase in maintenance each year?

1430

E-2

1

Vendor: **Caliber Public Safety**

A. Technical Solution		
1. Fulfillment of the requirements as stated in this RFP	20	10
2. Understanding of the work to be performed	20	15
3. Technical approach and methodology to accomplish the work	20	15
4. Completeness and competence in addressing the scope of work	20	20
5. Demonstrated and reliable technology with previous use and success	20	10
	100	70

B. Project Management		
1. Completeness and responsiveness of project management plans	15	15
2. Project Team assigned	15	15
3. Experience in development and implementing similar systems	15	10
4. Familiarity with NIBRS terminology and requirements	20	15
5. Ability to meet deadlines	15	0
6. Special consideration for detailed project plan	20	20
	100	75

C. Proposal Format		
Cover letter	10	10
Section 1 Proposal executive summary	10	7
Section 2 Technical solution and description	10	10
Section 3 Project management description	10	10
Section 4 Vendor section for additional information	10	10
Section 5 Pricing section - to include product and maintenance/support pricing	10	10
Appendix A Supplemental and Collateral Material	10	0
Appendix B Vendor financial qualifications and annual reports	10	0
Appendix C Vendor purchase contract	10	0
Appendix D Vendor software license agreements	10	0
	100	57

D. Technical Specifications - Basic Requirements		
1. Ability to capture and preserve NIBRS data pursuant to current FBI Tech Spec	20	20
2. System allows entry of standard values for each data element	20	20
3. System meets additional WA State IBR data collection requirements	20	20
4. System performs editing and validation of data	20	20
5. System provides capability for submission of NIBRS data	20	20
	100	100

E. Technical Specifications - Preferences		
A. Administrators and Users		
1. Levels of user privileges: administrator, power user, report generator	2	2
2. User receives immediate notification when upload successful or failed	2	2
3. User receives reason in message if a file upload error occurs	2	2
4. System allows user to cancel duplicate file upload	1	1
5. State system administrators (SSAs) have access to a contact database	1	1
6. SSAs receive notifications when file uploads stop, fail, or duplicate	2	2
7. SSAs have access to standard, ad hoc, crime mapping reports	2	2
8. SSAs are able to monitor system through utilities function	2	2
9. SSAs are able to manage local user accounts	1	1
Sub-Total	15	15
B. Data Entry and File Upload		
1. Submission options include both batch file upload and individual incident entry	2	2
2. Individual incident entry (IIE) has data validation on each field	2	2
3. IIE is user friendly	1	1

4. IIE has drop down menus	2	2
5. IIE mandatory or invalid fields are highlighted	1	1
6. IIE cannot advance without completing mandatory fields	1	1
7. IIE mandatory fields highlight per offense	1	1
8. When IIE complete, NIBRS check lists errors and returns user to screen	1	1
9. IIE entry of date or calendar option	1	1
10. IIE hot key options are available	1	1
11. IIE entry sequence: Admin, Offense, Victim, Offender, Property, Arrestee	1	0
12. IIE of domestic violence: DV is associated with the Victim	2	2
13. IIE entry of property: ability to enter immediately with the offense	1	1
14. IIE entry of time: pop-up explaining "00" rule	1	0
Sub-Total	**18**	**16**
C. Data Reports		
1. System provides report writing capability; includes standard and ad hoc reports	2	2
2. System allows data output in MS Access, Excel, Word, PDF in report & data form	2	2
3. LEAs have access to other LEA data for report extraction	1	1
4. Data report extraction includes ad hoc, crime mapping, and data quality	2	2
5. Standard reports include:		
a. Summary of offenses	1	1
b. Summary of offenses - Domestic Violence	1	1
c. Offenses by location	1	1
d. Arrests by Offense and Age Category	1	1
e. Hate Crime	1	1
f. Activity Log (by month or year)	1	1
g. Outstanding Errors and Incidents/Arrests Not Checked	1	1
h. Static report (snapshot) of database	1	1
Sub-Total	**15**	**15**
D. Data Validation and Error Notification		
1. System meets all FBI and WA State data validation edits and error checks	2	2
2. System sends electronic error reports back to submitting agency	2	2
3. System performs data validations/error checks before FBI file submission	2	2
4. Local and State SA are able to access batch error upload report	2	2
5. Incidents with errors are included in the ad hoc and summary reports	2	2
6. The FBI error messages can be easily edited to make them user friendly	1	0
7. There is no Time-Window Base Date Calculation	2	2
8. The error list does not include errors without a case number	1	1
Sub-Total	**14**	**13**
E. State System		
1. The system authenticates access with levels of users	2	2
2. The state system administrators (SSAs) designate roles for local users	2	2
3. The SSAs are able to enter and update data directly through the application	2	2
4. There are two databases: training and production	2	2
a. The training database displays data field descriptions when hovering	1	0
b. SSAs can transfer files from training to production	1	1
c. Production database has permanent archive ability	2	2
Sub-Total	**12**	**11**
F. System Features		
1. System discovers NIBRS batch submissions automatically	2	2
2. System provides batch submissions and IIE to repository via web browser	2	2
3. Data are immediately available for reports after State system acceptance	2	2
4. Domestic Violence (DV) indicator is associated with Victim	1	1
a. DV default is set for based on certain relationships, i.e. Spouse		
b. If default is triggered, a pop-up question asks, "Are you sure?"		
5. Gang Involvement indicator is set as mandatory	1	1

6. All related cases for Multiple Clearance indicator are displayed	1	1
a. User is able to delete a case number on the list		
7. Data values not relevant to WA State or utilized by FBI can be "greyed out"	1	1
8. System journal is available for SSAs to track IIE data entry and updates	1	1
9. Pop-up windows asking "Are you sure?" are available		
10. Journal is available in Utilities for SSAs to track agency information, error rates, and agency	1	1
11. Zero Report can be entered even if the file contains a correction from previous month	1	1
12. Agency can override Zero Report month if an incident is now available for the month	1	1
13. NIBRS data can be converted to Summary format for certification purposes		
Sub-Total	**14**	14
G. Vendor Responsibilities		
1. Vendor has FBI certified state repository in at least one other state	1	0
2. Vendor has system that is FBI submission-capable	2	0
3. Vendor has a minimum of two years' experience with NIBRS repository development	1	1
4. Vendor presents logical solutions and proposed record layouts	1	1
5. Vendor included record layouts and report samples in the technical section	1	1
6. Vendor has customer service available Monday through Friday, 8am-4pm, Pacific Time	1	1
a. Vendor has process for Work Order Number assignment		
b. SSAs are able to check status of work order via on-line tracking system		
7. Vendor will update system per FBI requirements at no additional cost	1	1
8. Vendor will update tables or allow SSAs to update tables in timely manner	1	1
9. Vendor provides user-friendly electronic manuals, error messages, pop-up windows	1	1
10. Vendor provides comprehensive user and technical personnel training	1	1
11. Vendor specified hardware components necessary for proposed repository	1	1
Sub-Total	**12**	9
Total for Section E. Technical Specifications - Preferences	**100**	93

Add-On Components		
1. Mandatory Web-Browser is available	**40**	40
2. Crime Mapping (not mandatory) is available	**20**	20
3. Mandatory Data Migration	**40**	40
	100	100

Management Requirements		
1. Project Plan:		
a. Comprehensive in scope and detail	**10**	10
b. Plan includes project tasks, approximate dates, and time in hours	**10**	10
2. Project Schedule: required components and recertification with FBI	**10**	10
3. Roles and Responsibilities Defined	**10**	10
4. Project Change Control:		
a. Bug reporting	**10**	10
b. Product enhancement	**10**	10
c. Work order number process	**10**	10
5. Testing:		
a. WASPC project team has access to software for application testing	**10**	0
b. Minimum 60-day acceptance testing	**10**	10
c. FBI recertification plan	**10**	5
	100	85

Evaluation 3 (Phase 1)

NIBRS RFP Evaluation Total Score

Score 667.5

Vendor Name: **Caliber Public Safety**

	Point Value	Points Given	Comments (Use additional page if necessary)
I Preliminary Evaluation	300		
II Technical Solution	100	100	
III Project Management	100	93	
IV Proposal Format	100	100	
V Technical Specifications - Basic Requirements	100	100	
VI Technical Specifications - Preferences	100	74.5	
VII Add-On Components	100	100	
VIII Management Requirements	100	100	
Sub-Total I - VIII	1,000		
References:			
Reference 1	100		
Reference 2	100		
Oral Presentation	200		
Price / Value	500		

Total Points Possible 1,900

Vendor: **Caliber Public Safety**

A. Technical Solution		
1. Fulfillment of the requirements as stated in this RFP	20	20
2. Understanding of the work to be performed	20	20
3. Technical approach and methodology to accomplish the work	20	20
4. Completeness and competence in addressing the scope of work	20	20
5. Demonstrated and reliable technology with previous use and success	20	20
	100	100

B. Project Management		
1. Completeness and responsiveness of project management plans	15	15
2. Project Team assigned	15	12
3. Experience in development and implementing similar systems	15	15
4. Familiarity with NIBRS terminology and requirements	20	17
5. Ability to meet deadlines	15	14
6. Special consideration for detailed project plan	20	20
	100	93

C. Proposal Format		
Cover letter	10	10
Section 1 Proposal executive summary	10	10
Section 2 Technical solution and description	10	10
Section 3 Project management description	10	10
Section 4 Vendor section for additional information	10	10
Section 5 Pricing section - to include product and maintenance/support pricing	10	10
Appendix A Supplemental and Collateral Material	10	10
Appendix B Vendor financial qualifications and annual reports	10	10
Appendix C Vendor purchase contract	10	10
Appendix D Vendor software license agreements	10	10
	100	100

D. Technical Specifications - Basic Requirements		
1. Ability to capture and preserve NIBRS data pursuant to current FBI Tech Spec	20	20
2. System allows entry of standard values for each data element	20	20
3. System meets additional WA State IBR data collection requirements	20	20
4. System performs editing and validation of data	20	20
5. System provides capability for submission of NIBRS data	20	20
	100	100

E. Technical Specifications - Preferences		
A. Administrators and Users		
1. Levels of user privileges: administrator, power user, report generator	2	2
2. User receives immediate notification when upload successful or failed	2	1
3. User receives reason in message if a file upload error occurs	2	1
4. System allows user to cancel duplicate file upload	1	1
5. State system administrators (SSAs) have access to a contact database	1	1
6. SSAs receive notifications when file uploads stop, fail, or duplicate	2	1
7. SSAs have access to standard, ad hoc, crime mapping reports	2	2
8. SSAs are able to monitor system through utilities function	2	2
9. SSAs are able to manage local user accounts	1	1
Sub-Total	15	12
B. Data Entry and File Upload		
1. Submission options include both batch file upload and individual incident entry	2	2
2. Individual incident entry (IIE) has data validation on each field	2	1
3. IIE is user friendly	1	1

4. IIE has drop down menus	2	2
5. IIE mandatory or invalid fields are highlighted	1	1
6. IIE cannot advance without completing mandatory fields	1	0
7. IIE mandatory fields highlight per offense	1	1
8. When IIE complete, NIBRS check lists errors and returns user to screen	1	1
9. IIE entry of date or calendar option	1	1
10. IIE hot key options are available	1	1
11. IIE entry sequence: Admin, Offense, Victim, Offender, Property, Arrestee	1	1
12. IIE of domestic violence: DV is associated with the Victim	2	2
13. IIE entry of property: ability to enter immediately with the offense	1	.5
14. IIE entry of time: pop-up explaining "00" rule	1	0
Sub-Total	**18**	13.5
C. Data Reports		
1. System provides report writing capability; includes standard and ad hoc reports	2	2
2. System allows data output in MS Access, Excel, Word, PDF in report & data form	2	2
3. LEAs have access to other LEA data for report extraction	1	1
4. Data report extraction includes ad hoc, crime mapping, and data quality	2	1
5. Standard reports include:		
a. Summary of offenses	1	.5
b. Summary of offenses - Domestic Violence	1	.5
c. Offenses by location	1	.5
d. Arrests by Offense and Age Category	1	.5
e. Hate Crime	1	.5
f. Activity Log (by month or year)	1	.5
g. Outstanding Errors and Incidents/Arrests Not Checked	1	.5
h. Static report (snapshot) of database	1	1
Sub-Total	**15**	10.5
D. Data Validation and Error Notification		
1. System meets all FBI and WA State data validation edits and error checks	2	2
2. System sends electronic error reports back to submitting agency	2	1
3. System performs data validations/error checks before FBI file submission	2	2
4. Local and State SA are able to access batch error upload report	2	2
5. Incidents with errors are included in the ad hoc and summary reports	2	2
6. The FBI error messages can be easily edited to make them user friendly	1	1
7. There is no Time-Window Base Date Calculation	2	2
8. The error list does not include errors without a case number	1	1
Sub-Total	**14**	12
E. State System		
1. The system authenticates access with levels of users	2	2
2. The state system administrators (SSAs) designate roles for local users	2	2
3. The SSAs are able to enter and update data directly through the application	2	1
4. There are two databases: training and production	2	1
a. The training database displays data field descriptions when hovering	1	.5
b. SSAs can transfer files from training to production	1	.5
c. Production database has permanent archive ability	2	1
Sub-Total	**12**	9
F. System Features		
1. System discovers NIBRS batch submissions automatically	2	1
2. System provides batch submissions and IIE to repository via web browser	2	1
3. Data are immediately available for reports after State system acceptance	2	1
4. Domestic Violence (DV) indicator is associated with Victim	1	.5
a. DV default is set for based on certain relationships, i.e. Spouse		
b. If default is triggered, a pop-up question asks, "Are you sure?"		
5. Gang Involvement indicator is set as mandatory	1	.5

6. All related cases for Multiple Clearance indicator are displayed	1	.5
a. User is able to delete a case number on the list		
7. Data values not relevant to WA State or utilized by FBI can be "greyed out"	1	.5
8. System journal is available for SSAs to track IIE data entry and updates	1	.5
9. Pop-up windows asking "Are you sure?" are available		
10. Journal is available in Utilities for SSAs to track agency information, error rates, and agency	1	.5
11. Zero Report can be entered even if the file contains a correction from previous month	1	.5
12. Agency can override Zero Report month if an incident is now available for the month	1	.5
13. NIBRS data can be converted to Summary format for certification purposes		
Sub-Total	14	7
G. Vendor Responsibilities		
1. Vendor has FBI certified state repository in at least one other state	1	1
2. Vendor has system that is FBI submission-capable	2	2
3. Vendor has a minimum of two years' experience with NIBRS repository development	1	1
4. Vendor presents logical solutions and proposed record layouts	1	.5
5. Vendor included record layouts and report samples in the technical section	1	0
6. Vendor has customer service available Monday through Friday, 8am-4pm, Pacific Time	1	1
a. Vendor has process for Work Order Number assignment		✓
b. SSAs are able to check status of work order via on-line tracking system		✓
7. Vendor will update system per FBI requirements at no additional cost	1	1
8. Vendor will update tables or allow SSAs to update tables in timely manner	1	1
9. Vendor provides user-friendly electronic manuals, error messages, pop-up windows	1	1
10. Vendor provides comprehensive user and technical personnel training	1	1
11. Vendor specified hardware components necessary for proposed repository	1	1
Sub-Total	12	10.5
Total for Section E. Technical Specifications - Preferences	100	74.5

Add-On Components		
1. Mandatory Web-Browser is available	40	40
2. Crime Mapping (not mandatory) is available — want upgrade to ESRI	20	20
3. Mandatory Data Migration	40	40
	100	100

Management Requirements		
1. Project Plan:		
a. Comprehensive in scope and detail	10	10
b. Plan includes project tasks, approximate dates, and time in hours	10	10
2. Project Schedule: required components and recertification with FBI	10	10
3. Roles and Responsibilities Defined	10	10
4. Project Change Control:		
a. Bug reporting	10	10
b. Product enhancement	10	10
c. Work order number process	10	10
5. Testing:		
a. WASPC project team has access to software for application testing	10	10
b. Minimum 60-day acceptance testing	10	10
c. FBI recertification plan	10	10
	100	100

Evaluation A (Phase I)

NIBRS RFP Evaluation Total Score

Score 631.5

Vendor Name: **Caliber Public Safety**

	Point Value	Points Given	Comments (Use additional page if necessary)
I Preliminary Evaluation	300		
II Technical Solution	100	96	
III Project Management	100	95	
IV Proposal Format	100	53	
V Technical Specifications - Basic Requirements	100	100	
VI Technical Specifications - Preferences	100	93.5	
VII Add-On Components	100	100	
VIII Management Requirements	100	100	
Sub-Total I - VIII	1,000		
References:			
Reference 1	100		
Reference 2	100		
Oral Presentation	200		
Price / Value	500		

Total Points Possible 1,900

E-A

Vendor: **Caliber Public Safety**

A. Technical Solution		
1. Fulfillment of the requirements as stated in this RFP	20	20
2. Understanding of the work to be performed	20	20
3. Technical approach and methodology to accomplish the work	20	20
4. Completeness and competence in addressing the scope of work	20	15
5. Demonstrated and reliable technology with previous use and success	20	15
	100	90

B. Project Management		
1. Completeness and responsiveness of project management plans	15	15
2. Project Team assigned	15	15
3. Experience in development and implementing similar systems	15	15
4. Familiarity with NIBRS terminology and requirements	20	20
5. Ability to meet deadlines	15	10
6. Special consideration for detailed project plan	20	20
	100	95

C. Proposal Format		
Cover letter	10	10
Section 1 Proposal executive summary	10	9
Section 2 Technical solution and description	10	10
Section 3 Project management description	10	8
Section 4 Vendor section for additional information	10	8
Section 5 Pricing section - to include product and maintenance/support pricing	10	8
Appendix A Supplemental and Collateral Material	10	0
Appendix B Vendor financial qualifications and annual reports	10	10
Appendix C Vendor purchase contract	10	0
Appendix D Vendor software license agreements	10	0
	100	53

D. Technical Specifications - Basic Requirements		
1. Ability to capture and preserve NIBRS data pursuant to current FBI Tech Spec	20	20
2. System allows entry of standard values for each data element	20	20
3. System meets additional WA State IBR data collection requirements	20	20
4. System performs editing and validation of data	20	20
5. System provides capability for submission of NIBRS data	20	20
	100	100

E. Technical Specifications - Preferences		
A. Administrators and Users		
1. Levels of user privileges: administrator, power user, report generator	2	2
2. User receives immediate notification when upload successful or failed	2	2
3. User receives reason in message if a file upload error occurs	2	2
4. System allows user to cancel duplicate file upload	1	1
5. State system administrators (SSAs) have access to a contact database	1	1
6. SSAs receive notifications when file uploads stop, fail, or duplicate	2	1
7. SSAs have access to standard, ad hoc, crime mapping reports	2	2
8. SSAs are able to monitor system through utilities function	2	2
9. SSAs are able to manage local user accounts	1	1
Sub-Total	15	14
B. Data Entry and File Upload		
1. Submission options include both batch file upload and individual incident entry	2	2
2. Individual incident entry (IIE) has data validation on each field	2	2
3. IIE is user friendly	1	1

4. IIE has drop down menus	2	2
5. IIE mandatory or invalid fields are highlighted	1	1
6. IIE cannot advance without completing mandatory fields	1	1
7. IIE mandatory fields highlight per offense	1	1
8. When IIE complete, NIBRS check lists errors and returns user to screen	1	1
9. IIE entry of date or calendar option	1	1
10. IIE hot key options are available	1	1
11. IIE entry sequence: Admin, Offense, Victim, Offender, Property, Arrestee	1	1
12. IIE of domestic violence: DV is associated with the Victim	2	2
13. IIE entry of property: ability to enter immediately with the offense	1	1
14. IIE entry of time: pop-up explaining "00" rule	1	.5
Sub-Total	**18**	17.5
C. Data Reports		
1. System provides report writing capability; includes standard and ad hoc reports	2	2
2. System allows data output in MS Access, Excel, Word, PDF in report & data form	2	2
3. LEAs have access to other LEA data for report extraction	1	1
4. Data report extraction includes ad hoc, crime mapping, and data quality	2	2
5. Standard reports include:		
a. Summary of offenses	1	1
b. Summary of offenses - Domestic Violence	1	1
c. Offenses by location	1	1
d. Arrests by Offense and Age Category	1	1
e. Hate Crime	1	1
f. Activity Log (by month or year)	1	1
g. Outstanding Errors and Incidents/Arrests Not Checked	1	1
h. Static report (snapshot) of database	1	1
Sub-Total	**15**	15
D. Data Validation and Error Notification		
1. System meets all FBI and WA State data validation edits and error checks	2	2
2. System sends electronic error reports back to submitting agency	2	2
3. System performs data validations/error checks before FBI file submission	2	2
4. Local and State SA are able to access batch error upload report	2	2
5. Incidents with errors are included in the ad hoc and summary reports	2	2
6. The FBI error messages can be easily edited to make them user friendly	1	.5
7. There is no Time-Window Base Date Calculation	2	2
8. The error list does not include errors without a case number	1	1
Sub-Total	**14**	13.5
E. State System		
1. The system authenticates access with levels of users	2	2
2. The state system administrators (SSAs) designate roles for local users	2	2
3. The SSAs are able to enter and update data directly through the application	2	2
4. There are two databases: training and production	2	2
a. The training database displays data field descriptions when hovering	1	.5
b. SSAs can transfer files from training to production	1	1
c. Production database has permanent archive ability	2	2
Sub-Total	**12**	11.5
F. System Features		
1. System discovers NIBRS batch submissions automatically	2	2
2. System provides batch submissions and IIE to repository via web browser	2	2
3. Data are immediately available for reports after State system acceptance	2	2
4. Domestic Violence (DV) indicator is associated with Victim	1	1
a. DV default is set for based on certain relationships, i.e. Spouse		
b. If default is triggered, a pop-up question asks, "Are you sure?"		
5. Gang Involvement indicator is set as mandatory	1	1

6. All related cases for Multiple Clearance indicator are displayed	1	.5
a. User is able to delete a case number on the list		
7. Data values not relevant to WA State or utilized by FBI can be "greyed out"	1	.5
8. System journal is available for SSAs to track IIE data entry and updates	1	1
9. Pop-up windows asking "Are you sure?" are available		
10. Journal is available in Utilities for SSAs to track agency information, error rates, and agency	1	1
11. Zero Report can be entered even if the file contains a correction from previous month	1	.5
12. Agency can override Zero Report month if an incident is now available for the month	1	.5
13. NIBRS data can be converted to Summary format for certification purposes		
Sub-Total	14	12
G. Vendor Responsibilities		
1. Vendor has FBI certified state repository in at least one other state	1	.5
2. Vendor has system that is FBI submission-capable	2	1
3. Vendor has a minimum of two years' experience with NIBRS repository development	1	1
4. Vendor presents logical solutions and proposed record layouts	1	1
5. Vendor included record layouts and report samples in the technical section	1	1
6. Vendor has customer service available Monday through Friday, 8am-4pm, Pacific Time	1	1
a. Vendor has process for Work Order Number assignment		
b. SSAs are able to check status of work order via on-line tracking system		
7. Vendor will update system per FBI requirements at no additional cost	1	1
8. Vendor will update tables or allow SSAs to update tables in timely manner	1	1
9. Vendor provides user-friendly electronic manuals, error messages, pop-up windows	1	1
10. Vendor provides comprehensive user and technical personnel training	1	.5
11. Vendor specified hardware components necessary for proposed repository	1	1
Sub-Total	12	10
Total for Section E. Technical Specifications - Preferences	100	93.5

Add-On Components		
1. Mandatory Web-Browser is available	40	40
2. Crime Mapping (not mandatory) is available	20	20
3. Mandatory Data Migration	40	40
	100	100

Management Requirements		
1. Project Plan:		
a. Comprehensive in scope and detail	10	10
b. Plan includes project tasks, approximate dates, and time in hours	10	10
2. Project Schedule: required components and recertification with FBI	10	10
3. Roles and Responsibilities Defined	10	10
4. Project Change Control:		
a. Bug reporting	10	10
b. Product enhancement	10	10
c. Work order number process	10	10
5. Testing:		
a. WASPC project team has access to software for application testing	10	10
b. Minimum 60-day acceptance testing	10	10
c. FBI recertification plan	10	10
	100	100

Phase 2 Evaluation

Evaluator A (Phase 2)

Vendor: Caliber

A. Technical Specifications - Basic Requirements	Yes	No	Unknown
1. System appears to capture NIBRS data pursuant to current FBI Tech Spec	X		
Comments: Although not all named by FBI standards			
2. System allows entry of standard values for each data element	X		
Comments:			
3. System meets additional WA State IBR data collection requirements (Not expected in demo)	X		
Comments:			
4. System performs editing and validation of data	X		
Comments: But does not always capture correct information			
5. System provides capability for submission of NIBRS data	X		
Comments:			

B. Technical Specifications - Preferences			
A. Administrators and Users			
1. Levels of user privileges: administrator, power user, report generator	X		
2. User receives immediate notification when upload successful or failed	X		
3. User receives reason in message if a file upload error occurs	X		
4. System allows user to cancel duplicate file upload	X		
5. State system administrators (SSAs) have access to a contact database	X		
6. SSAs receive notifications when file uploads stop, fail, or duplicate But can see in list.		X	
7. SSAs have access to standard, ad hoc, crime mapping reports	X		
8. SSAs are able to monitor system through utilities function	X		
9. SSAs are able to manage local user accounts	X		
Comments: Names and user friendliness are not always there			
B. Data Entry and File Upload			
1. Submission options include both batch file upload and individual incident entry	X		
2. Individual incident entry (IIE) has data validation on each field Appears so	X		
3. IIE is user friendly		X	
4. IIE has drop down menus	X		
5. IIE mandatory or invalid fields are highlighted Only on error side		X	
6. IIE cannot advance without completing mandatory fields		X	
7. IIE mandatory fields highlight per offense		X	
8. When IIE complete, NIBRS check lists errors and returns user to screen	X		
9. IIE entry of date or calendar option	X		
10. IIE hot key options are available - Tabbing and first letter pop.	X		
11. IIE entry sequence: Admin, Offense, Victim, Offender, Property, Arrestee	X		
12. IIE of domestic violence: DV is associated with the Victim - on offense screen		X	
13. IIE entry of property: ability to enter immediately with the offense	X		
14. IIE entry of time: pop-up explaining "00" rule		X	

CA

Comments: Number some to move through. Lots of extra 'clicks' to make things work.			
C. Data Reports			
1. System provides report writing capability; includes standard and ad hoc reports – I think	X		
2. System allows data output in MS Access, Excel, Word, PDF in report & data form	X		
3. LEAs have access to other LEA data for report extraction Setting – although		X	
4. Data report extraction includes ad hoc, crime mapping, and data quality	X		
5. Standard reports include:			
a. Summary of offenses	X		
b. Summary of offenses - Domestic Violence	X		
c. Offenses by location	X		
d. Arrests by Offense and Age Categoy	X		
e. Hate Crime	X		
f. Activity Log (by month or year) – not Report but available	X		
g. Outstanding Errors and Incidents/Arrests Not Checked – maybe in 'TOOLS'		X	
Comments:			
Reports never worked for me. – Standard – Kept Spinning. Ad Hoc worked.			
Beginning to think variables don't like me – lol			
D. Data Validation and Error Notification			
1. System meets all FBI (and WA State) data validation edits and error checks	X		
2. System sends electronic error reports back to submitting agency			X
3. System performs data validations/error checks before FBI file submission	X		
4. Local and State SA are able to access batch error upload report	X		
5. Incidents with errors are included in the ad hoc and summary reports			X
6. The FBI error messages can be easily edited to make them user friendly			X
7. There is no Time-Window Base Date Calculation			X
8. The error list does not include errors without a case number			X
Comments:			

- Lack of follow through with issues, timeliness, etc. –
- more advantage as have our data to use – as we are familiar. but when things don't work it doesn't matter.

Evaluator A (Phase 2)

Caliber

- Technical specifications are not up to NIBRS standards
- User friendliness is not there yet. Too many steps in the entry of data.
- Highlights only if error in incident
- DV indicator is on offense screen, not on the victim screen
- A lot of extra clicks to move through incident.
- Reports were not working, but eventually some did.
- Lack of follow through and timeliness in customer service

Evaluator ID (Phase 2

Vendor: TAC 10 / CAliber

A. Technical Specifications - Basic Requirements	Yes	No	Unknown
1. System appears to capture NIBRS data pursuant to current FBI Tech Spec	✓		
Comments:			
	✓		
2. System allows entry of standard values for each data element			
Comments:			
3. System meets additional WA State IBR data collection requirements (Not expected in demo)	✓		
Comments:			
4. System performs editing and validation of data	✓		
Comments:			
5. System provides capability for submission of NIBRS data	✓		
Comments:			

B. Technical Specifications - Preferences			
A. Administrators and Users			
1. Levels of user privileges: administrator, power user, report generator	✓		
2. User receives immediate notification when upload successful or failed	✓		
3. User receives reason in message if a file upload error occurs	✓		
4. System allows user to cancel duplicate file upload	✓		
5. State system administrators (SSAs) have access to a contact database			✓
6. SSAs receive notifications when file uploads stop, fail, or duplicate	✓		
7. SSAs have access to standard, ad hoc, crime mapping reports	✓		
8. SSAs are able to monitor system through utilities function	✓		
9. SSAs are able to manage local user accounts	✓		
Comments:			
B. Data Entry and File Upload			
1. Submission options include both batch file upload and individual incident entry	✓		
2. Individual incident entry (IIE) has data validation on each field			✓
3. IIE is user friendly		✓	
4. IIE has drop down menus	✓		
5. IIE mandatory or invalid fields are highlighted			
6. IIE cannot advance without completing mandatory fields – only when fixing errors		✓	
7. IIE mandatory fields highlight per offense		✓	
8. When IIE complete, NIBRS check lists errors and returns user to screen	✓		
9. IIE entry of date or calendar option	✓		
10. IIE hot key options are available			✓
11. IIE entry sequence: Admin, Offense, Victim, Offender, Property, Arrestee		✓	
12. IIE of domestic violence: DV is associated with the Victim		✓	
13. IIE entry of property: ability to enter immediately with the offense	✓		
14. IIE entry of time: pop-up explaining "00" rule		✓	

Comments: Entry is slow - not very smooth. Gives a couple of false errors. Does not show all errors @ once.			
C. Data Reports			
1. System provides report writing capability; includes standard and ad hoc reports	✓		
2. System allows data output in MS Access, Excel, Word, PDF in report & data form		✓	✓
3. LEAs have access to other LEA data for report extraction Would have to "Allow"	✓		
4. Data report extraction includes ad hoc, crime mapping, and data quality			✓
5. Standard reports include:			
a. Summary of offenses			
b. Summary of offenses - Domestic Violence			
c. Offenses by location			
d. Arrests by Offense and Age Categoy			
e. Hate Crime			
f. Activity Log (by month or year)			
g. Outstanding Errors and Incidents/Arrests Not Checked			
Comments: Ad Hoc reports - Was not able to save report. It could export it to Excel.			
Master search function seems like would be better than Ad Hoc, but it is very cluttered with unneeded items			
D. Data Validation and Error Notification			
1. System meets all FBI (and WA State) data validation edits and error checks	✓		
2. System sends electronic error reports back to submitting agency	✓		
3. System performs data validations/error checks before FBI file submission	✓		
4. Local and State SA are able to access batch error upload report	✓		
5. Incidents with errors are included in the ad hoc and summary reports			✓
6. The FBI error messages can be easily edited to make them user friendly			✓
7. There is no Time-Window Base Date Calculation		✓	
8. The error list does not include errors without a case number			✓
Comments:			
There is a "time windows" question in data entry section.			

Evaluator B (Phase 2)

Notes on Caliber Public Safety System

Domestic Violence flag still on the offense page. This will need to be moved to the victim section.

When arresting an offender from a Group A incident, the system does not pull the age of the offender into the arrest screen. All other information from the offender section does come forward to the arrest screen.

On the Information tab; there is a question that needs to be removed: Is this a Window Segment?

To add relationship data – You have to add the victims and then edit each victim to add the relationship.

Data entry is slow. There are a lot of unnecessary "clicks".

System did give a couple of "False" errors and does not show all errors at one time.

Ad Hoc reports- Was not able to save report. I was able to export to Excel. The values are show as "codes". For example; in property description it shows "77" when it should show "Other"

Master search function seems like it would be better for Ad Hoc reports, but it is very cluttered and not user friendly. The dropdown menus have a lot of items that do not pertain to NIBRS.