

# **Beyond 20/20**

20-Apr-2016

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

Re: Response to RFP CJIS-2016-01

Dear Ms. Smith,

Beyond 20/20 is pleased to have the opportunity to bid on the replacement for your State UCR Repository.

With our extensive understanding of NIBRS, Beyond 20/20 is experienced, ready, and deeply committed to helping the State realize its objectives as it moves forward into implementation and use of the new NIBRS repository system. We are mindful of your goals and have crafted our proposal to ensure a successful project implementation.

As the CEO of the company, I am authorized to obligate Beyond 20/20. For all feedback and negotiations, please communicate with Del Khalife, our Director of Business Development. His phone number is 613-563-3993 x252 and his email is [del@beyond2020.com](mailto:del@beyond2020.com).

Beyond 20/20 Inc. formally accepts the requirements of RFP2016-01 including all amendments made as of April 19th 2016. We acknowledge receipt of two sets of questions and answers for the RFP.

Yours sincerely,



Chris Bonyun, CEO  
Beyond 20/20 Inc.  
613-563-3993

## TABLE OF CONTENTS

<b>Section 1: Proposal Executive Summary .....</b>	<b>1</b>
<b>Section 2: Technical Solution and Description .....</b>	<b>3</b>
2.1 Basic Requirements.....	3
2.2 Preferences .....	6
2.3 Add-On Components.....	25
<b>Section 3: Management Requirements.....</b>	<b>29</b>
3.1 Project plan .....	29
3.2 Project Schedule.....	30
3.3 Roles AND Responsibilities.....	34
3.4 Project Change Control .....	34
3.5 Testing.....	34
3.6 Maintenance and Support.....	35
3.7 Training.....	37
3.8 Documentation .....	37
3.9 Vendor Issues and Concerns .....	37
<b>Section 4: Additional Information .....</b>	<b>39</b>
4.1Qualifications and Experience.....	39
4.2 Vendor Information.....	39
4.3 Current Customer Base and References .....	41
<b>Section 5: Pricing – Product, Maintenance and Optional Extras.....</b>	<b>43</b>
Introduction .....	43
Application Pricing and Yearly Maintenance .....	43
Project Implementation and Management Services.....	43
System Requirements .....	44
Training and Documentation .....	44
Insurance.....	44
Payment Terms and Schedule.....	45
Optional Add-ons and Customizations.....	45
Resource pricing schedule.....	46
Contracts and Licenses.....	46
<b>Appendix A: Supplemental and Collateral Material .....</b>	<b>47</b>
Crime Insight Overview .....	47

Crime Insight Repository Overview.....48

Crime Insight Reporting Overview .....53

Sample Reports .....57

Appendix B: Vendor Financial Qualifications and Annual Reports .....63

Appendix C: Vendor Purchase Contract.....65

Appendix D: Vendor software License AgreementS .....67

EULA.....67

←Missing  
from  
proposal

## SECTION 1: PROPOSAL EXECUTIVE SUMMARY

Beyond 20/20 is pleased to propose our “Crime Insight” product, as a solution for a state-level repository and analytics reporting for the Washington Association of Sheriffs and Police Chiefs. This document provides an overview of the solution that Beyond 20/20 offers.

Since 2004, Beyond 20/20 has offered online reporting services for states that collect and report National Incident-Based Reporting System (NIBRS) crime data to the FBI. In that time, Beyond 20/20 has developed a very good reputation for understanding the NIBRS data, the meaning of the information contained within it, and how best to present it to users.

In 2012, Beyond 20/20 expanded its solution to include a Repository that is used to collect the information. Many states have repository systems in place that do not completely meet their needs, and Beyond 20/20 is well positioned to help these states improve their ability to manage their incident-based reporting (NIBRS or state-specific variant) information.

The key roles of the NIBRS repository are:

- a) To allow individual jurisdictions to provide their incident-based data;
- b) To apply validation rules to the data to ensure that it meets the state and FBI requirements;
- c) To convert the data into the FBI-standard NIBRS format;
- d) To package the data and report it to the FBI;
- e) To report the results of the validation done both in the repository itself and by the FBI on the data submitted, to both the State program and the FBI; and
- f) To prepare the data for the web-based reporting.

In addition, the key roles of the NIBRS reporting solution are:

- a) To facilitate statistical reporting (tables, charts, maps) on the NIBRS data, across all the different combinations of input fields;
- b) To support the generation of the annual Crime in Washington publication;
- c) To help the state UCR program identify valid but suspicious data to be discussed with the submitting agencies;
- d) To publish statistical information to the public and other interested parties in a carefully managed way; and
- e) To support the management of the overall process with operational reports

The Beyond 20/20 Crime Insight Repository structure is flexible enough to allow states to capture state-specific information, both in the form of additional codes/values for some fields and in the form of completely new data fields/records. In addition, it has been designed in a way that changes to the NIBRS definition over time (either the FBI standard or the state-specific elements) can be implemented as easily as possible.

This proposal includes a detailed response to each of the requirements outlined in the RFP, including the necessary functionality for both the Repository and Reporting elements of the solution. Our proposal includes an implementation project plan with a timeline and dependencies, as well as necessary training recommended for the WASPC staff to learn how to use/manage this system. Also included is the time needed for the WASPC to achieve full NIBRS certification by the FBI.

## SECTION 2: TECHNICAL SOLUTION AND DESCRIPTION

***In this section, Beyond 20/20 has reproduced and directly responded to each of the requirements stated in the RFP. A more general description of the proposed solution, our Crime Insight product, is provided in Appendix A.***

### 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.)

***Response: The Crime Insight repository has been implemented in three states and currently achieves an excellent 0.3% error rate across these states. The primary source for errors is because we follow the latest FBI specification, while the data is being submitted to the old FBI system, which is based on a much older specification. The error rate will be closer to 0% when the FBI completes development on their new system (currently scheduled to be live in January 2017). Beyond 20/20 also keeps up with all updates to the FBI specification, and will make support for this available to clients who are active with their support and maintenance agreement.***

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>).

***Response: Crime Insight supports all NIBRS fields and is maintained to allow all of the latest FBI changes each year. The software was developed for version 1.0 of the specification, and we have updated it to account for the changes in version 2.1, which is currently under review. When the FBI releases version 2.2 in the summer of 2016, Crime Insight will be updated accordingly.***

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.)

***Response: Crime Insight supports all NIBRS fields and is maintained to allow all of the latest FBI changes each year. The software was developed for version 1.0 of the specification, and we have updated it to account for the changes in version 2.1, which is currently under review. Beyond 20/20 has contributed some feedback to the FBI and hopes to see updates in the next version. When the FBI releases version 2.2 in the summer of 2016, Crime Insight will be updated accordingly.***

***In addition to the ability to capture data from submitted files, Crime Insight includes a web-based data entry system for the direct entry of NIBRS incidents. All entered data is put through the same validation process as file-based submissions.***

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.

***Response: Each implementation of Crime Insight includes the ability to process state-specific fields in addition to the standard FBI NIBRS definitions. The set of valid entries in each field is driven by a table that is modified for each customer, where necessary. Beyond 20/20 also factors in the time and cost to develop state-specific fields/rules into the implementation project. For the WA project, Beyond 20/20 anticipates immediately accepting two variants of the WA-specific records. One of these will include the Domestic Violence flag in the Offense segment, as is currently the case; the other will include the DV flag in the Victim segment, where WASPC would ideally like to see it.***

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.

***Response: See our response to point 1. We achieve a very low error rate by implementing all the same rules that are defined by the FBI (even those that the FBI themselves have not yet implemented.)***

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.)

***Response: See our response to points 1 and 3.***

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.

***Response: Beyond 20/20's project plan always includes the time for the state to obtain FBI certification. During this time, the State UCR Program is typically entering data into both the legacy system (for the FBI live environment) and Crime Insight (for certification). This process typically lasts between 4 and 6 months depending on the ability of the State UCR Program to manage the dual entry.***

## 2.2 PREFERENCES

### A. Administrators and Users

#### 1. Local System Administrator and Users

- a. Levels of user privileges: administrator, power user, report generator.

**Response:** *Crime Insight has the following levels of users:*

- (i) **Repository Administrators** – *View/track the progress of all submissions to the repository, typically responsible for chasing agencies for submissions and corrections.*
- (ii) **Reporting Administrators** – *Maintain the set of reports that are shown for use by the administrators, agencies and the general public; also typically the person who identifies what data is released to agencies and the general public. This seems to be analogous to the “Report Generator” role identified by WASPC.*
- (iii) **Agency Users** – *Upload files for one or more agencies, use the incident editor (where permitted), view QC reports and statistical reports; in some states agency users can only view their own data, in others they can see everything, depending on how the state program wants it configured. Some agency users are entitled to view reports for the agency, but not upload any data. This is configurable on a per-user basis.*
- (iv) **General Public** – *View data that has been released to the public site, using reports that have been set up by the Reporting Administrator.*

*It is often the case that the Repository Administrator and Reporting Administrator are the same person, the UCR Program Manager.*

*If WASPC would like additional roles to be defined in the system, it may be possible to add them, with a potential effect on cost and time lines.*

- b. Local users should receive immediate notification when a file uploaded successfully or if there is a file upload error.

**Response:** *Users are provided immediate (within minutes) feedback on the web interface when a file is uploaded and can log in at any time to view the current status of submissions. The system does not currently email notifications to users regarding submissions to the system, but this is in our roadmap for future delivery.*

- c. A file upload error should indicate the reason for the error; i.e., naming convention, incorrect file format, incidents already on file, etc.

***Response: Crime Insight displays all error messages on screen, with specific details including the error number a description of the error and the location where it was found (i.e. what incident number, line number in file, etc). The error number itself is a hyperlink to a more detailed description about the error. WASPC will have the ability to modify the contents of this description to include state-specific text, such as common conditions for this error that have been seen in the past.***

- d. If the file is a duplicate, the system should allow the user to cancel the upload.

***Response: Crime Insight warns the user if a file with the same file name has previously been loaded. However, as it stands, Crime Insight does not have any problem loading duplicate files. Each record is processed and if it is already in the system, it is automatically overwritten. The advantage of this approach is that an agency can view errors and correct them directly in the file without changing anything else. As no harm is done by loading a duplicate file, no errors are generated in this case.***

## 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.

***Response: This functionality is partially included in the Crime Insight system. For each user of the system, we capture the user's name, email address, and jurisdiction(s) for which they may contribute and/or view data. The product also includes a population loader, and will store historical population data. This allows for calculation of crime rates.***

***Crime Insight does not currently include fields for jurisdiction employee counts or jail statistics. These would constitute a WA-specific customization, for which an additional charge will apply.***

***Also, there is currently no built-in email capabilities for communicating with agencies. This would be a useful extension and is in our roadmap, but is not implemented today.***

- 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.

***Response: At any time, the administrators of Crime Insight can log into the system and view what files have been uploaded, errors found, current outstanding errors, etc. Currently the system does not include any email notifications, but we are planning to add them in an upcoming release.***

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

***Response: The ad hoc reporting interface allows users to generate reports based on a set of "cubes", that bring related data together for easy reporting. In addition, users can save reports for their own use, and administrators can save reports for everyone to see. In Crime Insight, reports can be configured as tables or charts. Beyond 20/20 has created a basic configurable mapping application that will allow crimes to be counted by county for comparison purposes. We have also worked with a mapping (GIS) company called Cartovista to produce both thematic and point mapping solutions. Should this be a requirement for the Washington repository, we can work with you to define exactly what is needed and put together a separate proposal for this functionality.***

***Beyond 20/20 has also built a variety of reports using Microsoft's SQL Server Reporting Services product, in those cases where specific formatting is required or the needs cannot be met with our ad hoc reporting tool. If WASPC has expertise in this area, you can build your own additional reports; if not Beyond 20/20 would be happy to build specific reports for your requirements.***

- 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.

***Response: Crime Insight includes the ability to view a record of all updates to the system and other "jobs", such as preparing data for reporting. When there is a queue of work to be done, the same presentation shows what is currently queued to be done.***

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

***Response: This is core functionality within Crime Insight.***

## B. Data Entry and File Upload

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

***Response: Crime Insight includes both a batch file upload capability and the ability to enter/edit incidents through a web interface.***

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.

***Response: The Crime Insight Incident Editor allows users to enter individual incidents into the system. At data entry, each field is presented with a drop-down list of valid entries. Following the data entry, a file is generated and passed through the Crime Insight batch upload process, ensuring that all entries meet all the validation rules stipulated by the FBI. Users are immediately notified of any issues found in the second round of validation, and are presented with the chance to correct them in the same Incident Editor screens.***

- b. Missing mandatory fields or invalid data entry errors should highlight during IIE.

***Response: Please see the previous response. Beyond 20/20 will be improving the Incident Editor in a forthcoming release of Crime Insight, and the new version will include more checking of missing mandatory fields during the entry process, rather than having to wait for the full back-end validation to take place.***

- c. The mandatory fields should highlight according to the offense.

***Response: This is not currently in place, but we will add it to the list of requirements for the updated version of the Incident Editor.***

- d. The user should not be able advance to next screen without completing mandatory fields.

***Response: This is not currently in place, but we will add it to the list of requirements for the updated version of the Incident Editor.***

- e. When the IIE is complete, the NIBRS check should list errors and return the user to screen and highlight the error(s).

***Response: See response to bullet a. Highlighting fields with errors is already part of our plan for the updated Incident Editor in an upcoming release.***

- f. Any field with a date entry should allow the option to type the date or use a calendar.

***Response: This is part of the core functionality of the Incident Editor.***

- g. It is desirable that hot keys be available to facilitate data entry.

***Response: This is not currently in place, but we will add it to the list of requirements for the updated version of the Incident Editor.***

3. The sequence of IIE screens should be:

***Response: The user is required to enter the administrative data first. Following that, they can enter the data in whatever order they want, as there are a set of tabs across the top of the page. The order of the tabs is as described in this section.***

- a. Administrative; time entry must have a pop-up explaining “00” rule.

***Response: If WASPC wants additional text on the screen, this will be accommodated as part of our customization process.***

- b. Offense; with the ability to immediately enter Property associated with the offense.

***Response: Directly jumping from an offense to related property is not part of the core functionality of the Incident Editor. However, the user can choose to move between tabs as they like. In the NIBRS specification, there is no direct link between property and offense – our Incident Editor matches the NIBRS specification in this regard.***

- c. Victim; the Domestic Violence indicator should be associated with the Victim.

***Response: We see a discrepancy between this requirement (which we understand to be new) and the current Washington technical specification, which states that the DV flag is part of the Offense segment. We propose to implement a WA-specific implementation in which the DV flag is stored at the Victim level, and entered as such in the Incident Editor. We would modify your technical specification to include the DV flag as part of the Victim segment, but would ensure that our batch file processing would accept the DV flag in either the Offense or Victim segment. If it is received in the Offense segment, we will implement logic (to be agreed with WASPC) to move it from Offense to Victim in our Repository.***

- d. Offender.

- e. Property.

- f. Arrestee.

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.

***Response: Crime Insight includes an interactive crime reporting and analytics tool. This tool allows users and site administrators to create reports on demand and then save them for repeated use. For a typical client, we implement three different sites with different permissions for data access and different expectations regarding the types of reports saved on it.***

***The "Administrative" site is typically set up for the UCR Program, the Statistical Analysis Center and any other organization that should have full access to all the data. The reports on this site tend to be heavily geared towards tracking submissions, errors, quality control, etc, which are needed for the UCR Program to ensure that the data is of the highest quality. Reports for generating the annual "Crime in ..." publication are also typically on this site.***

***The "LEA" site is geared towards submitting agencies and allows them to perform statistical analysis on data before it is released more generally. There are also reports on this site for tracking errors and for quality control, in order to encourage agencies to take more responsibility for the quality of their own data. Often, data on this site is restricted so that agencies can only see their own data.***

***The third "Public" site is provided to give data access directly to the public. Only data that has been vetted can appear on this site. The reports on this site are exclusively designed to convey specific information to the public. No access to record level data is provided on this site.***

***The Crime Insight solution also comes with a set of pre-formatted reports built using Microsoft's Reporting Services. Either WASPC or Beyond 20/20 can create additional reports using this tool, querying the Repository database directly.***

***Examples of all of these types of reports are given in the appendix.***

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

***Response: Reports built in the ad hoc reporting tool can be exported in either CSV or Excel formats. This includes both aggregate reports and record-level reports. CSV files can then be imported into any tool, such as Excel or Access. Reports built in Microsoft's Reporting Services can be exported in XML, CSV, PDF, MHTML, Excel, TIFF or Word format.***

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

***Response: Beyond 20/20 normally implements three separate sites with access to the data for reporting. One of these, the LEA site, is intended for agencies to view the data. Data access is controlled separately for each site. In some states, LEAs can only see their own data because this is a state-wide requirement. In other states, LEAs can see all the data in the system. In one state, there is a hybrid approach, where there are pockets of LEAs that can see each others' data, but otherwise each agency can only see their own. For the WA implementation, we will set up the LEA site with full access to each others' data unless the hybrid solution is more appealing to WASPC.***

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.

***Response: The Crime Insight reporting and analytics tool allows users to create their own report. They can select "dimensions" (i.e. data elements) to be placed in the report, identify which "members" (i.e. data values) to be used in the report, arrange the report by placing dimensions on rows or columns, apply calculations, filter, sort, etc.***

- b. Crime Mapping.

***Response: Beyond 20/20 offers two different types of mapping in our solution. The basic mapping allows users to view general differences in crime rates between counties. In this solution, the UCR program can configure which rates are visible on the map. Beyond 20/20 also offers a much more sophisticated mapping solution based on software from CartoVista. This mapping can include both thematic mapping and point mapping, using the latitude and longitude in the administrative segment.***

***The quote that we have provided includes an optional price for the basic mapping. In order to quote on the more sophisticated mapping we would need to enter into separate discussions to determine the requirements and desired functionality.***

- c. Data Quality; these reports are for use by the SSAs and local agency contributors to audit data quality.

***Response: Beyond 20/20's Crime Insight includes three different levels of data quality reports in the system:***

- (i) In the Repository front-end, users are provided immediate feedback with all errors/warnings found when the file is uploaded and subsequent errors found and reported by the FBI.***
- (ii) Within the ad hoc reporting tool, these errors can be analyzed by error type, submitting agency, RMS vendor, offense type, etc. The set of standard reports includes pre-defined reports on this "errors cube", but the users can easily create their own.***
- (iii) Crime Insight also includes a single report that performs over 60 different validation checks on incidents that passed validation. These checks are roughly equivalent to the QC checks performed by the FBI and are designed to highlight suspicious situations, rather than reject records outright. A sample of this report is included in Appendix A.***

***All of these reports can be set up on the Admin site (for the UCR program) and/or the LEA site (for submitting agencies to check their own data).***

- 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.

***Response: All of these reports are easily created/saved in the ad hoc reporting tool, and will be included as part of the WA solution. Reporting on the activity log is done using our "Submissions" cube, which tracks the number of records submitted by each agency over time, the user submitting the update, and the lag between when the incident occurred and when it was reported. There is no report on incidents/arrests that have not been checked, because all updates to the system are immediately 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.

***Response: We have produced a number of reports for our clients that support the generation of the annual "Crime In ..." reports. As with any other report, these connect to the database and pull the latest numbers. It is possible to download these reports in a format such as PDF in order to keep them static. Some of our clients have decided to keep a static snapshot of the entire Repository and to use this in the creation of the "Crime In..." publication. This snapshot can then be kept indefinitely and used as a reference if there is any need to justify any of the numbers in the 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.

***Response: Crime Insight performs a full validation, including all FBI and state-specific data checks, as soon as the file is entered into the system. As it currently stands, the submitting user and the site administrator can view the results of the validation immediately. We have plans to add email notification of the status of the upload in a future version, but this is not in place today.***

- a. The State System must perform data validations and locate errors before the file goes to the FBI.

***Response: Only incidents that pass the Crime Insight validation are sent to the FBI. This has resulted in a very low error rate with the FBI in those states where we are implemented.***

- 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.

***Response: When an administrator logs into our system, they can see all uploads performed by all agencies and the status of each upload (number of errors found,***

*specific listing of each error). On a separate page, the administrator can track all outstanding errors.*

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).

*Response: The system as currently designed shows only valid incidents passing validation in the statistical reporting. The goal of this approach is to have the state-generated numbers match as closely as possible to the FBI numbers. We have provided an option in the pricing to implement statistical reporting on all data, including submissions that fail validation.*

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.

*Response: There are two levels of error messages in Crime Insight. There is a short message that is generated whenever an incident fails a validation rule. These messages are currently hard-coded into the application. However, when the user clicks on any error number shown in the application, a much more detailed page is presented showing the reason(s) why the error may be produced. This page is easily customized by the State UCR program to include a description of specific situations that may relate to the issue.*

4. There should not be a Time Windows error.

*Response: There are no Time Windows errors in the Crime Insight system. We are currently getting these errors from the FBI in other implementations because the FBI has not yet caught up to their current specification, but when the new system is in place, these errors will not be produced by the FBI either. When we receive these errors from the FBI, we are marking the incidents with a warning, and will resubmit them to the new FBI system, when ready.*

5. The Error Report list:
  - a. Should not include "outside of base date" comment (unable to correct, so don't display).

*Response: This error does not exist within the Crime Insight system.*

- b. Should not include errors without case number (unable to access, so don't display).

***Response: Crime Insight currently reports errors for incidents without case numbers, but we acknowledge that there is no way to clear these issues. On our roadmap, we have plans to allow the repository administrator to clear errors that cannot and/or will not be resolved in order to keep the presentation as clean as possible.***

#### 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).

***Response: Crime Insight can only be accessed by authenticated users. Different levels of access include the ability to submit files, edit incidents, view reports, access to different levels of data, etc.***

2. The system must provide the State System Administrators (SSAs) the ability to designate roles and responsibilities for other administrators and users.

***Response: The Crime Insight web interface includes a page for administrators to add/remove users, reset passwords, define the level of access for each user, and assign one or more ORIs to the user. Each user can only submit data for ORIs to which they have been assigned.***

3. The system must allow the SSAs the ability to enter and update system data directly through the application.

***Response: Crime Insight allows administrators to submit agency files and/or edit incidents directly into the system. There is a separate interface for adding annual population data into the system from an Excel file. Beyond 20/20 is also working on an administrator interface to allow the UCR program to modify code lists directly through the web interface.***

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.

***Response: This is part of a standard Crime Insight implementation.***

- 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.

***Response: All files submitted to the Crime Insight system are available for download by the site administrator. Once downloaded from the test/certification system to the administrator's workstation, this file can then be uploaded to the live system.***

- c. Production database; with permanent statistical archive ability.

***Response: This is part of a standard Crime Insight implementation.***

#### F. System Features

1. The system must automatically discover NIBRS batch submissions; the schedule is State user-defined.

***Response: Files are processed as soon as they are submitted to Crime Insight, so there is no schedule for processing them. There is a configurable schedule for other tasks, such as preparing the cubes for ad hoc reporting and converting the NIBRS data to Summary.***

2. The system must provide batch submissions or individual incident entry to state repository via a web browser.

***Response: A web browser is the only interface into Crime Insight, for both file submissions and incident entry.***

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).

***Response: There are two steps to the Crime Insight solution. The data validation and acceptance of individual incidents happens immediately on receipt of a file and when an incident is entered through the user interface. A second phase, which prepares the data for reporting and analysis occurs in a batch process, which is run nightly. Depending on the size of the Washington database, it may be possible to set this process up to run more frequently, if there is a need for it.***

***The only change to the database when the EDS file is received is that any records rejected by the FBI are marked as errors, and removed from the valid data set. As the product currently stands, these incidents are removed from the statistical reporting system.***

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".

***Response: The DV indicator is a state-specific field, and as such, will need to be customized as part of the implementation project. We can therefore implement it in a way that matches the WASPC requirements and will suggest a default based on the victim relationships. This is different from the implementation for every other field, in which no default is suggested at all, in order to encourage each field to be properly considered.***

- b. If a default is triggered, a desirable feature for users would be a pop-up window asking, "Are you sure ...?"

***Response: This can be implemented as part of the customization for the Washington system. Our current roadmap includes many similar improvements to the IIE for improved usability and user guidance.***

5. The Gang Involvement indicator is mandatory.

***Response: This will be part of the customization for WASPC.***

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.

***Response: This is not currently functionality of Crime Insight, but we will look to add it to the product in future releases.***

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.

***Response: This is part of a standard Crime Insight implementation. The product includes a list of all valid entries for each field. These lists are verified with the client as part of any implementation. The project for WASPC will include removing "Common Law Spouse" from the table of valid values for relationships, and "99" from the list of valid property types.***

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.

***Response: Incidents entered/edited via the Incident Editor are submitted to the system in the same way as the batch process. The IIE generates a file with a single incident in it. Crime Insight includes a web page that shows all files submitted to the system, both batch and incidents submitted through the Incident Editor. Administrators can use this page to view who has submitted what transactions to the system.***

9. A desirable feature for users would be a pop-up window asking, "Are you sure ...?"

***Response: This seems to be a repeat of requirement 4b. As part of the implementation project, Beyond 20/20 will work with WASPC to determine the complete list of customizations to the Incident Editor, and will implement those that are agreed.***

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.

***Response: This is part of a standard Crime Insight implementation. The administrator can view the status of all uploads directly in the Crime Insight user interface. In addition, through the ad hoc reporting environment, the administrator can do detailed analysis of historical submissions including missing submissions, error rates, outstanding errors, and reporting latency. There is no Utilities or Maintenance menu, as this functionality is incorporated directly into the reporting site.***

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.

***Response: This is part of a standard Crime Insight implementation.***

- b. Should allow an agency to override a Zero Report month if an incident is now available for that month.

***Response: A Zero Report can be submitted and deleted through the Incident Editor. So if a Zero is submitted incorrectly, it can subsequently be dropped, prior to sending any incidents for the 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.

***Response: Crime Insight includes a module for Summary data. This includes the conversion of NIBRS to Summary, as well as direct submission of Summary data from agencies and to the FBI. A separate cost for this module has been included in the pricing matrix as part of this proposal.***

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.

***Response: Crime Insight has been certified in Massachusetts and is nearing certification in both New Hampshire and South Carolina.***

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

***Response: Crime Insight generates a file for FBI submission at the click of a button. At present this is a text file that adheres to the FBI specification v2.1. Development is complete for submission of an XML file, that follows the IEPD provided by the FBI in February 2016. In addition, Beyond 20/20 is engaged with the FBI on a project to automate the communication between Crime Insight and the FBI's NIBRS system.***

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

***Response: Beyond 20/20 started working on the NIBRS repository in 2012 and has invested heavily in the product ever since.***

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

***Response: Beyond 20/20 recommends that WASPC move to an XML-based file structure for agency submissions. This file structure would be based on the FBI NIBRS IEPD, extended for state-specific elements. We would also recommend moving the DV flag from the Offense segment to the Victim segment. As part of the implementation project, we would work with WASPC to define how any other required data elements may be gathered.***

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

***Response: Beyond 20/20 does not have a standard record layout. We follow the FBI specification and customize it as needed for each client. As part of the project, we will ensure that Crime Insight has full support for the current record layout, as described in the WA NIBRS Book 2 Specifications document. This ensures that agencies and RMS vendors are not required to make any changes as part of project. We will then work with WASPC to specify changes as required. Crime Insight will accept multiple variants of files being submitted, so that agencies can migrate to the new structure as they are able. Sample reports are shown in Appendix A.***

6. The Vendor must have Customer Service availability: Monday through Friday, 8am-4pm, Pacific Time.

***Response: Our standard hours for support are 9:00AM to 7:00PM Eastern Time, Monday to Friday.***

- a. Customer Service includes a process for Work Order Number assignment.

***Response: For clients that require a work order number, Beyond 20/20 will use our web-enabled bug tracking system, Mantis. Our response times are such that most of our clients find it easier to work without such formality.***

- 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.

***Response: Beyond 20/20 will create accounts on the Mantis system so WASPC will be able to log in and view the status of outstanding items.***

7. The Vendor must be able to edit the system as the national UCR Program requires without additional cost to the State of Washington.

***Response: Beyond 20/20 charges an annual maintenance fee, which includes automatic support for all FBI-specified changes. These updates are rolled out to each client according to a schedule agreed with the client.***

- 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.

***Response: Beyond 20/20 receives email notifications from the FBI and our clients when changes are announced to NIBRS specifications. We also follow the quarterly bulletins published by the FBI. When there are new State requirements, these are typically submitted to our Sales team, who will identify the work required and create a new Statement of Work for changes to the system. These changes typically include updates to lists of valid values for each field, new/changed validation rules, additional fields in the submitted files and/or changes to the Incident Editor.***

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

***Response: Beyond 20/20 has a reputation for very timely response to all requests, both support queries and updates to the software. We are working on a user interface feature that will allow our clients to update code list tables, but we find that our clients prefer for us to do it. In order to provide this service reliably, Beyond 20/20 requests VPN access to the machines running Crime Insight on the client site.***

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

***Response: This is part of a standard Crime Insight implementation.***

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

***Response: Every implementation project of Crime Insight involves a site visit for training. This is typically a team of two people: one who trains the technical personnel on the operation of the system, and one who trains the business personnel on the functionality of the product. This site visit is done towards the end of the project, so the concepts are fresh when the product goes live. It is included in the implementation plan in section 3.2 below.***

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.

***Response: Please see the System Requirements section in Section 5***

a. Server storage capacity should be estimated for five years of use.

***Response: Beyond 20/20 will be able to give an estimate of server storage requirements once we have received and processed the historical WA NIBRS data. However, it is our expectation that the disk space identified in our hardware section will be more than sufficient for the next five years.***

b. The server operating system must be compatible with Windows Server 2008 or higher.

***Response: Crime Insight is compatible with Windows Server 2008 and above. Our currently recommendation is Windows Server 2012.***

c. The server database software must be compatible with Windows SQL Server 2010 or higher.

***Response: Crime Insight has been developed for SQL Server 2008, 2008R2 and 2012. We will be investigating SQL Server 2016 when it is fully available from Microsoft.***

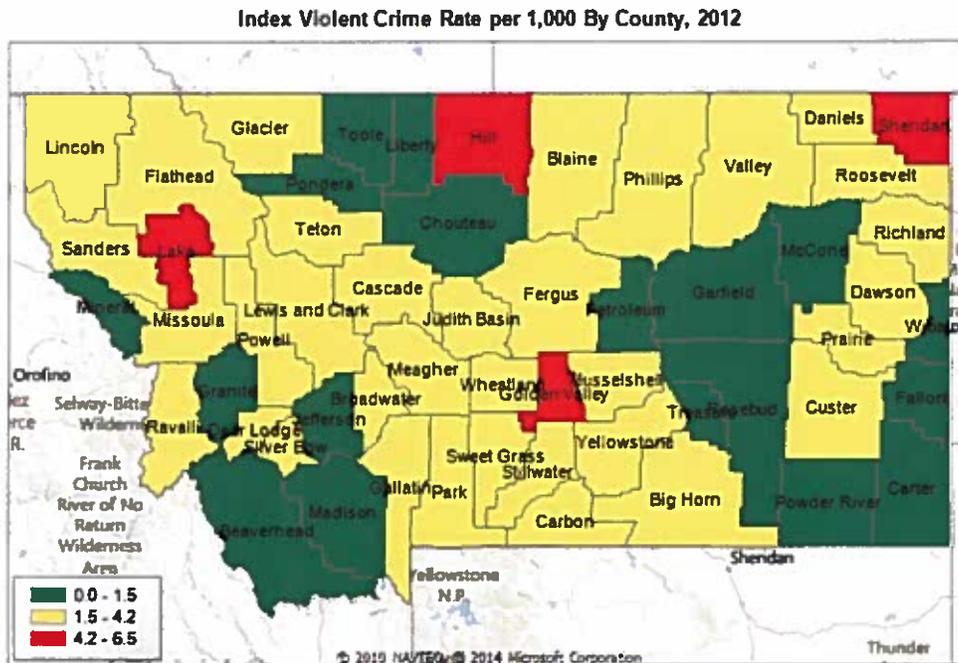
2.3 ADD-ON COMPONENTS

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.

**Response:** *The Crime Insight Repository provides a web-based interface for permitted users to easily upload and submit their data as well as generate reports. Please see Appendix A for a complete overview of the web interface. Crime Insight supports multiple web browsers including, IE9+, Chrome, Firefox, and EDGE.*

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.

**Response:** *Beyond 20/20 has developed a county-level thematic map capability that allows users to view the variation of crime across the State. Users can select the specific crime indicator and time period that they wish to see on the map. Hovering over any county shows the specific details, and clicking on a county takes the user to a tabular report showing a more detailed breakdown of crime in the county. The following shows an example of the map from Montana.*



**The map can include buttons for zooming and panning.**

*This solution includes a tool that gets run on the server to enable specific indicators for the map and to set up the tabular report shown when the user clicks on a region. The map is intended to be a fixed display that the public may have access to, rather than a sophisticated mapping tool for rich analytics.*

*Beyond 2020 also offers a more robust point mapping system that is designed by our partner company CartoVista. If a more sophisticated mapping application is of interest to WASPC this can be scoped out and a project estimate can be provided.*

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.

*Response: Conversion of the historical data to the Beyond 20/20 database can be a challenging part of the project. Beyond 20/20 is familiar with the structure of several existing Repository databases, including Motorola and Zuercher, and has experience with reviewing the databases and determining the underlying logic. We have needed this in order to do our dynamic reporting. A key element of all Beyond 20/20 solutions is the ability to pull data from existing Repositories and to convert it to our data model. To do this, we use our own ETL (data transformation) tool. Once the script is created, it can be run and re-run as necessary.*

*The biggest challenge with the conversion is the decision regarding what to do with records in the existing repository that do not conform to the current validation rules. We have two approaches that we have taken to load the data from the existing database:*

- a) Run the entire validation logic as part of the historical load, rejecting any records that fail validation; or*
- b) Run only those checks that are necessary for the data to fit in the data model with referential integrity.*

*We would typically opt for the second option, thus ensuring that any reports run off the older data match those were generated off the old repository. A significant step in any B2020 project is a detailed comparison of reports. We use our OLAP cubes and the web interface to these cubes to generate reports of the same structure as existing reports. The results are then compared and research done to explain/resolve any differences.*

*The risk of not re-validating old incidents is that if an amendment or correction is received to these incidents, the updated incident may be rejected by the FBI on resubmission. This risk is low, and in this case, the worst case scenario is that the agency will be notified that their incident is no longer valid and they will need to resolve the issue.*

***If the first option is taken with WASPC, there will be a long stage in the project where each issue found during the migration of the data will need to be resolved – are the incidents systematically corrected in some way, or are they removed from the data set, or are they loaded with the known errors.***

***Regardless of the approach taken to migrating the data, the other element that is critical in the historical load is capturing the status of the database itself. For instance, if there are records in the historical data load that have not yet been submitted to the FBI, this information must be retained so that they will be submitted as part of the first file after the historical data load is done. This is important because the data load is run repeatedly, with the last occasion being as part switching the live environment over to B2020. In this case, the historical load process includes all updates up to the most recent load into the legacy system.***

***There is no real limit on the amount of history stored within the Crime Insight database. In Massachusetts we have loaded and have dynamic reporting on over 20 years of history. The WASPC requirement is to load historical data from 2006 forward which is within our capabilities.***

***Beyond 20/20 recently successfully migrated approximately 25 years of legacy data from an older COBOL based system for the State of South Carolina. We are staffed with expert database architects and are confident that we can accomplish any required data migration task having successfully done so in the past. We strongly recommend migrating all the available legacy data to ensure a smooth transition with no unforeseen data gaps.***

## SECTION 3: MANAGEMENT REQUIREMENTS

### 3.1 PROJECT PLAN

Beyond 20/20 has put together the detailed schedule that appears in section 3.2 below. This is based on our review of the RFP and the document “2016Jan WA NIBRS Book 2 Specifications”.

The Beyond 20/20 approach to NIBRS implementations involves the following major elements:

- a) Implementation of state-specific fields, validation rules and logic for generating NIBRS from the state IBR content, including updating the incident editor to support these fields;
- b) Load of historical data from the legacy repository software, which involves a review / discussion of those records that would no longer be valid in the new repository software;
- c) Implementation of the data cubes, which are the data structure from which the ad hoc reporting is done, ensuring that state-specific elements are included and state-specific reports can be generated;
- d) Validation of ad hoc reports to ensure that they match any legacy reports, or differences can be explained and understood;
- e) Setup of two sites for the Repository, and three sites for ad hoc reporting;
- f) Implementation of custom reports, as required; and
- g) Certification by the FBI, ensuring that the state’s error rates are within expectations and there is not a significant change in the rate of crimes being reported.

There are opportunities for parallel work on these tasks, although there are some interdependencies. For instance, Beyond 20/20 will start the design of the cubes early in the project, but cannot implement them until the historical data is loaded. The FBI certification can start as soon as the repository implementation is done, and can be done in parallel with the development and testing of the reports.

The key dependencies for this project are the delivery of the legacy data (usually a backup of the full database is the easiest approach for this), a year of agency submission files, a year of FBI submission files, and specific examples of reports that need to be generated. As part of the project, we will review these elements to ensure that we have the best possible understanding of how these elements work together (reverse engineering, where necessary, the logic to produce the necessary numbers).

Early in the project, Beyond 20/20 will present the result of the analysis that we do: first with a detailed project plan that outlines what high-level changes are needed to meet the requirements, then a detailed data analysis of the data conversion that is necessary, and finally a specification for the state-specific cubes and custom reports that need to be built.

Throughout this process, the Beyond 20/20 Project Manager will stay in constant contact with WASPC project manager, reporting on the status of the project and raising issues with understanding how the state-specific elements are to be handled. Regular updates and periodic meetings will be held to ensure that the project remains on track. The more engaged our clients are in the process, the easier it will be to resolve issues as they arise.

Beyond 20/20 also requires a strong change management process to handle unexpected issues as they arise. For example, in some states we have found that the agencies are not following the specification and the repository needs special logic to handle all the exceptional agencies. The price and the project plan we have quoted assumes that the agencies are all following the specification. If we find the need for additional special case logic, we will follow the change management process, determining if additional time/funds are necessary to cover these situations.

It will be WASPC's responsibility to run the parallel run phase: passing agency data to both the legacy repository and Crime Insight. There are two goals of this phase: (a) to ensure that the validation logic in Crime Insight is at least as good as (and preferably much better than) the legacy system; and (b) to pass the resulting NIBRS files to the FBI for certification. Prior to starting this phase, Beyond 20/20 will conduct training/orientation on the software to ensure that WASPC staff are able to use the system efficiently. Throughout this process, Beyond 20/20 will help with keeping the test Crime Insight up to date. This may involve running this history load process repeatedly to ensure that the two systems are kept in synch.

### 3.2 PROJECT SCHEDULE

The following project schedule is based on a set of planned inclusions/exclusions, specifically around what additional functionality will need to be built. Any changes to these may affect the price and the timeline.

The project and base pricing in section 5 include custom development to meet WA-specific needs:

- a) Support for state-specific fields and values, including Domestic Violence, the extension to the Criminal Activity Type field, and the address/lat/long fields.
- b) Support for offenses to be accepted, but not sent to the FBI (i.e. violation of no contact or protection orders)
- c) Support for two structures of submission files: one with DV in the Offense segment and one with DV in the Victim segment
- d) Extension to the current version of the Incident Editor to provide support all of the above

The following requests are not part of the product as it currently stands, and have not been included in the project schedule or costs. They are on the Crime Insight roadmap and will be available to WASPC at no charge, provided that the maintenance is active:

- a) New version of the Incident Editor, which will include usability improvements and many of the requested functionality of the IIE. If WASPC would like to ensure that this functionality is implemented exactly to your needs, and as part of the project, an additional charge will apply, and this has been shown as an optional component in the pricing.
- b) Ability to select multiple incidents when viewing/setting the multiple clearance indicator in the Incident Editor. Note that unless WASPC changes the specification of the input file, this will not be possible for incidents submitted in the batch file processing.
- c) Email notifications to users and administrators when specific functions are performed and/or when errors are found in the system.
- d) Beyond 20/20 has a plan to add the ability for administrators to mark errors as being cleared. This would allow administrators to keep the interface as tidy as possible by eliminating errors that cannot or will not be corrected, such as those where the incident number is empty or invalid.

The following items are not included in the project plan, but are potential customizations or add-ons for WASPC. They are all shown at the bottom of the pricing in section 5. For some of them, Beyond 20/20 understands the requirement clearly and has provided a price. For others, they will need to be more clearly specified in discussions with WASPC, in order to determine the cost and timeline for delivery.

- a) Including incidents with errors in reporting
- b) Converting NIBRS to UCR Summary
- c) Crime Trend Dashboard
- d) Basic Thematic mapping
- e) Enhanced Crime Mapping
- f) Agency-level data (Contact information, FTE, Jail stats)
- g) Broadcast messages, such as system alerts
- h) Additional user roles

The detailed step-by-step project plan and milestones are shown below:

ID	Task	Owner	Dependency	Completion (From signature)
0	Contract executed	WASPC (Legal, Signing Authority)		0
1	Deliver backup of existing Repository database, agency submission files and technical documentation to B2020	WASPC (IT and UCR Program)		2 weeks
2	Project Plan – validate the differences between the existing B2020 solution and WASPC requirements and produce plan	B2020	Task 1, and access to WASPC staff for discussions. WASPC to provide any required reports to be replicated.	4 weeks
<b>MILESTONE 1: Project Plan Complete – 4 weeks</b>				
3	Detailed analysis of agency submission files and legacy repository data structure	B2020	WASPC communication, Task 2	8 weeks
4	Customize data load process/validation for VA-specific fields/codes/rules	B2020	Task 3	16 weeks
5	Beyond 20/20 testing of WASPC files	B2020	Task 4	18 weeks
6	Make repository test site available to WASPC	B2020	Task 5	19 weeks
7	Develop conversion tool to load data from old database.	B2020	Task 3, Can be done in parallel with the above. Back and forth dialog between B2020 and WASPC IT to look at each issue and plan to resolve	13 weeks
8	Put historical data onto test site	B2020	Task 6,7	19 weeks
<b>MILESTONE 2: Repository Site ready for WASPC Testing – 19 weeks</b>				

<b>ID</b>	<b>Task</b>	<b>Owner</b>	<b>Dependency</b>	<b>Completion</b>
9	Create cubes for ad-hoc reporting, include WA jurisdictions and population	B2020	Milestone 2	22 weeks
10	Run reports from updated database and compare to reports from old repository. Issues found may relate to the historical data load process or the data model in the cubes.	WASPC/ B2020	Concurrent with Task 9, B2020 to update data/cubes as necessary	22 weeks
11	Deploy Crime Insight ad-hoc reporting solution	B2020	Task 9 and 10	23 Weeks
12	Create reports as identified in Task 2	B2020	Milestone 2	undefined, Additional cost may apply
<b>MILESTONE 3: Reporting Site ready for MSP Testing – 23+ weeks</b>				
13	Run tests with existing files on repository.	WASPC (UCR Program)	Milestone 2, B2020 to provide support and make changes as necessary	31 weeks
14	Test Incident Entry UI on test B2020 site	WASPC (UCR Program)	Milestone 2, B2020 to provide support and make changes as necessary	31 weeks
15	Parallel run – files are loaded into both existing repository and B2020, compare results. Expect this process to last 6 months, although it may be much quicker.	WASPC/ B2020	Task 6	45 Weeks
16	Test FBI submissions, and obtain FBI certification	WASPC/ B2020	Task 6	45 Weeks
17	Site visit: Training and Launch	WASPC/ B2020	Milestone 3, Task 13,14	46 Weeks
<b>MILESTONE 4: Go Live – 46 weeks</b>				
18	Make site available for agency self-service ad hoc reporting	WASPC/ B2020	Milestone 4	46+ weeks

### 3.3 ROLES AND RESPONSIBILITIES

The project timeline above shows the owner of each task, as well as dependencies on other parties. Beyond 20/20 will assign a project manager to oversee the implementation project. The project manager will be the primary point of contact for WASPC. The project manager will build the detailed project plan and provide status updates to WASPC.

The key areas where input from WASPC will be required are:

- a) Delivery of sufficient information and data to allow for the analysis of the existing system;
- b) Identification of specific reports that will need to be replicated/built on the new system, including those that will support the creation of the "Crime in Washington" publication;
- c) Parallel run of Crime Insight with the legacy system, which is the majority of the acceptance testing process;
- d) Review of reports to ensure that they produce the correct numbers;
- e) Management of the relationship with the FBI during the certification process

### 3.4 PROJECT CHANGE CONTROL

During the implementation project, WASPC will report all issues to Beyond 20/20's Project Manager and/or our Support Manager, depending on the stage of the project. These will be reviewed and addressed as clarifications, bugs or change requests. Any issue, other than a quick response, will be entered into our bug tracking system called Mantis. Beyond 20/20 will also enter issues into Mantis to allow all parties to be aware of them. WASPC will have online access to Mantis to view the status of all issues.

When an issue is identified as a change request, the Beyond 20/20 Project Manager will be responsible for identifying the implications of the change to both the project timeline and costs. These implications will be discussed/agreed with WASPC and the change will either be added to the project plan or filed as a potential future change.

### 3.5 TESTING

In the RFP, WASPC has asked for details on how Beyond 20/20 addresses three types of testing: application testing, acceptance testing and FBI re-certification.

For application testing, Beyond 20/20 will grant WASPC access to a test/demo site during the evaluation period. This site is set up to take files in the standard FBI structure, so it will not demonstrate the WA-specific fields and functionality. Beyond 20/20 is also prepared to give a live demonstration on this site as part of any presentation requested by WASPC.

As part of the project, Beyond 20/20 will set up a site with the WA-specific elements included and will grant WASPC access to this site as soon as the development and our internal testing is complete.

Acceptance testing and FBI re-certification testing will be accomplished during the parallel run phase of the project, identified in the schedule above. During this time, WASPC will be exercising every part of the system by uploading files that have been received from agencies, entering incidents using the Incident Editor, and generating FBI files. The parallel run will highlight areas where the Crime Insight validation differs from the legacy system. These will be used to determine if any changes are necessary. At the same time, the FBI files will be passed over to the FBI as part of their re-certification exercise. Once the FBI has process sufficient files with a low error rate, they will process with the data analysis part of the certification, ensuring that the data appears to be correct and complete.

### 3.6 MAINTENANCE AND SUPPORT

Beyond 20/20 operates with standard support hours from Monday to Friday, 9:00am to 7:00pm EST. The support line number is 1-888-879-2020 ext. 222. It is preferred that support requests are made by email ([support@beyond2020.com](mailto:support@beyond2020.com)), due to the nature of support queries and the supporting documentation/information required to maximize first call resolution rates. This information is provided on our website [www.beyond2020.com](http://www.beyond2020.com). The technical support staff at Beyond 20/20 are very well versed in Incident Based Crime Data and are able to assist with most operational or analytical related technical support requests.

Beyond 20/20 support operates with the following incident management model:

Priority 1	Priority 2	Priority 3	Priority 4
System Failure	Critical	Error	Enhancement or Training
No system feature is currently functioning; application is completely unavailable or severely impaired.  Multiple people are/or the entire office is unable to function.	System is not functioning properly and a suitable workaround is not available. A core component of the system is no longer functional.  Multiple people are or entire office is impeded from working, but work is able to continue in a limited capacity. Or, one person is unable to function.	System is functioning but is degraded by an error or limit to future productivity. A workaround may be implemented and used until further analysis is performed.  One person is impeded from working, but work is able to continue in a limited capacity.	System is functioning according to design specifications. Incident can be regarded as an enhancement or new feature suggestion to be included in a future release. End user may have a question about the functionality of the application.

A case is created for each support request made by the WASPC UCR program with corresponding Severity level that determines response time and assigned technical support resource. These cases are captured in our bug tracking system, Mantis, to which WASPC will have access. Case updates are provided to the user as new information becomes available.

Included with Maintenance are all required product releases, updates and patches. Mandatory releases are communicated via email and followed up with a phone call for any non-respondents. This communication will include bug details, new features, update to system requirements if required and communication details for follow up and scheduling.

In order to provide the best service, including performing software upgrades when necessary, Beyond 20/20 requests VPN access to our client systems. We can often trouble-shoot all issues quickly and effectively with minimal impact to users and our clients' IT personnel.

### 3.7 TRAINING

Onsite training for the Beyond 20/20 software is typically scheduled in parallel with the implementation. A train-the-trainer approach is anticipated for standard training delivery. Typically, onsite training will occur over a 2-3 days' period and the pre-defined curriculum will cover the entire Crime Insight solution including:

1. Crime Insight repository:

- Incident file Submission
- Validation
- FBI Submission and EDS return
- Incident Editing
- User Management

2. Crime Insight reporting:

- Ad-hoc report creation
- Folders and Grouping
- Calculations
- Canned Reporting
- Anomalies verification (QC report, microdata and single incident report)

A 15-part online training videos series is also available to the WASPC on the Beyond 20/20 YouTube channel [www.youtube.com/crimeinsight](http://www.youtube.com/crimeinsight).

### 3.8 DOCUMENTATION

As part of the solution, Beyond 20/20 provides online help and user manuals for both the Repository and Reporting components of Crime Insight. We also provide technical documentation for our clients' IT staff, including system architecture and operational information.

### 3.9 VENDOR ISSUES AND CONCERNS

Beyond 20/20's main concern with this RFP is the requirement to show incidents that have failed validation as part of the statistical reporting. In the 8 states where we have implemented our ad hoc reporting, this has never been an issue. These states use our tools to find/fix errors to get all important incidents through validation.

This requirement will result in a fundamental redesign of our database, which currently stores records with errors in a different way from records without errors. Having said that, we can see the merit of this approach. For instance, it does not make sense to suppress a murder not be reported just because an incorrect code was provided for the Offender Suspected of Using field.

For that reason, we have provided a price for the change that is below the actual cost to make the change. We have kept it separate, as an optional add-on, so that WASPC can evaluate whether or not the change should be implemented.

## SECTION 4: ADDITIONAL INFORMATION

### 4.1 QUALIFICATIONS AND EXPERIENCE

Beyond 20/20 has provided the requested financial statements in Appendix B.

*Not included*

### 4.2 VENDOR INFORMATION

VENDOR NAME: Beyond 20/20 Inc.

YEAR STARTED: Established in 1987 as Ivation Data Systems Inc.

LOCATION OF HEADQUARTERS: Ottawa, Ontario, Canada at 265 Carling Ave. Suite 300 K1S 2E1

TAXPAYER ID NUMBER: 102544749

#### BRIEF HISTORY:

Beyond 20/20 Inc. was formed in 1987 as a consulting firm specializing in data. The founding partners – all highly experienced in the field of socioeconomic and statistical computing – soon realized there was a need for innovative, easy-to-use software tools and the provision of expertise in the dissemination and manipulation of multidimensional data.

Our software is a comprehensive suite of dissemination, analysis and visualization products for organizational data, for the Internet and desktop environments. Our proven solutions can integrate with data warehousing products such as Microsoft's SQL Server Analysis Services, in providing a robust scalable web based reporting solution. Our solutions have provided customers with the ability to dynamically access complex data through tabular presentations, maps and charts – allowing them to identify cycles, trends and geographic distributions.

Since Beyond 20/20 first developed a NIBRS reporting solution for the state of Vermont in 2004, we have always kept NIBRS accuracy and the associated business rules as a top priority. Our solution integrates best of breed software in order to deliver to our clients a single source for all NIBRS data collection and reporting. Our Crime Insight NIBRS reporting tool is implemented in eight states: Tennessee, South Carolina, Massachusetts, Vermont, Colorado, New Hampshire, Montana and North Dakota.

Our solution includes all data elements from the Federal NIBRS Guidelines in addition to supporting state-specific IBRS elements. We work hard to stay current with NIBRS issues. We have been active in conferences with the Association of State Uniform Crime Reporting Programs (ASUCRP), Justice Research and Statistics Association (JRSA), and maintain regular contact with our state clients regarding the anticipated changes to their NIBRS needs. We are also active members of the IJIS UCR subcommittee of the CJIS Programs Advisory Committee. As a result, we have developed a strong understanding of NIBRS and its intricacies for statistical reporting. Our venture into NIBRS repositories further reinforces our commitment to understanding the challenges faced with collecting and sharing NIBRS data.

**CURRENT NUMBER OF EMPLOYEES:** 15, all of whom are highly technical

**TYPE OF ENTITY:** Beyond 20/20 is a privately held corporation

**POTENTIAL CLAIMS:** Beyond 20/20 is under no investigations, claims or disputes and is in a healthy financial position.

**FINANCIAL HISTORY:** Beyond 20/20 has never filed for bankruptcy and is under no threat of insolvency.

**FINANCIAL DATA:** 3 years of reviewed financial reports are included in appendix B

**ANNUAL REPORT:** Beyond 20/20 does not produce an annual report, but does produce reviewed financial statements, which are included in Appendix B.

#### 4.3 CURRENT CUSTOMER BASE AND REFERENCES

Beyond 20/20 currently supports 8 states with our NIBRS reporting solution including: Vermont, New Hampshire, Massachusetts, South Carolina, Tennessee, North Dakota, Montana and Colorado. Massachusetts, South Carolina and New Hampshire also run the Crime Insight NIBRS repository. Almost all our clients have expressed interest in switching from their current end of life legacy repository over to the Beyond 20/20 repository system as well and we expect this transition to take place in the coming 2 years.

#### REFERENCES:

- 1. Agency Name:** South Carolina Law Enforcement Division (SLED)  
**Address:** P.O. Box 21398, Columbia, SC 29221  
**Contact:** Alexandra Perez-Caballero  
**Tel:** (603) 223-3869  
**Email:** [acaballero@sled.sc.gov](mailto:acaballero@sled.sc.gov)  
**Project Summary:** NIBRS reporting and repository solution implemented. Currently in final phase of FBI NIBRS certification.  
**Number of users:** 300, every agency has access  
**Implementation date:** Reporting 2007; Repository 2015  
**FBI Certification:** In progress  
**Approximate Cost:** \$300,000
- 2. Agency Name:** NH Department of Safety  
**Address:** 33 Hazen Drive, Concord, NH 03305  
**Contact:** Karen E. Lamb  
**Tel:** (603) 223-3869  
**Email:** [Karen.Lamb@dos.nh.gov](mailto:Karen.Lamb@dos.nh.gov)  
**Project Summary:** NIBRS reporting and repository solution implemented. Currently in final phase of FBI NIBRS certification.  
**Number of users:** small, Karen does most of the work herself  
**Implementation date:** Reporting 2010; Repository 2015  
**FBI Certification:** In progress, expect certification by end of April  
**Approximate Cost:** \$200,000

- 3. Agency Name:** Tennessee Bureau of Investigation  
**Address:** 901 R.S. Gass Blvd. Nashville, TN 37216  
**Contact:** Jackie Vandercook  
**Tel:** (615) 744-4014  
**Email:** [Jackie.vandercook@tn.gov](mailto:Jackie.vandercook@tn.gov)  
**Project Summary:** NIBRS reporting solution, with continuous extensions.  
**Number of users:** Unlimited. Every agency has access, as does the general public  
**Implementation date:** 2008  
**FBI Certification:** Certified  
**Cost:** \$600,000 including annual improvements
  
- 4. Agency Name:** Massachusetts Executive Office of Public Safety & Security  
**Address:** One Ashburton Place, Suite 611 Boston, MA 02108  
**Contact:** Cliff Goodband  
**Tel:** (617) 274-5570  
**Email:** [Cliff.Goodband@State.MA.US](mailto:Cliff.Goodband@State.MA.US)  
**Project Summary:** NIBRS reporting and repository solution  
**Number of users:** 300, every agency has access  
**Implementation date:** Reporting 2008, Repository 2012  
**FBI Certification:** Certified  
**Cost:** \$250,000

## SECTION 5: PRICING – PRODUCT, MAINTENANCE AND OPTIONAL EXTRAS

## INTRODUCTION

This section describes the pricing for the solution. Prices for the core solution, including payment schedule are given first, followed by the costs for optional add-ons and our resource pricing for custom development.

## APPLICATION PRICING AND YEARLY MAINTENANCE

Product	Description	Yearly Maintenance	Software
Crime Insight Repository	Software License	20%	\$ 100,000
Crime Insight Reporting	Software Licence, including data model	20%	\$ 80,000
Total Software Cost	---	\$ 36,000	\$ 180,000

## PROJECT IMPLEMENTATION AND MANAGEMENT SERVICES

Implementation Project	Resource	Daily Rate	Effort (Days)	Cost \$
Data Migration	Intermediate app-dev	\$1,000.00	16	\$ 16,000
Quality Assurance	QA Tester	\$700.00	6	\$ 4,200
Training (On-site)	Software Trainer	\$1,000.00	3	* \$ 8,000
Cube design	Intermediate app-dev	\$1,000.00	10	\$ 10,000
State Specific Customisations	Intermediate app-dev	\$1,000.00	30	\$ 30,000
Report Validation/Creation	Business Analyst	\$1,250.00	4	\$ 5,000
Install	Application Operations	\$750.00	8	\$ 6,000
Project Management	Project Manager	\$1,500.00	10	\$ 15,000
<b>Total</b>			<b>87</b>	<b>\$ 94,200</b>

\* Training is for one 3-day on-site visit to train business and technical personnel. It includes \$5,000 for travel, expenses and incidentals related to training.

## SYSTEM REQUIREMENTS

Beyond 20/20 recommends a two-server configuration as follows. These may be either physical servers or virtual servers. The environment would be duplicated, with one pair of servers for test and another for production.

### Web Server

- 40 gigs HD
- 4 gigs RAM
- 2 core CPU
- Windows 2008 - 2012 R2

### SQL Server (one for test, one for production),

- 500 gigs HD
- 16 gigs RAM
- 4 cores CPU recommended
- SQL Server 2008 - 2012 R2 (2012 R2 recommended)
- Windows 2008 - 2012 R2

## TRAINING AND DOCUMENTATION

Training costs are shown as a separate line item in the Project Implementation and Management Services section above. Product documentation is included with the product and does not incur an additional cost. In addition, Beyond 20/20 will work with WASPC to update the file structure document to move the DV flag from the Offense segment to the Victim segment.

Any other state-specific documentation may incur an additional charge.

## INSURANCE

Beyond 20/20 has a variety of different insurance policies. An overview is given in Appendix B.

## PAYMENT TERMS AND SCHEDULE

<b>Payment Schedule Based On Milestones</b>			
<b>Deliverable</b>	<b>Milestone Event</b>	<b>Schedule (See section 3.2 for details)</b>	<b>Payment Upon Approval</b>
Milestone #1	Project Plan complete	4 weeks	\$ 80,000
Milestone #2	Repository site ready for WASPC Testing	19 weeks	\$ 70,000
Milestone #3	Reporting site ready for WASPC Testing	23 weeks	\$ 60,000
Milestone #4	Go Live	46 weeks	\$ 64,200
Maintenance Year 1	Due on completion of Milestone 4		\$ 36,000
Maintenance Year 2	Due 12 months after Milestone 4		\$ 36,000
Maintenance Year 2	Due 24 months after Milestone 4		\$ 36,000
<b>Grand Total of Initial Cost Year 1 to 3</b>			<b>\$ 382,200</b>

## OPTIONAL ADD-ONS AND CUSTOMIZATIONS

<b>Item</b>	<b>Description</b>	<b>Yearly Maintenance</b>	<b>Software</b>
<b>IIE modifications ahead of planned product enhancements</b>	Software Customization	--	\$ 25,000
<b>Reports to include incidents with errors</b>	Software Customization	--	\$ 40,000
<b>UCR Summary Module</b>	Add-on component	20%	\$ 30,000
<b>Crime Trend Dashboard</b>	Add-on component	20%	\$ 25,000
<b>Basic Thematic Mapping</b>	Add-on component	20%	\$ 25,000
<b>Enhanced Crime Mapping</b>	Software Customization		TBD
<b>Agency-level data (contact information, employees, jail stats)</b>	Software Customization		TBD
<b>Broadcast alerts, messaging</b>	Software Customization		TBD
<b>Additional User Roles</b>	Software Customization		TBD

**RESOURCE PRICING SCHEDULE**

The following resource pricing schedule outlines individual resource cost that may be incurred for any out of scope project items required by the State.

Resource Or Position Title / Skills	Rate / Hour	Rate / Day
1. Senior application developer	\$160.00	\$1,200.00
2. Intermediate application developer / ETL / Data modeller	\$135.00	\$1,000.00
3. Junior application developer / ETL / Data modeller	\$100.00	\$750.00
4. Data architect	\$200.00	\$1,500.00
5. Report developer	\$90.00	\$700.00
6. QA Tester	\$90.00	\$700.00
7. Systems operations	\$65.00	\$500.00
8. Application operations	\$100.00	\$750.00
9. Technical writer	\$80.00	\$600.00
10. Business analyst	\$165.00	\$1,250.00
11. Project management	\$200.00	\$1,500.00
12. Training - application instruction	\$135.00	\$1,000.00
11. Technical Support	\$100.00	\$750.00

**CONTRACTS AND LICENSES**

This proposal is for a fixed-price contract with some fixed-price optional add-on components / customizations. Beyond 20/20 does not have a standard purchase contract and will conform to the contract normally used by WASPC. Our End User License Agreement is included in Appendix D.

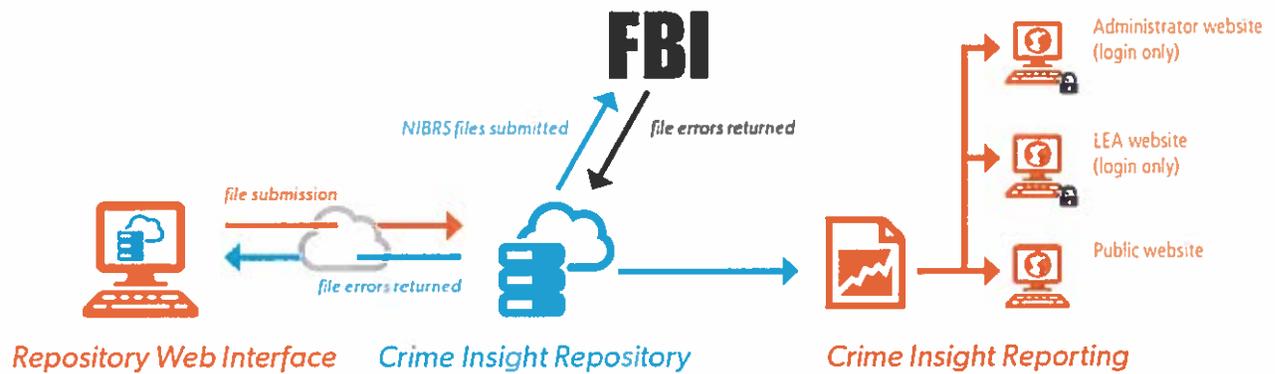
APPENDIX A: SUPPLEMENTAL AND COLLATERAL MATERIAL

CRIME INSIGHT OVERVIEW

Beyond 20/20's Crime Insight product is a complete solution for collection of incident-based data, and consists of three main components:

- a) A web interface for collecting IBR data;
- b) The data model, which includes both the operational database and data cubes, with the incident data packaged for convenient reporting; and
- c) The reporting engine, a web browser for generating / viewing reports on crime data, with different instances for each type of end user.

The following diagram shows how these elements fit together.



**Agencies can:**

- Submit data files
- Review and correct errors
- Resubmit files

**Administrators can:**

- Review and correct errors
- Manage users
- Review activity by user and date/time
- Manage data elements

**The Crime Insight Repository automatically:**

- Validates uploaded files
- Converts files to FBI NIBRS format
- Prepares files for submission to the FBI
- Consolidates errors identified by Crime Insight and FBI

**Users of all three websites can:**

- Manipulate views by dragging, dropping and nesting dimensions
- Perform cross-tabulations
- Add filters, sort, drill down, drill through, and aggregate data
- Produce highly targeted reports
- Perform in-depth analysis
- Conduct detailed research

## CRIME INSIGHT REPOSITORY OVERVIEW

The Crime Insight repository solution improves NIBRS submissions by allowing the contributing agencies to view their data and any related errors quickly after submission. The State can encourage contribution, and demonstrate the importance of reporting the data correctly.

In addition to the above, the solution consists of many other optional components:

- a) Quality Control report, showing data that appears to be suspect according to more than 80 different rules that go beyond the standard FBI checks;
- b) A Crime Trend Dashboard to provide an overview of the state of crime in the Washington, or a specific agency;
- c) A mapping tool that allows the level of crime to be reflected at the County or Region level;
- d) A point-mapping tool, showing the exact location of crimes, provided that latitude and longitude are provided for each incident; and
- e) A NIBRS-to-Summary conversion and tool, leveraged for comparative purposes between NIBRS and Summary counts.

The main goals of the Crime Insight Repository are to collect valid incident-based data from the agencies, provide instantaneous feedback on any issues that are found, and to pass accumulated data to the FBI on a regular basis. A typical submission will be processed in approximately 60 seconds allowing the uploader to quickly see errors that require attention.

The solution consists of a web-based user interface and the back-end, which contains the database and all the data processing logic. Agencies log into the web interface and upload their agency files. The system starts processing the file immediately and shows any errors as they are found. Agency users can then click on the error message to get more information about it. Agencies can correct these errors and upload the file again, or wait until the next processing cycle to submit these corrections. A full history of all uploads is shown.

All changes to the Beyond 20/20 Repository are performed through a submission queue. The contents of the queue, including the submitted file, date/time and specific request, are all stored and connected to every data point in the system. In this way, there is a full audit trail of all activity on the database. The Repository software also includes a front-end screen that allows users at any Agency to view the history of submissions for the agency. Administrators on the site can view the history of submissions from all agencies.

The license for the Beyond 20/20 Repository and Reporting environments includes the option of having up to two instances (test and live) of the software running on behalf of the client. These may be hosted on Beyond 20/20 servers, or at the State. As the software is entirely web

enabled, the location of the servers is not important to us. In addition, as we do development, we maintain a separate version of the software running on our own servers. This is where we drop releases from development for the State to review, test and accept. Once any changes are acceptable, they are released to the State's test environment, and finally to the live system.

The State may also wish to have an instance that is an exact copy of the live system. This instance would be used for agencies/vendors to use for their own testing. As their software is changed, they may need to test the delivery of files from their updated system to ensure that the State system continues to accept these files. There is no additional charge for this environment.

#### USER INTERFACE DESCRIPTION

The following screenshot shows the data upload page for the Repository.

Massachusetts Crime Perspective Version 0.7

Welcome administrator [Sign out](#)

Data upload | Data status | Reference file editor | FBI submissions | Summary data

Upload a file...

Upload a file

Browse ...

Upload Cancel

Upload history

Agency	Date	File name	Status
[Admin]	Wednesday, May 21, 2014 3:10 PM	MA0941100.X.1991.3	<a href="#">Completed with 3 warnings</a>
[Admin]	Wednesday, May 21, 2014 1:43 PM	MA0941100.X.1991.2	<a href="#">Completed with 1 error</a>
[Admin]	Tuesday, May 20, 2014 3:49 PM	MA0941100.X.1991.3	<a href="#">Completed with 3 warnings</a>
[Admin]	Tuesday, May 20, 2014 10:40 AM	MA0951100.A.2014.1	<a href="#">Completed</a>
[Admin]	Tuesday, May 20, 2014 9:47 AM	MA0093000.A.2014.04	<a href="#">Completed with 13 errors</a>
[Admin]	Monday, May 19, 2014 6:22 PM	MA0941100.X.1991.3	<a href="#">Completed with 3 warnings</a>
[Admin]	Monday, May 19, 2014 6:19 PM	MA0941100.X.1991.2	<a href="#">Completed with 1 error</a>
[Admin]	Monday, May 19, 2014 6:18 PM	MA0941100.X.1991.1	<a href="#">Completed</a>

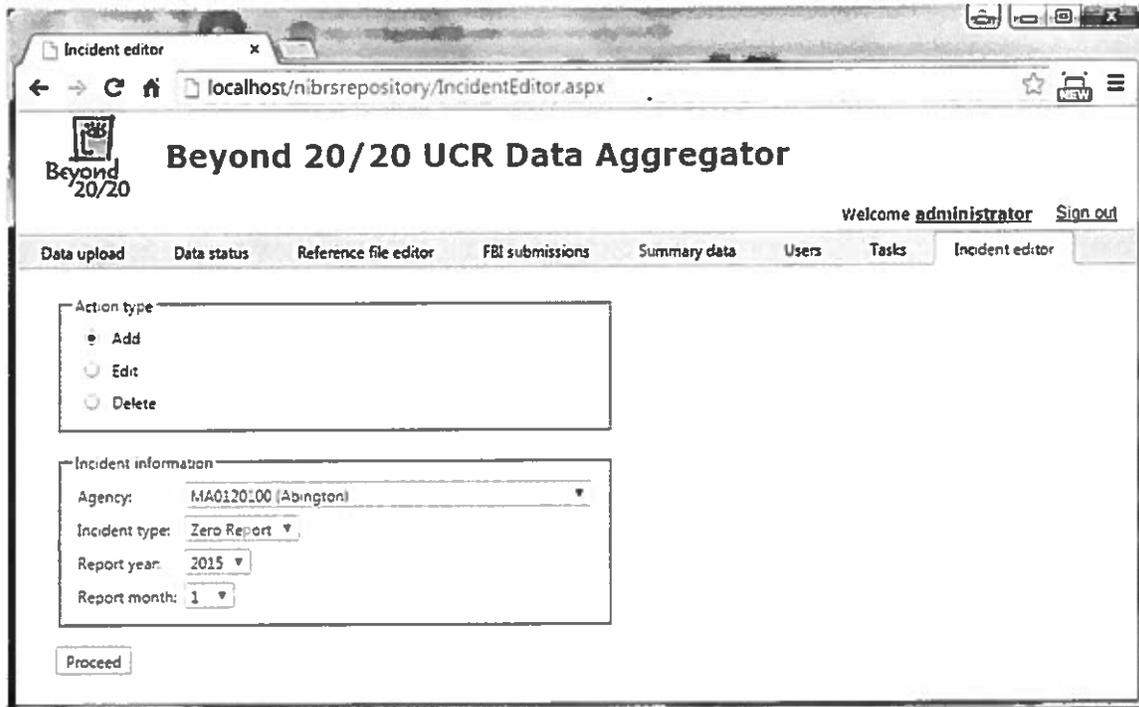
In addition to the history of uploads users can query the status of all of their data to find all outstanding errors in the system. When errors are corrected, they are automatically removed from this list.

The following image shows the data status page for a single agency.

Agency	Incident / B-Arrest / Zero Report	File name	Line number	Error code	Type	Description
Springfield	✘	✘				
Springfield	14 1381 OF	MA0071800.X.2014.2	3230	390	✘ error	Illogical property description for the offer
Springfield	14 1637 OF	MA0071800.X.2014.2	2279	390	✘ error	Illogical property description for the offer
Springfield	SPR201203569	history-copy_00031992	6315784	701	✘ error	Arrest Date must be populated with valid
Springfield	14 306 AR	MA0071800.X.2014.2	4656	404 MA	⚠ warning	LEOKA (MA) Officer Assignment Type m
Springfield	14 336 AR	MA0071800.X.2014.2	4552	404 MA	⚠ warning	LEOKA (MA) Officer Assignment Type m
Springfield	14 423 AR	MA0071800.X.2014.2	4227	404 MA	⚠ warning	LEOKA (MA) Officer Assignment Type m

The system contains all the edit checks identified by the FBI specifications, as well as any State-specific ones in the State’s own variant of NIBRS. As part of the ongoing maintenance of the system, Beyond 20/20 will provide updates to the system for any new FBI-specified rules. State-specific rules can be updated at any time, but require a services contract for the implementation.

In the latest version of the Repository a new feature was introduced to allow State or Agency Auditors to quickly and easily correct incident errors. The Incident editor allows users to Add, Edit or delete an incident.



The incident editor interface walks the user through all fields that require completion and provides alert window notifications if the user is attempting to process an invalid submission with missing data.

The screenshot displays the 'Group A Incident Editor' interface. At the top, it shows 'Current values: 120,290,35A' and 'New values (max. 10):' with a list of offense codes. A dialog box is open, showing a list of offense codes with '120 (Robbery)' selected. Below the dialog are 'OK', 'Cancel', and 'Clear' buttons. The main editor form has tabs for 'Administrative', 'Offenses (3)', 'Properties (4)', 'Victims', 'Offenders', and 'Arrestees'. The 'Offenses (3)' tab is active, showing 'Select offenses' and 'Offense 1 of 3'. Below this, there are fields for 'Offense code: 120', 'Attempted/completed: 6', 'Offender using: N', 'Location type: 20', 'Number of premises entered: 0', 'Method of entry: none', 'Criminal activity: none', 'Weapon type: 30', and 'Bias motivation: 88'. 'Submit' and 'Cancel' buttons are visible at the top right of the editor form.

This feature is also gaining traction as a lightweight RMS to be leveraged by small 1-3 person agencies that are not equipped with NIBRS supported RMS system, whereby incidents can be submitted directly into the repository.

System administrators at the State can generate FBI submission files at any time. These files will contain all records that have been submitted to the State since the previous FBI submission, provided that they pass the edit checks. As the FBI does not yet accept automated file submission, the FBI files must be downloaded to the administrator's workstation and emailed to the FBI. After the FBI has processed the file, a response file (EDS file) is generated and emailed back to the administrator. The administrator can upload the file, and any errors reported by the FBI are automatically fed back into the system where agency users can view them.

#### ADMINISTRATIVE FUNCTIONS

Site administrators can control the set of users who have access to the site and the jurisdiction(s) for which they can provide data. Administrators are allowed to submit data files for any agency. The following image displays the User Management tab, where user creation

and permissions are assigned. Users can be assigned to a single or multiple ORI as required. Administrators can also quickly de-activate or modify user permissions.

REPOSITORY												
Data upload    Data status    Reference file editor    FBI submissions    Summary data <b>Users</b> Tasks												
+ Add new user    Settings												
User Name	First Name	Last Name	Organization	Email	ORI	ORI details Update	Custom1	Custom2	Custom3	Administrator	Enabled	
Abington	A	Sington	MA0120100		MA0120100	✓					✓	✗
Acton	A	cton	MA0090100		MA0090100	✓					✓	✗
Acushnet			MA0030100		MA0030100	✓					✓	✗
Adams			MA0020100		MA0020100	✓					✓	✗
administrator	Daniel	Eibel	Fusion Center	support@beyond2020.com						✓	✓	✗
Agawam			MA0070100		MA0070100	✓					✓	✗
Aiford			MA0020200		MA0020200	✓					✓	✗
Amesbury			MA0050100		MA0050100	✓					✓	✗
Amherst			MA0080100		MA0080100	✓					✓	✗
AmherstCollege			MA008019E		MA008019E	✓					✓	✗

Another function available to the system administrator is the ability to control the set of valid values accepted in each field in the record. This is controlled using reference tables that list the codes and the values for each field. For example, the set of valid location types is stored in one table, and the set of property types in another. The only limitation is that these tables only control the valid values. Any other special validation logic (such as which offense codes are applicable to each property type) must be programmed by Beyond 20/20 engineers.

Crime Insight also includes the ability to track all data that is submitted to the Repository. All records carry sufficient information to track them back to the file in which they were delivered. The system automatically tracks which records have been exported to the FBI and uses this information in order to ensure that each FBI file only contains records that are new or updated since the previous FBI file was generated. Each FBI file is retained and can be downloaded again if there is any need to track what records were submitted in any submission to the FBI.

As all this information is available in the database, Beyond 20/20 can generate any additional reports that are required by the State. If there is a need to include this information in the ad hoc reporting tool (see next question), we can configure the system to do this as well.

DATA MODEL

The Beyond 20/20 Repository product is driven by a set of tables that define the valid codes and labels for each field in the NIBRS data structure. They also define hierarchy relationships, such as the county in which each jurisdiction resides, or groupings of offense codes in Crimes Against Persons, Property or Society. Taken in their entirety, these tables comprise the data dictionary for the product. If necessary, Beyond 20/20 could create a document that shows the content of all these tables as part of the implementation project. However, this will not be a

replacement for the technical specification to be provided to each agency. Traditionally, this document is produced by the State, and Beyond 20/20 adheres to it. However, if the State of Washington would like Beyond 20/20 to build and maintain this document as well, we can certainly do so.

#### CRIME INSIGHT REPORTING OVERVIEW

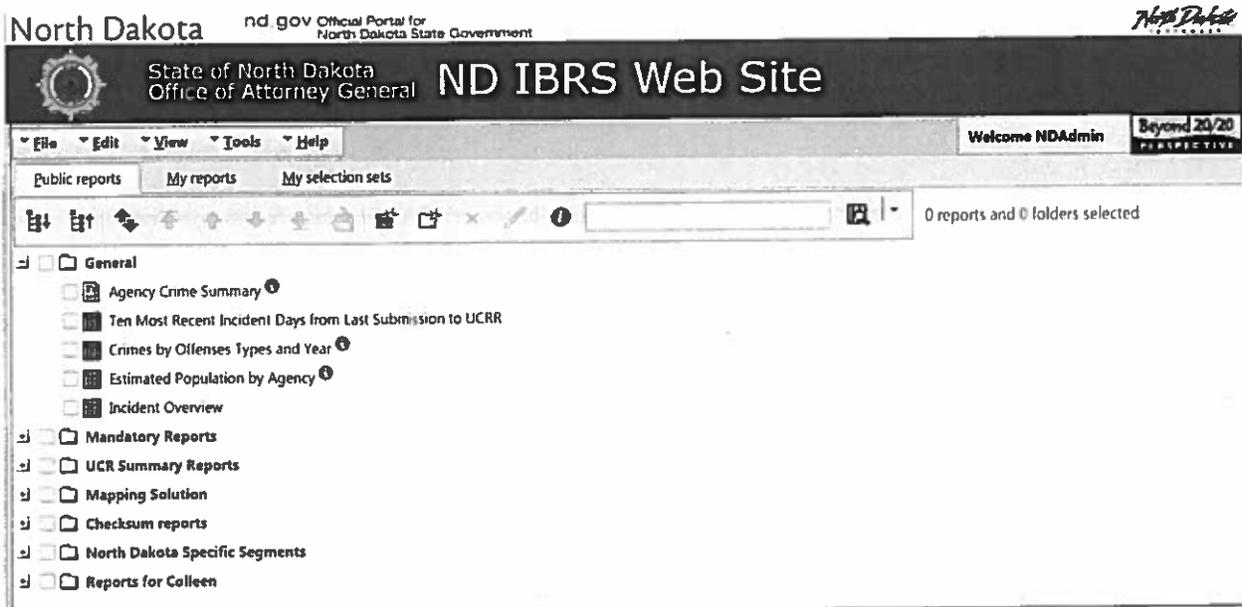
Beyond 20/20 has been providing support for reporting on NIBRS data since 2004. Over this time, our knowledge of typical State reporting requirements has grown. Our reports have been designed to support the following functions:

- a) **Quality Control (QC)** – Many States require the ability to report on data submitted by the agencies that appears to be suspect, above the hard edit checks performed by any Repository. The Beyond 20/20 NIBRS Reporting system has been used to identify many different situations that require further investigation by the reporting agency. Examples include offenders over 90 years of age, statutory rape with a family relationship, exceptional clearances with unknown offender, etc. Beyond 20/20 has extended the reporting system to include a single report that performs over 80 different QC checks across all incidents for an agency and reports on any suspect data found. This can be run in an automated way, generating a single report for each agency in the State.
- b) **Audit** – The Beyond 20/20 NIBRS Reporting System has been used to prepare State auditors as they prepare to visit an agency, highlighting areas in which the audit team may want to delve deeper. From the statistical reports, users can view the individual submissions, including the incident ID, which allows auditors to go back to the original police report at the agency. We have also developed a dashboard that can be used by this team.
- c) **Self-service reporting for agencies** – Some agencies submitting NIBRS data to the State have an interest in doing statistical reporting on their data, and not all RMS systems are able to generate these reports. Beyond 20/20's State clients make the reporting environment available to agencies to allow them to report on their data. As the data is updated daily, the reports can be generated within 24 hours of the data being submitted to the Repository. In some states, all agencies can view data submitted by all agencies; in others each can only report on their own data and State-wide totals.
- d) **Reporting to the public** – Our State clients are often approached by the general public and/or the media with specific questions about crime data/trends. The Beyond 20/20 NIBRS Reporting system makes it easy to generate reports that can then be passed back to the person making the request. An important time saver for some states is allowing the public direct access to the self-serve reporting system to generate their own reports. In these cases, the system is restricted to show only data that has been formally

accepted by the State, usually released on an annual basis a few months into the following year.

- e) **Reporting to policy makers** – As with reporting to the public, the State requires the ability to generate meaningful reports for policymakers and other influencers in the government. In addition to the self-serve reporting (which our clients often run on behalf of their clients), Beyond 20/20 offers a crime trend dashboard, which gives an overview of the situation with crime in the State or any jurisdiction within the State.
- f) **Support for annual crime data publications** – “Crime in Washington” and similar reports in other States include many different tables and charts showing the status of crime in the State. These tables/charts are easily generated and exported (in Excel or PDF formats) using the Beyond 20/20 reporting system. In addition, in Tennessee, we have generated fixed-format reports using Microsoft’s Reporting Services to generate entire pages of content for the “Crime in Tennessee” report. Each year, this report is generated automatically, saving the UCR team much effort that they previously expended on these pages.

The Beyond 20/20 solution is a web-based system that allows users to view, modify, save, and download reports based on the NIBRS data. It includes a set of standard reports that are easily configured by system administrators. The following screenshot shows the front page for the North Dakota internal site.



Reports can be saved in either tabular or chart format. The following shows a typical table.

**Crimes by Offenses Types and Year**  
 Current date: 5/31/2014 7:10:18 AM (Eastern Daylight Time)  
 Jurisdiction (Jurisdiction): North Dakota  
 Measures: Number of Crimes

Rows 1-50 of 63 Columns 1-4 of 4

Incident Date	2010	2011	2012	2013
Offense Type				
All Offense Types	31,997	35,095	38,866	39,539
Crimes Against Person	7,635	7,692	8,530	8,606
Homicide Offenses	12	14	23	15
Murder	9	13	16	11
Negligent Manslaughter	2		7	4
Justifiable Homicide	1	1		
Assault Offenses	6,883	6,967	7,214	7,874
Vehicular Homicide				
Suicide				
Aggravated Assault	845	1,044	1,082	1,158
Simple Assault	4,814	4,999	5,424	5,424
Intimidation	819	824	1,077	1,137
Stalking	405	100	131	155
Kidnapping/Abduction	70	66	71	87
Sex Offenses, Forcible	566	532	622	573
Forcible Rape	226	220	261	244

Once in any of these reports, users can select “dimensions” to be included in the report. These dimensions loosely correspond to fields within the NIBRS data. For any dimension, users can select the “members” or values that are relevant for the report. For instance, a user may wish to see a report that breaks down the age of victims by the day of the week on which the incident occurred, for a given date range within a given jurisdiction.

**Report contents**  
 Instructions: Click on dimension names below and select members (on right) to include in your report

**Measures**

- Jurisdiction
- Agency Status
- Offense Type **▾**
- Criminal Activity Type
- Offense Attempted or Completed
- Offender Used
- Method of Entry
- Type of Weapon/Force Involved
- Bias Motivation
- Incident Date **▾**
- Day of Week **▾****
- Incident Hour of Day
- Location Type
- Offender Age

**Crimes by Offenses Types and Year**  
**Day of Week**  
 Select by: Save selection set... Show report Show report list Help

Members \* Totals Percentages Custom groups Calculated members

Members 1-8 of 8

Select/Clear members by level All Lowest level Range... Default member: All Days of Week

Tip: Use "Expand all" dropdown list to expand to a given level

- All Days of Week (Default member)
- Sunday
- Monday
- Tuesday
- Wednesday
- Thursday
- Friday
- Saturday

Selecting dimensions and members, as well as arranging reports, adding calculations and other special features of the report can all be done with simple mouse clicks and drag/drop operations. Users can quickly toggle between viewing the resulting data in table and chart forms.

Users with sufficient permissions can also use Crime Insight's "microdata" capability to view the individual records that make up the aggregated number shown in any cell of the table. Once in this view, users can sort this data or filter it based on other criteria. This view also includes incident numbers so that users can go back to source data to find out more information about the incident(s) in question.

A typical implementation of Beyond 20/20's web reporting consists of three sites that differ in the target audience and available data. One of these is an internal site, which has access to all data that has been loaded into the system. This site is used for quality control, audit, and state-wide reporting for policy and/or research at the State level. A second site is made available to contributing agencies so they can see all of their own data, review QC reports and do their own analysis. A third site is made available to the general public, containing only data that has been fully reviewed and released (typically from the prior year) and no incident-level data at all.

#### AD-HOC REPORTING

---

This is the area for which Beyond 20/20 is most known and where our service in NIBRS started. As part of the Crime Insight product, we have built a set of multi-dimensional OLAP "cubes". These cubes contain all the data from the submitted NIBRS data, where each cube roughly corresponds to a segment of NIBRS, but include the linkages across the various segments. In this way, some very rich reporting can be done. Beyond 20/20 has created a web application that allows users to browse these cubes, apply calculations (such as totals, percentages, averages, standard deviations, etc.), show charts, and display maps. The mapping element of the software is provided by a third-party GIS applications expert, but has been embedded seamlessly into our application.

#### CUSTOM REPORTING

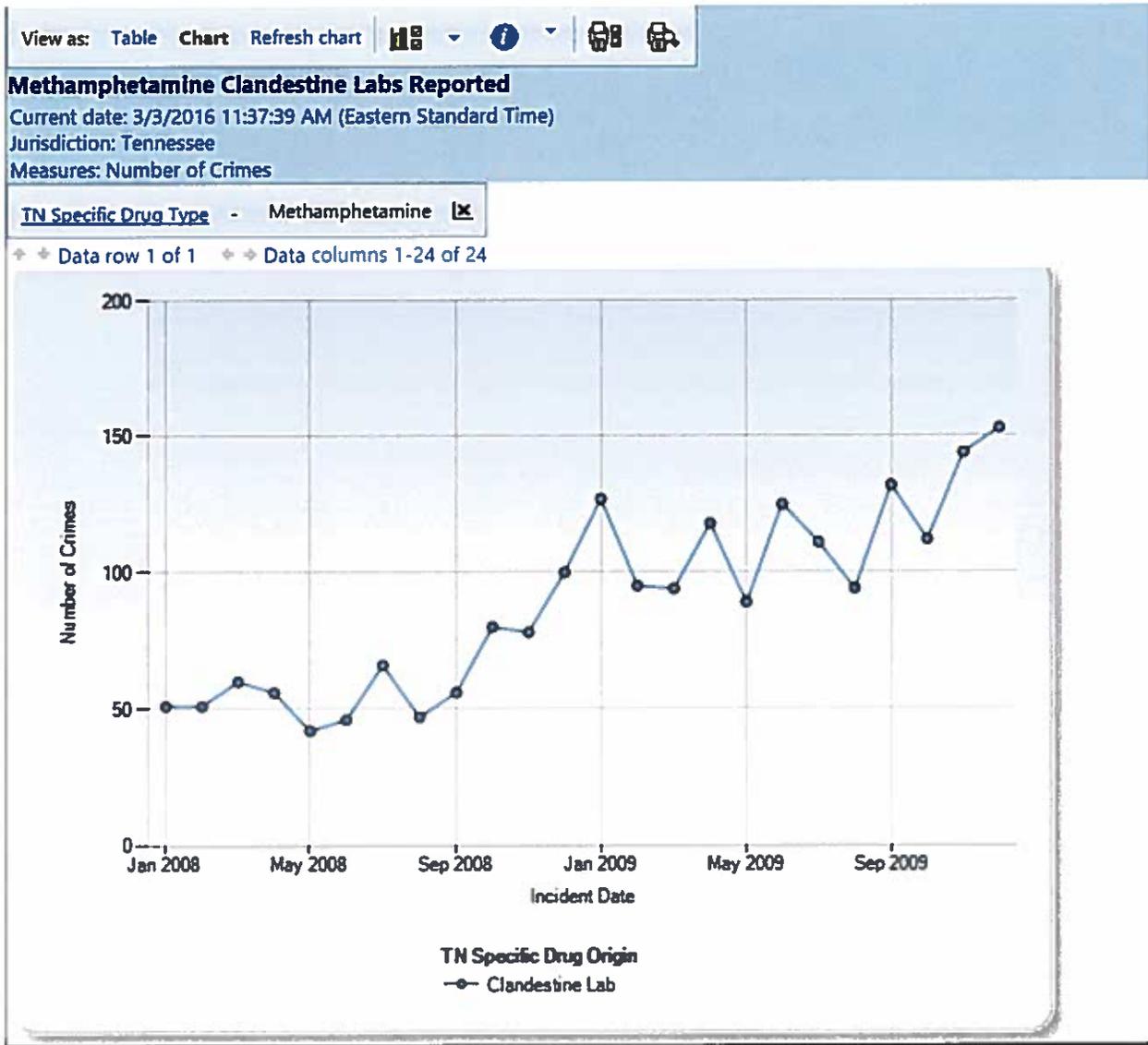
---

With any Crime Insight deployment, Beyond 20/20 also provides some fixed-structure reporting, using Microsoft's Reporting Services tool. These reports can include multiple tables, graphics, maps and other objects blended together to meet the needs of specific reporting. Beyond 20/20 has used these to build pages for the Crime in Tennessee report, mapping for Montana and dashboards to highlight crime trends.

SAMPLE REPORTS

This section includes sample reports that can be created using the Crime Insight Reporting solution.

The state of Tennessee was able to leverage the Crime Insight Reporting solution to generate a report on Methamphetamine Clandestine Labs. Clandestine lab location was used along with number of crimes to identify whether crimes related to this location is a growing trend. Similar reports can be generated on any NIBRS values. Visualisations can also be modified to improve cognitive load.



The below detailed study of violent crime in Tennessee in 2014, is focusing on the relationships between victims and offenders. Not surprisingly, we can find:

1. Female on Female violent crime is primarily between acquaintances, but includes a lot of family members.
2. Cross-gender violent crime is overwhelmingly in intimate relationships
3. Male on Male violent crime is largely between acquaintances, but include strangers as well.

Offense Type - Violent Crime Drag dimensions here so they do not show as a row or column in table

Offender Gender	Female				Male			
Victim Gender	Female		Male		Female		Male	
Measures	Victims	Number of Victims Pct						
Victim to Offender Relat...								
Intimate	4,155	18.93	9,598	57.56	31,399	59.25	3,715	9.92
Family	6,916	31.58	2,712	16.26	7,884	14.89	7,490	20.01
Acquaintance	10,144	46.21	3,645	21.86	10,145	19.16	16,909	45.17
Stranger	2,030	9.25	1,635	9.81	4,889	9.23	10,652	28.46

Leveraging the microdata features (blue target symbol) within data tables allows the user to start at a high level numerical perspective, then drill into an incident list and even a single incident report. This deep level drill down capability allows analysts to see a complete picture of where numbers are coming from and identify common cause.

Aggregated Table:

View as: Table Chart Microdata

**Crime Against Persons by County**  
 Current date: 3/7/2016 9:40:02 AM (Eastern Standard Time)  
 Rows 1-12 of 12 Columns 1-16 of 16

Measures - Number of Crimes Incident Date - 2015 Drag dimensions here so they do not show as a row or column in table

Offense Type	Crimes Against Person	Murder and Nonnegligent M...	Negligent Manslaughter	Justifiable Homicide	Kidnapping/Abduction	Forcible Rape
Jurisdiction by Geography						
Belknap	+ 676				+ 9	+ 16
Carroll	+ 332				- 5	+ 5
Cheshire	+ 491				- 9	- 12
Coos	+ 220					+ 3
Grafton	+ 549				- 10	+ 23
Hillsboro	+ 3,516	+ 10			+ 46	+ 101
Merrimack	+ 1,009		+ 1		- 14	+ 27
Rockingham	+ 2,016	- 1	+ 1		+ 39	+ 39
Strafford	+ 1,235				+ 13	+ 40
Sullivan	+ 382				+ 3	+ 8
Unknown county						
Missing						

Incident List:

**Microdata: Crime Against Persons by County**  
 Current date: 3/7/2016 9:42:20 AM (Eastern Standard Time)  
 Offense Type: Kidnapping/Abduction  
 Jurisdiction by Geography: Belknap  
 Incident Date: 2015

Incident Data Rows 1-9 of 9 Columns 1-16 of 16

#	ORI	Incident Number	Incident Date	Incident Month	Day of Week	Hour of Day	County	Agency Name	Agency Status	Incident Clearance
1	NH0011400	15-18-OF	2015-01-01	January	Thursday	11:00pm-11:59pm	Belknap	Laconia	ORI Active	Not Cleared
2	NH0011400	15-73-AR	2015-01-20	January	Tuesday	10:00pm-10:59pm	Belknap	Laconia	ORI Active	Cleared by Arrest
3	NH0011400	15-28-AR	2015-01-08	January	Thursday	2:00am-2:59am	Belknap	Laconia	ORI Active	Cleared by Arrest
4	NH0011400	15-387-OF	2015-01-24	January	Saturday	7:00pm-7:59pm	Belknap	Laconia	ORI Active	Cleared by Arrest
5	NH0011400	15-134-AR	2015-02-06	February	Friday	1:00pm-1:59pm	Belknap	Laconia	ORI Active	Cleared by Arrest
6	NH0011000	15-284-OF	2015-05-07	May	Thursday	6:00pm-6:59pm	Belknap	Gifford	ORI Active	Not Cleared
7	NH0011400	15-534-AR	2015-05-21	May	Thursday	6:00pm-6:59pm	Belknap	Laconia	ORI Active	Cleared by Arrest
8	NH0010600	15-250-AR	2015-07-22	July	Wednesday	7:00pm-7:59pm	Belknap	Belmont	ORI Active	Cleared by Arrest
9	NH0011200	15-43-OF	2015-09-05	September	Saturday	8:00am-8:59am	Belknap	Gilmanton	ORI Active	Not Cleared

Single Incident:

**Jurisdiction : NH0011400 | Laconia**

**Incident Number : 15-28-AR**

**Administrative**

Jurisdiction : NH0011400 | Laconia

Incident Number : 15-28-AR

Incident Date : 01/08/2015 Hour : 02 Cargo Theft :

Clearance Code : ARR

Clearance Description : Cleared by Arrest Clearance Date:

**Offenses**

Offense		Attempted/ Completed	Location Type		# Premises Entered	Method of Entry	
Code	Description		Code	Description		Code	Description
100	Kidnapping/Abduction	C	20	Residence/Home			Missing
13A	Aggravated Assault	C	20	Residence/Home			Missing

**Offenses - Weapons**

Offense	Weapon Type	
Code	Code	Description
100	40	Personal Weapons (Hands, Feet, Teeth, Etc.)

The State-wide Crime Summary report is included in the product. A sample is shown below:

**Tennessee Statewide - 2014**

<b>2014 Population Estimate</b>	<b>6,549,352</b>
<b>Offense Overview</b>	
Offense Total	536,597
Number Cleared	213,063
Percent Cleared	39.71 %
Group A Crimes per 100,000 population	8,193.1
<b>Arrest Overview</b>	
Total Arrests	360,704
Adult Arrests	334,339
Juvenile Arrests	26,365
Unknown Age	27
Arrests per 100,000 population	5,507.5
Average number offenses/incident	1.17

Domestic Violence Victims		
Offense	Reported	Cleared
Murder	83	78
Aggravated Assault	11,232	8,219
Simple Assault	52,089	32,703
Intimidation	9,830	3,401
Stalking	765	295
Forcible Rape	549	247
Forcible Sodomy	155	61
Sexual Assault W/Object	105	55
Forcible Fondling	613	230
Incest	12	7
Statutory Rape	166	92
Kidnapping/Abduction	763	521
<b>Total</b>	<b>76,362</b>	<b>45,909</b>

TIBRS Group B Arrests		
Offense	Adult	Juvenile
Bad Checks	2,284	2
Curfew/Vagrancy	8	1,550
Disorderly Conduct	6,325	2,374
DUI	26,954	175
Drunkennes	17,481	196
Family-Non Violent	3,473	74
Liquor Law Violations	6,169	936
Peeping Tom	20	1
Trespass	8,193	858
All Other Offenses	119,747	3,543
<b>Total Group B</b>	<b>190,654</b>	<b>9,709</b>

TIBRS Group A Offenses	Offenses		Arrests	
	Reported	Cleared	Adult	Juvenile
<b>Crimes Against Persons</b>				
Murder	369	248	263	19
Negligent Manslaughter	6	6	4	1
Kidnapping/Abduction	1,225	707	477	17
Forcible Rape	1,930	640	234	68
Forcible Sodomy	450	153	27	13
Sexual Assault W/Object	249	97	21	8
Forcible Fondling	2,334	823	243	81
Incest	12	7	7	0
Statutory Rape	516	274	186	1
Aggravated Assault	29,865	16,465	13,076	1,224
Simple Assault	84,193	46,143	23,585	4,160
Intimidation	27,028	7,109	2,696	454
Stalking	1,539	542	333	6
Commercial Sex Acts	34	14	2	0
Involuntary Servitude	1	0	2	0
<b>Crimes Against Property</b>				
Arson	1,087	231	162	63
Bribery	30	22	17	0
Burglary	46,731	5,964	4,775	848
Counterfeiting/Forgery	7,343	2,288	1,514	56
Destruction/Damage/Vandalism	52,340	9,919	3,549	1,028
Embezzlement	2,609	1,216	646	15
Extortion/Blackmail	131	33	15	3
Fraud - False Pretenses	11,889	3,194	1,398	28
Fraud - Credit Card/ATM	9,395	1,725	659	19
Fraud - Impersonation	5,829	2,203	1,687	63
Fraud - Welfare	351	191	67	0
Fraud - Wire	704	40	17	0
Motor Vehicle Theft	13,008	2,777	1,688	277
Robbery	7,323	1,787	1,622	381
Stolen Property Offenses	890	674	670	68
Theft - Pocket-picking	488	41	23	17
Theft - Purse Snatching	266	51	20	5
Theft - Shoplifting	36,652	23,003	22,624	3,008
Theft From Building	31,976	5,715	2,637	366
Theft From Coin Machine	361	30	18	3
Theft From Motor Vehicle	28,253	2,360	1,450	279
Theft of Motor Vehicle Parts	11,567	427	247	21
Theft - All Other Larceny	34,245	4,629	4,112	490
<b>Crimes Against Society</b>				
Drug/Narcotic Violations	47,546	40,634	38,371	2,501
Drug/Narcotic Equipment Violations	25,333	23,050	10,393	502
Gambling - Betting/Wagering	36	28	108	19
Gambling - Operating/Promoting	26	18	18	0
Gambling - Equipment Violations	88	76	45	10
Gambling - Sports Tampering	4	3	0	0
Pornography/Obscene Material	609	219	81	49
Prostitution	1,339	1,201	1,248	0
Prostitution Assisting/Promoting	122	108	91	0
Purchasing Prostitution	62	57	44	0
Weapon Law Violations	8,213	5,921	2,513	485
<b>Total Group A Offenses</b>	<b>536,597</b>	<b>213,063</b>	<b>143,685</b>	<b>16,656</b>

The following screenshot shows our integrated Quality Control report, which performs over 60 checks that are not part of the formal validation in the Repository. Each incident that fails any of these checks is included in the report, with details of the issue(s) found. The QC report is part of the core product.

**Agency QC Exceptions**  
**TN0200100 - Parsons Police Department**  
 From 01/01/2013 To 12/31/2013

**Arrestee Issues**  
 No Arrestee Issues found.

**Offender Issues**  
 No Offender Issues found.

**Offense Issues**

**Aggravated Assault with Minor Injury and Personal Weapons**

Incident Number	Incident Date	Sequence Number	Offense Code	Weapon Code	Injury Code
131121030022	11/17/2013	1	13A	40	M

By definition, an Aggravated Assault must have a weapon other than Personal Weapons if injury is minor. Change weapon type or report as Simple Assault

**Property Issues**

**Pending Inventory over 90 Days**

Incident Number	Incident Date	Loss	Category
2014-10-558	10/14/2014	Stolen	88

Pending Inventory should be used as a temporary description. The above property was classified as "pending inventory" more than three months ago and should be updated to the appropriate category.

**Victim Age Issues**

**Victim Under Age 6**

Incident Number	Incident Date	Seq #	Age
131108092446	10/15/2013	2	BB

Please confirm that victim age was under age 6. Correct as necessary.

**Victim Other Issues**

**TN - College Student Not in Reporting County**

Incident Number	Incident Date	Seq #	Campus	School CID
21851	07/29/2013	1	Y	3178

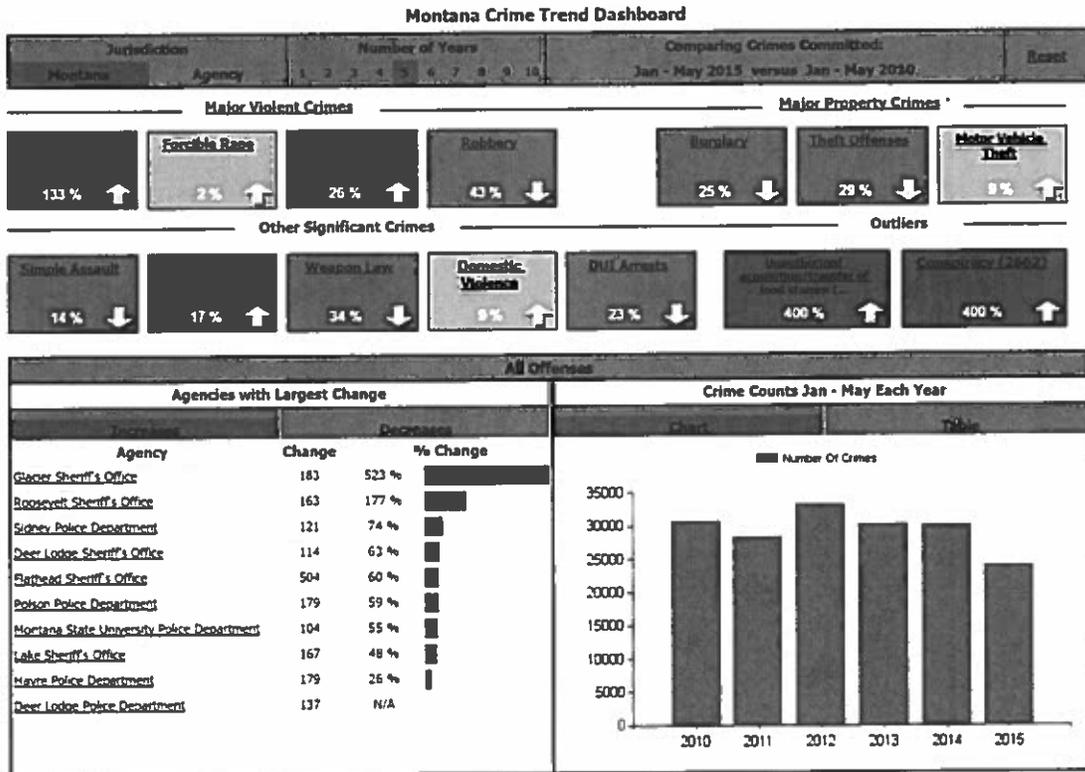
Please remove college student information for this victim. College student information is only applicable for colleges/universities in your county.

**LEOKA ORI**

Incident Number	Incident Date	Seq #	Type Code	LEOKA ORI
130912094629	08/30/2013	1	L	

Valid Data: Please review the Leoka Ori column. Valid Ori's must have the state abbreviation in capital letters and contain a total of 9 characters. Note: Your ORI should not appear in the list. This field should only be used if an officer from another jurisdiction is assaulted or killed in the line of duty in your jurisdiction.

The following screenshot shows our Crime Trend Dashboard, which is available as an add-on at additional cost. A complete description of this dashboard is available upon request.



APPENDIX B: VENDOR FINANCIAL QUALIFICATIONS AND ANNUAL REPORTS

APPENDIX C: VENDOR PURCHASE CONTRACT

Beyond 20/20 will work with the State supplied purchasing contract. All relevant terms to purchase are covered under the End User Licensing Agreement.

## APPENDIX D: VENDOR SOFTWARE LICENSE AGREEMENTS

## EULA

Beyond 20/20 Inc.  
Beyond 20/20™ License Agreement

Before opening the package containing the Beyond 20/20 software or clicking “ACCEPT” when this license is shown when installing or using the software, please carefully read this license, which contains the terms and conditions under which you are acquiring a license to use the software. If you do not accept the terms and conditions of the license, please DO NOT INSTALL THE SOFTWARE AND promptly return the unopened OR UNINSTALLED SOFTWARE to the place AT WHICH YOU ACQUIRED IT for a full refund of ANY license fee paid. If you open THE ACCOMPANYING SOFTWARE OR INSTALL OR USE IT, you will be acquiring a license to use the SOFTWARE IN OBJECT CODE FORM, in accordance with the terms and conditions of this license Agreement, and You will be considered to have accepted and agreed to these terms and conditions.

**1. Grant of License**

a) Subject to the terms and conditions contained in this license agreement and in the product license registration (the “Registration”) (collectively, the “Agreement”) and subject to Beyond 20/20 Inc. having received and accepted full payment of the applicable license fee, Beyond 20/20 Inc. hereby grants to the licensee identified on the Registration (“You”) a non-assignable, non-exclusive, non-transferable, restricted license to use the software identified on the Registration (the “Software”) in object code form solely on the computer(s), at the site(s), for the subject matter(s), for the type of use, for the number of permitted users and for the term specified on the Registration. “Software” means (a) all of the contents of the disk(s), CD-ROMs, or other media with which this Agreement is provided, including but not limited to (i) Beyond 20/20 and third party software delivered by Beyond 20/20 with the license agreement and (ii) related explanatory written material (“Documentation”); and (b) modified versions, upgrades, updates, additions, maintenance releases and copies of the Software, if any, provided to You by Beyond 20/20 Inc. if a separate license agreement is not delivered with or as part of them.

b) If Beyond 20/20 Inc. has permitted You to install the Software for evaluation purposes, You agree to evaluate the Software only for the evaluation period specified on the Registration. You agree not to use the Software to process data in a live, production mode. You also agree to remove the Software and all files generated by the Software from Your computer and to return the Software to Beyond 20/20 Inc. at the end of the evaluation period except if you obtain a further license from Beyond 20/20.

c) All license fees are exclusive of applicable taxes. You will be solely responsible for all applicable sales or equivalent tax consequences, which may relate to or arise from this Agreement.

## **2. Confidentiality**

You acknowledge that the Software and Documentation relating thereto contain confidential information of Beyond 20/20 Inc. and its licensors and You agree not to disclose such confidential information, either directly or indirectly, to any third party. For the purposes of this Agreement, confidential information shall include, but shall not be limited to, product plans, commercial plans, policies, functional and technical specifications and other proprietary information furnished by Beyond 20/20 Inc. or its licensors (the "Confidential Information"), but shall not include information that has become generally available to the public, other than as a result of Your breach of any obligation under this Agreement or information disclosed to You on a non-confidential basis by a third party who did not owe an obligation of confidence in respect of such information. You agree to treat the Confidential Information in the same manner as You treat Your own confidential information, but in no case will the degree of care be less than reasonable care. Without limiting the generality of the foregoing, the Confidential Information shall be accessible only to You and Your employees and contractors with a need for access to same for the purposes of performing their duties, and You shall advise such employees and contractors of the confidentiality restrictions contained herein and ensure their compliance with such restrictions. Upon Beyond 20/20 Inc.'s request when this Agreement has expired or is terminated, You shall promptly return to Beyond 20/20 Inc. or destroy all Confidential Information that has been supplied to You by Beyond 20/20 Inc. You acknowledge and agree that any actual or threatened unauthorized use, reproduction, distribution or disclosure of Confidential Information is likely to cause irreparable harm and significant injury, the degree of which would be difficult to ascertain, and which would not likely be compensable by money damages alone, and therefore: (a) Beyond 20/20 Inc. and its licensors will have the right to seek an order to enforce the terms of this Agreement by specific performance; and (b) You agree that in such an event the issuance of an injunction is likely to be an appropriate remedy, without prejudice to any other rights and remedies that Beyond 20/20 Inc. or its licensors may have for Your breach of this Agreement.

## **3. Ownership**

The copyright, intellectual property, and all other right, title and interest in the Software, Documentation, and any Beyond 20/20 tables, extracts and files created with the Software including, without limitation, any Executables produced with the Software, remain the exclusive property of Beyond 20/20 Inc. and/or its licensors. Physical copies of the Software remain the property of Beyond 20/20 Inc. and/or its licensors and such copies are deemed to be on loan to You during the term of this Agreement. The data content of the Beyond 20/20 tables and extracts belong to the owners of the data.

## **4. Restrictions**

No rights are granted to You except those expressly set forth in writing in this Agreement. You agree not to modify, translate, adapt, reverse engineer, decompile or disassemble, or otherwise attempt to discover the source code of the Software. In addition, except to the extent specifically permitted in this Agreement, You agree not to:

(i) Rent, lease, assign, sub-license, sell, transfer, transmit, publish, distribute, permit concurrent use of, grant other rights, or otherwise disseminate or provide access to the Software or any files created with the Software including, without limitation any Executables, whether voluntarily or by the operation of law or otherwise, except as expressly set out in writing;

(ii) Provide use of the Software in a computer service business, network, time sharing, or interactive cable television arrangement to persons who are not properly licensed by Beyond 20/20 Inc.;

(iii) Create derivative works with any part of the Software;

(iv) make copies of the Software or Documentation, except that You may make one (1) backup copy of the Software, provided Your back-up copy is not installed or used on any computer unless the computer(s) on which the Software is permitted to be installed is inoperable as a result of a technical malfunction or other similar condition;

(v) Use the Beyond 20/20 tables or extracts created using the Software on any other computer systems unless You are properly licensed to use a Beyond 20/20 browser on those computer systems; or

(vi) Make the Software available over the Internet.

## **5. Trademarks and Copyright**

The Software and any copies that You are permitted to make are owned by Beyond 20/20 Inc. and its licensors. Any copies that You are permitted to make pursuant to this Agreement must contain the same copyright and other proprietary notices that appear on or in the Software and Documentation and you must not alter or remove any such copyright or other notice on the original copy of the Software or Documentation. You acknowledge that "Beyond 20/20 Inc.", "Beyond 20/20", "Beyond 20/20 Publisher's Edition", "Beyond 20/20 Browser", "Beyond 20/20 Professional Browser", "Beyond 20/20 Publication Browser", "Beyond 20/20 Web Data Server", "Beyond 20/20 Perspective", "Beyond 20/20 Toolkit" "Beyond 20/20 Data Connection Wizard" and "Beyond 20/20 Crime Insight" are trademarks of Beyond 20/20 Inc. You shall not make any use of such trademarks without the prior written consent of Beyond 20/20 Inc. This Agreement does not grant You any intellectual property rights in the Software.

## **6. Limited Warranty**

Beyond 20/20 Inc. warrants to You that the Software will perform substantially in accordance with the Documentation for thirty (30) days following Your acquisition of the Software, provided Beyond 20/20 Inc. has received payment from You of the applicable license fee. During such 30-Day Warranty and provided the Software is operated as directed in the Documentation, Beyond 20/20 Inc. warrants that: (i) the Software functions substantially as described in the Documentation, and (ii) the media containing the Product, if provided by

Beyond 20/20 Inc., is free from defects in material and workmanship and will so remain for thirty (30) days from the date You acquired the Software.

Beyond 20/20 Inc.'s sole responsibility for any breach of this warranty shall be, at Beyond 20/20 Inc.'s sole discretion: (i) to replace the defective media, or (ii) to advise You how to achieve the same functionality with the Software as described in the Documentation through procedures different from those set forth in the Documentation. Repaired, corrected, or replaced Software and Documentation shall be covered by this limited warranty for the period remaining under the warranty that covered the original Software. Only if You inform Beyond 20/20 Inc. of Your problem with the Software during the warranty period and provide evidence satisfactory to Beyond 20/20 Inc. of the date You purchased a license to the Software will Beyond 20/20 Inc. be obligated to honor this warranty. Beyond 20/20 Inc. will make reasonable commercial efforts to replace and advise under this warranty and if the problem persists following such replacement or advice, Beyond 20/20 Inc. will refund the license fees paid hereunder provided You return to Beyond 20/20 Inc. all copies of the Software and Documentation and purge all copies from Your systems.

Beyond 20/20 Inc. shall have no responsibility for the Software if it has been altered in any way, if the media or the Software has been damaged by accident, abuse or misapplication, or if the problem arises out of use of the Software in conjunction with software not supplied by Beyond 20/20 Inc. Unless otherwise expressly agreed to in writing, Beyond 20/20 Inc. is not responsible for the installation or integration of the Software or for any data conversion required in order to use the Software.

Except as otherwise expressly provided in this agreement, at to the maximum extent permitted by law, Beyond 20/20 Inc. and its licensors provide the Software and any related services strictly "As Is" and with all faults. Beyond 20/20 Inc. does not warrant that the Software will be error free or secure or that its operation will be uninterrupted. The limited warranty contained in this agreement is in lieu of all other warranties, conditions, undertakings or terms, express or implied, written or oral, and Beyond 20/20 Inc. hereby disclaims all warranties and conditions of any kind including but not limited to implied warranties and conditions of merchantability, fitness for a particular purpose, non-infringement of third parties' rights, and those arising by statute or from a course of dealing, usage or trade. No Beyond 20/20 Inc. agent, employee, representative, or dealer is authorized to modify, extend or add to this warranty. The warranties in this Agreement give You specific legal rights. You may have other rights, which vary from jurisdiction to jurisdiction.

## **7. Limitation of Liability**

Except at otherwise expressly provided in this agreement, You assume the entire risk as to the results and performance of the Software. Under no circumstances and under no legal theory, whether in tort, contract or otherwise, shall Beyond 20/20 Inc. or its agents, licensors, suppliers or resellers have any liability to You or any other person or entity for any direct, indirect, incidental, special, exemplary, consequential or other damages of any kind or nature whatsoever, including but not limited to loss of good will, loss of data, loss of software or

hardware, loss of profit, work stoppage, computer failure or malfunction, or any and all other commercial or economic damages or losses, even if Beyond 20/20 Inc. has been advised of the possibility of such damages or if such damages could have been reasonably foreseen.

Without limiting the provisions of this section, the maximum aggregate liability of Beyond 20/20 Inc. and its agents, licensors, suppliers or resellers in connection with this agreement or the Software, whether arising in tort, contract, or otherwise, shall not exceed the license fee paid by You to Beyond 20/20 Inc. Under this Agreement, this section shall survive and apply notwithstanding any fundamental breach or the failure of essential purpose of this Agreement. You agree that these limitations of liability are agreed allocations of risk and are reflected in the fees paid under this Agreement. Nothing in this Agreement shall restrict Beyond 20/20 Inc.'s liability in a manner which is expressly prohibited by applicable statute or regulation.

#### **8. Publicity**

You authorize Beyond 20/20 Inc. to publicly reference You as a user of the Software. You grant Beyond 20/20 Inc. the right to publish and disclose Your name and the general nature of usage including, without limitation, in brochures, press releases, proposals, promotional literature, on its web site and other publications and public disclosures.

#### **9. Termination**

Beyond 20/20 Inc. may terminate this license due to Your failure to comply with any of the provisions of this Agreement. Upon termination, all Your license rights to the Software shall cease and You agree to purge the Software from Your systems and destroy or return to Beyond 20/20 Inc. all copies of the Software and Documentation and provide evidence satisfactory to Beyond 20/20 Inc. of such purging and destruction or return.

#### **10. U.S. Government Restricted Rights Legend**

Pursuant to FAR 12.212(a) and DFAR 227.7202-1(a), use, duplication or disclosure by the Government is subject to the terms of Beyond 20/20 Inc.'s standard form license.

#### **11. Export Restrictions**

You hereby agree and confirm that You are not a resident of, and this transaction is not in any way connected with, any jurisdictions which are prohibited by applicable law, including without limiting the foregoing, jurisdictions included under the Area Control List of the Exports and Imports Permit Act of Canada. You agree and confirm that this transaction is in full and complete compliance with the laws of the jurisdiction to which the Software is delivered, and that You shall not, in any manner whatsoever, either remove, convey, export or transmit the Software from such jurisdiction other than in compliance with all applicable laws.

#### **12. Governing Law**

This Agreement shall be governed by the laws of the Province of Ontario, Canada, without giving effect to the principles of conflicts of law, and excluding (i) that body of law applicable to choice of law and (ii) the United Nations Convention on Contracts for the International Sale of

Goods. You agree that the courts of such province constitute a convenient forum for any such litigation and You attorn and submit to the non-exclusive jurisdiction of such courts.

### **13. General**

If any provision of this Agreement is found to be invalid or unenforceable, such provision shall be severed from this Agreement and the remaining provisions shall remain in full force and effect. A delay or failure by either party to exercise any right, or a partial or single exercise of any right, shall not constitute a consent to any subsequent breach. Neither party shall be responsible for any failure or delay in complying with the terms of this Agreement resulting from events of force majeure beyond the control of such party which could not be avoided by exercise of due care.

You shall have no right to assign this Agreement any rights or obligations under this Agreement. Notwithstanding any provision to the contrary in any purchase order, all purchase orders from You shall be conclusively deemed to be governed by this Agreement and any terms additional to or inconsistent with this Agreement shall be deemed stricken from such purchase order.

This Agreement (including the Registration) contains the complete understanding and agreement of the parties and supersedes all prior agreements or understandings, oral or written, relating to the subject matter herein. In the event of any conflict or inconsistency between this Agreement and the Registration, the terms of the Registration shall prevail to the extent of such conflict or inconsistency. This Agreement may be amended only in writing and executed by both parties.

The parties confirm that it is their wish that this Agreement as well as all other documents relating to this Agreement, including notices, be drawn up in English only. Les parties aux présentes confirment que c'est leur volonté que la présente convention de même que tous les documents, y compris les avis, qui s'y rattachant, soient rédigés en anglais.

The provisions of this Agreement that are expressed or by their sense and context are intended to survive the termination of this Agreement shall so survive, including without limitation, Sections 2, 3, 5, 6, 7 and 13.

© 1995-2016 Beyond 20/20 Inc. All rights reserved.

BEYOND 20/20 INC.

265 Carling Avenue, Suite 300, Ottawa, Ontario, Canada K1S 2E1  
www.beyond2020.com; sales@beyond2020.com

# **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**

NIBRS RFP Evaluation Total Score *Score 680*

Vendor Name: **Beyond 20/20**

Point Value    Points Given    Comments (Use additional page if necessary)

	Point Value	Points Given	Comments (Use additional page if necessary)
I Preliminary Evaluation	300	<i>250</i>	
II Technical Solution	100	<i>100</i>	
III Project Management	100	<i>100</i>	
IV Proposal Format	100	<i>100</i>	
V Technical Specifications - Basic Requirements	100	<i>100</i>	
VI Technical Specifications - Preferences	100	<i>100</i>	
VII Add-On Components	100	<i>80</i>	
VIII Management Requirements	100	<i>100</i>	
<b>Sub-Total I - VIII</b>	<b>1,000</b>	<i>930</i>	
<b>References:</b>			
Reference 1	100		
Reference 2	100		
Oral Presentation	200		
Price / Value	500	<i>200</i>	

Total Points Possible 1,900

Vendor: **Beyond 20/20**

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

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		
<b>A. Administrators and Users</b>		
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
<b>Sub-Total</b>	15	15
<b>B. Data Entry and File Upload</b>		
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
<b>Sub-Total</b>	<b>18</b>	<b>18</b>
<b>C. Data Reports</b>		
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
<b>Sub-Total</b>	<b>15</b>	<b>15</b>
<b>D. Data Validation and Error Notification</b>		
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
<b>Sub-Total</b>	<b>14</b>	<b>14</b>
<b>E. State System</b>		
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
<b>Sub-Total</b>	<b>12</b>	<b>12</b>
<b>F. System Features</b>		
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		
<b>Sub-Total</b>	<b>14</b>	<b>14</b>
<b>G. Vendor Responsibilities</b>		
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
<b>Sub-Total</b>	<b>12</b>	<b>12</b>
<b>Total for Section E. Technical Specifications - Preferences</b>	<b>100</b>	<b>100</b>

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	20
<b>Sub-Total</b>	<b>100</b>	<b>80</b>

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
<b>Sub-Total</b>	<b>100</b>	<b>100</b>

NIBRS RFP Evaluation Total Score

Score 651

Vendor Name: **Beyond 20/20**

Point Value    Points Given

Comments (Use additional page if necessary)

	Point Value	Points Given	Comments (Use additional page if necessary)
I Preliminary Evaluation	300		
II Technical Solution	100	90	
III Project Management	100	100	Need reference info
IV Proposal Format	100	80	
V Technical Specifications - Basic Requirements	100	100	
VI Technical Specifications - Preferences	100	83	
VII Add-On Components	100	100	
VIII Management Requirements	100	98	
<b>Sub-Total I - VIII</b>	<b>1,000</b>		
<b>References:</b>			
Reference 1	100		
Reference 2	100		
Oral Presentation	200		
Price / Value	500		\$310,700 first year + \$72,000 2y addtl maint

Total Points Possible 1,900

Vendor: **Beyond 20/20**

A. Technical Solution		
1. Fulfillment of the requirements as stated in this RFP	20	15
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	20
	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	15
6. Special consideration for detailed project plan	20	15
	100	100

*Referon*

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	0
Appendix C Vendor purchase contract	10	0
Appendix D Vendor software license agreements	10	10
	100	80

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		
<b>A. Administrators and Users</b>		
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	2
4. System allows user to cancel duplicate file upload	1	2
5. State system administrators (SSAs) have access to a contact database	1	0
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
<b>Sub-Total</b>	15	13
<b>B. Data Entry and File Upload</b>		
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	0

4. IIE has drop down menus	2	2
5. IIE mandatory or invalid fields are highlighted	1	0
6. IIE cannot advance without completing mandatory fields	1	0
7. IIE mandatory fields highlight per offense	1	0
8. When IIE complete, NIBRS check lists errors and returns user to screen	1	0
9. IIE entry of date or calendar option	1	1
10. IIE hot key options are available	1	0
11. IIE entry sequence: Admin, Offense, Victim, Offender, Property, Arrestee	1	1
12. IIE of domestic violence: DV is associated with the Victim	2	1
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
<b>Sub-Total</b>	<b>18</b>	<b>10</b>
<b>C. Data Reports</b>		
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	0
<b>Sub-Total</b>	<b>15</b>	<b>14</b>
<b>D. Data Validation and Error Notification</b>		
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	0
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	0
<b>Sub-Total</b>	<b>14</b>	<b>10</b>
<b>E. State System</b>		
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
<b>Sub-Total</b>	<b>12</b>	<b>12</b>
<b>F. System Features</b>		
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	1
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	0
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		
<b>Sub-Total</b>	<b>14</b>	<b>12</b>
<b>G. Vendor Responsibilities</b>		
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
<b>Sub-Total</b>	<b>12</b>	<b>12</b>
<b>Total for Section E. Technical Specifications - Preferences</b>	<b>100</b>	<b>83</b>

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
	<b>100</b>	<b>100</b>

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	8
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
	<b>100</b>	<b>98</b>

NIBRS RFP Evaluation Total Score

Score 647

Vendor Name: Beyond 20/20

	Point Value	Points Given	Comments (Use additional page if necessary)
<b>I Preliminary Evaluation</b>	300		
<b>II Technical Solution</b>	100	100	
<b>III Project Management</b>	100	90	
<b>IV Proposal Format</b>	100	84	
<b>V Technical Specifications - Basic Requirements</b>	100	94	
<b>VI Technical Specifications - Preferences</b>	100	84	
<b>VII Add-On Components</b>	100	100	
<b>VIII Management Requirements</b>	100	95	
<b>Sub-Total I - VIII</b>	<b>1,000</b>		
<b>References:</b>			
<b>Reference 1</b>	100		
<b>Reference 2</b>	100		
<b>Oral Presentation</b>	200		
<b>Price / Value</b>	500		

Total Points Possible 1,900

Vendor: **Beyond 20/20**

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	16
5. Ability to meet deadlines	15	15
6. Special consideration for detailed project plan	20	17
	100	90

C. Proposal Format		
Cover letter	10	10
Section 1 Proposal executive summary	10	10
Section 2 Technical solution and description	10	9
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	0
Appendix C Vendor purchase contract	10	5
Appendix D Vendor software license agreements	10	10
	100	84

D. Technical Specifications - Basic Requirements		
1. Ability to capture and preserve NIBRS data pursuant to current FBI Tech Spec	20	17
2. System allows entry of standard values for each data element	20	20
3. System meets additional WA State IBR data collection requirements	20	17
4. System performs editing and validation of data	20	20
5. System provides capability for submission of NIBRS data	20	20
	100	94

E. Technical Specifications - Preferences		
<b>A. Administrators and Users</b>		
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	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	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
	<b>Sub-Total</b>	14
<b>B. Data Entry and File Upload</b>		
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	.5
6. IIE cannot advance without completing mandatory fields	1	.5
7. IIE mandatory fields highlight per offense	1	.5
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	0
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
<b>Sub-Total</b>	<b>18</b>	<b>14</b>
<b>C. Data Reports</b>		
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	0
g. Outstanding Errors and Incidents/Arrests Not Checked	1	.5
h. Static report (snapshot) of database	1	1
<b>Sub-Total</b>	<b>15</b>	<b>13.5</b>
<b>D. Data Validation and Error Notification</b>		
1. System meets all FBI and WA State data validation edits and error checks	2	1
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	0
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	0
<b>Sub-Total</b>	<b>14</b>	<b>9</b>
<b>E. State System</b>		
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
<b>Sub-Total</b>	<b>12</b>	<b>11</b>
<b>F. System Features</b>		
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	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

fee

fee

6. All related cases for Multiple Clearance indicator are displayed	1	.5	fee
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	fee
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		<	NO
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		<	yes
<b>Sub-Total</b>	<b>14</b>	<b>12</b>	
<b>G. Vendor Responsibilities</b>			
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	FBI's
5. Vendor included record layouts and report samples in the technical section	1	10	FBI's
6. Vendor has customer service available Monday through Friday, 8am-4pm, Pacific Time	1	1	
a. Vendor has process for Work Order Number assignment		-	- NO, BUT web ACCESS
b. SSAs are able to check status of work order via on-line tracking system			yes
7. Vendor will update system per FBI requirements at no additional cost	1	1	Annual fee
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	
<b>Sub-Total</b>	<b>12</b>	<b>10.5</b>	
<b>Total for Section E. Technical Specifications - Preferences</b>	<b>100</b>	<b>84</b>	

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
	<b>100</b>	<b>100</b>

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	5
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
	<b>100</b>	<b>95</b>

NIBRS RFP Evaluation Total Score **Score 622.5**

Vendor Name: **Beyond 20/20**

Point Value    Points Given

Comments (Use additional page if necessary)

	Point Value	Points Given	Comments (Use additional page if necessary)
<b>I Preliminary Evaluation</b>	300		
<b>II Technical Solution</b>	100	80	
<b>III Project Management</b>	100	80	
<b>IV Proposal Format</b>	100	80	
<b>V Technical Specifications - Basic Requirements</b>	100	100	
<b>VI Technical Specifications - Preferences</b>	100	82.5	
<b>VII Add-On Components</b>	100	100	
<b>VIII Management Requirements</b>	100	100	
<b>Sub-Total I - VIII</b>	1,000		
<b>References:</b>			
<b>Reference 1</b>	100		
<b>Reference 2</b>	100		
<b>Oral Presentation</b>	200		
<b>Price / Value</b>	500		

Total Points Possible 1,900

Vendor: Beyond 20/20

A. Technical Solution		
1. Fulfillment of the requirements as stated in this RFP	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	80

B. Project Management		
1. Completeness and responsiveness of project management plans	15	15
2. Project Team assigned	15	0
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	15
	100	80

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	0
Appendix C Vendor purchase contract	10	0
Appendix D Vendor software license agreements	10	10
	100	80

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		
<b>A. Administrators and Users</b>		
1. Levels of user privileges: administrator, power user, report generator	2	1
2. User receives immediate notification when upload successful or failed	2	0
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
5. State system administrators (SSAs) have access to a contact database	1	1.5
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
<b>Sub-Total</b>	15	9
<b>B. Data Entry and File Upload</b>		
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	0

4. IIE has drop down menus	2	2
5. IIE mandatory or invalid fields are highlighted	1	.5
6. IIE cannot advance without completing mandatory fields	1	.5
7. IIE mandatory fields highlight per offense	1	.5
8. When IIE complete, NIBRS check lists errors and returns user to screen	1	.5
9. IIE entry of date or calendar option	1	1
10. IIE hot key options are available	1	0
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
<b>Sub-Total</b>	<b>18</b>	<b>13</b>
<b>C. Data Reports</b>		
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	0
h. Static report (snapshot) of database	1	1
<b>Sub-Total</b>	<b>15</b>	<b>14</b>
<b>D. Data Validation and Error Notification</b>		
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	0
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	1
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	.5
<b>Sub-Total</b>	<b>14</b>	<b>10.5</b>
<b>E. State System</b>		
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
<b>Sub-Total</b>	<b>12</b>	<b>12</b>
<b>F. System Features</b>		
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	1
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	0
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		✓
<b>Sub-Total</b>	<b>14</b>	<b>12</b>
<b>G. Vendor Responsibilities</b>		
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
<b>Sub-Total</b>	<b>12</b>	<b>12</b>
<b>Total for Section E. Technical Specifications - Preferences</b>	<b>100</b>	<b>825</b>

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
<b>Sub-Total</b>	<b>100</b>	<b>100</b>

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
<b>Sub-Total</b>	<b>100</b>	<b>100</b>

# **Phase 2 Evaluation**

Vendor: Beyond 20/20

A. Technical Specifications - Basic Requirements		Yes	No	Unknown
1. System appears to capture NIBRS data pursuant to current FBI Tech Spec		X		
Comments:				
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)				
Comments:				
4. System performs editing and validation of data		X		
Comments:				
5. System provides capability for submission of NIBRS data		X		
Comments:				

B. Technical Specifications - Preferences				
<b>A. Administrators and Users</b>				
1. Levels of user privileges: administrator, power user, report generator				Customization?
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				Y
6. SSAs receive notifications when file uploads stop, fail, or duplicate				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:				
<b>B. Data Entry and File Upload</b>				
1. Submission options include both batch file upload and individual incident entry		X		
2. Individual incident entry (IIE) has data validation on each field		X		
3. IIE is user friendly			X	
4. IIE has drop down menus		X		
5. IIE mandatory or invalid fields are highlighted			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			X	
11. IIE entry sequence: Admin, Offense, Victim, Offender, Property, Arrestee		X		
12. IIE of domestic violence: DV is associated with the Victim				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	

Comments: Not very user friendly, but works			
<b>C. Data Reports</b>			
1. System provides report writing capability; includes standard and ad hoc reports	X		
2. System allows data output in MS Access, Excel, Word, PDF in report & data form	X	X	
3. LEAs have access to other LEA data for report extraction			
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 Category			
e. Hate Crime			
f. Activity Log (by month or year)			
g. Outstanding Errors and Incidents/Arrests Not Checked			
Comments:			
Perspective has tutorials - charts, data, micro.			
Avail. to public or self			
<b>D. Data Validation and Error Notification</b>			
1. System meets all FBI (and WA State) data validation edits and error checks CAN?			
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 good messages			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:			

- Data entry section is functional, but not set-up to be user friendly
- Think reports will appeal to end users as they can be viewed different ways - micro/charts/Tables
- Still limited w/ reports (marijuana arrests)
- found perspective module for reports. This is good, just not the repository we would need
- would be valuable to have come out to demo repository, could have answered more questions.

Beyond 20/20

- Data Entry/File Upload is not very user friendly, but it works
- Data Reports – Has nice tutorials – charts, data, micros
- Good messages in FBI errors
- Think the reports would appeal to the end user as they can be viewed many different ways.
- Reports are still limited.
- Would have been valuable to come to do a demo on the repository, could have answered more questions at the given time.

Vendor: Beyond 20/20

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: <i>Correctly performs validation when using the "user" login - not when using the "Admin" login</i>				
5. System provides capability for submission of NIBRS data		/		
Comments:				

B. Technical Specifications - Preferences				
<b>A. Administrators and Users</b>				
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: <i>2: do the users receive email?</i>				
<b>B. Data Entry and File Upload</b>				
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			/	
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: *victimtype=L (LEO) not in dropdown menu on the "Admin" login - The data validation when using the "Admin" login is not correct. It does seem to be correct when using the "user" login*

C. Data Reports			
1. System provides report writing capability; includes standard and ad hoc reports	1		
2. System allows data output in MS Access, Excel, Word, PDF in report & data form		1	
3. LEAs have access to other LEA data for report extraction			1
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			1
c. Offenses by location	1		
d. Arrests by Offense and Age Category <i>(Adult &amp; Juv)</i>			
e. Hate Crime			
f. Activity Log (by month or year) <i>incidents by jurisdiction</i>			
g. Outstanding Errors and Incidents/Arrests Not Checked	1		

Comments: *\* The link provided for our use did not have the reports available. Had to find it online.*

D. Data Validation and Error Notification			
1. System meets all FBI (and WA State) data validation edits and error checks			1
2. System sends electronic error reports back to submitting agency			1
3. System performs data validations/error checks before FBI file submission			1
4. Local and State SA are able to access batch error upload report	1		
5. Incidents with errors are included in the ad hoc and summary reports			1
6. The FBI error messages can be easily edited to make them user friendly			1
7. There is no Time-Window Base Date Calculation			1
8. The error list does not include errors without a case number			1

Comments:

*\* When doing the validation, if there is an error, you must go back and input the case # again to correct the error.*

*Not very user friendly.*

### Notes on Beyond 20/20 System

Reviewed test data file provided to check segment lengths:

- Level 1 (Administrative) is correct length (0088)
- Level 2 (Offense) does not include multiple bias types (0063)
- Level 3 (Property) is correct length (00307)
- Level 4 (Victim) is correct length to include LEOKA (0141)
- Level 5 (Offender) does not include offender ethnicity (0045)
- Level 6 (Arrestee) is correct length (0110)
- Level 7 (Group B Arrest) is correct length

Manual incident entry into system is not very user friendly.

If the incident has an error, you must re-enter the incident number before you can correct the problem. This is time consuming and cumbersome.

Data validations seem to be correct for the offenses

Could not generate reports from the link provided to us.

Was able to go to a public site that uses this system and create reports. The reports were easy to pull, and could be exported to Excel. However, since it was a public site, was not able to verify all the data was available to us.