

IBM Analytics



600 Anton Blvd
Costa Mesa, CA 92626

April 22, 2016

Ms. Joan L. Smith,
CJIS Manager
Washington Association of Sheriffs & Police Chiefs (WASPC)
3060 Willamette Drive NE
Lacey, WA 98516

Dear Ms. Smith,

The Washington Association of Sheriffs & Police Chiefs (WASPC) provide critical support to state-wide law enforcement agencies in an effort to enhance public safety. In furtherance of this mission, the WASPC implementation of a National Incident-Based Reporting System (NIBRS) state-level repository will greatly improve its reporting and data collection capabilities for the foreseeable future.

To satisfy your requirements, we propose IBM i2 COPLINK on the Cloud to integrate and consolidate data within a single data repository from contributing agencies. Data will be structured to support the transition to the NIBRS system. There will be a significant effort in custom development work to comply with the WASPC requirements. IBM is prepared to provide the custom development work at a significantly reduced cost in exchange with WASPC becoming a Sponsor User to assist in the WASPC COPLINK/NIBRS development and to provide a reference for future implementations in other states.

COPLINK on the Cloud takes advantage of its built-in data integration capabilities to report existing criminal history records in the NIBRS format. In addition, COPLINK can also support new NIBRS data elements through a feature known as custom attributes. COPLINK on the Cloud allows the type of flexibility and scalability that is critical for WASPC as it collects data from multiple disparate sources. The program supports batch file submissions that are automatically transformed through an ETL process that includes extensive data error checking.

There are currently fifty COPLINK systems operating within the United States, hosted in twenty-one states. As a part of this established network, IBM will extend its existing agreement with the National Law Enforcement Telecommunications System (Nlets) to allow Cloud hosting services within one of the most secure and established CJIS-compliant facilities in the nation. Nlets is a consortium located in Arizona and is governed by the fifty states providing secure law enforcement communications to individual law enforcement agencies throughout North America.

We are excited about partnering with WASPC on this project to make the most robust, secure and flexible NIBRS state-level repository. We look forward to a long term relationship in support of the NIBRS state-level repository.

Sincerely,

Maria Rogers
mariaadr@us.ibm.com/ 914-329-9411

IBM PROPOSAL TO:

Washington Association of Sheriffs & Police Chiefs (WASPC)

For National Incident-Based Reporting System (NIBRS) State
Repository Replacement | RFP CJIS-2016-01

Prepared for Washington Association of Sheriffs & Police Chiefs (WASPC)
By: David Sanborn
600 Anton Blvd.
Costa Mesa, CA 92626
Telephone: 949-355-1422
Email: dmsanborn@us.ibm.com
April 22, 2016



Table of Contents

Section 1 Proposal Executive Summary	1
Our understanding of your goals	1
Our solution	1
Our value proposition for Washington Association of Sheriffs & Police Chiefs (WASPC)	2
Section 2 Technical solution and description	3
2.1 Basic Requirements	3
2.2 Preferences	5
2.3 Add-On Components	13
Section 3 Project management description	14
3.1 Project Plan	14
3.2 Project Schedule	18
3.3 Roles and Responsibilities	20
3.4 Project Change Control	22
3.5 Testing	23
3.6 System Maintenance and Support	23
3.7 Training	24
3.8 Documentation	26
3.9 Vendor Issues and Concerns	26
Section 4 Vendor section for additional information	27
4.1 Qualifications and Experience	27
4.2 Vendor Information	27
4.3 Current Customer Base and References	28
Vendors' Section	29
Section 5 Pricing section	30
5.1 Introduction	30
5.2 Technical Section	30
5.3 Project Implementation and Management Services	30
5.4 Maintenance and Support	31
5.5 Training	31
5.6 Documentation	31
5.7 Other Costs Not Specifically Requested	31
5.8 Project Management	31
5.9 Contracts and Licenses	31
5.10 General Liability Insurance	32
Appendix A Supplemental and Collateral Material	33
Appendix B Vendor financial qualifications and annual reports	34
Five-Year Comparison of Selected Financial Data	34
Appendix C Vendor purchase contract	36
Appendix D Vendor software license agreements	37
Nondisclosure Agreement	38
Attachments	39

Figure List

Figure 1: A sample Cognos Workspace Advanced report builder	6
Figure 2: Example of COPLINK data entry capability showing drop-down pick lists and mandatory fields.	7
Figure 3: Example of COPLINK error screen.	7
Figure 4: Sample COGNOS Report	8

Section 1 Proposal Executive Summary

The Washington Association of Sheriffs & Police Chiefs is tasked with the highly technical and critical task of implementing a new NIBRS system to support multiple agencies that are submitting both NIBRS and SRS data. Upon successful implementation, the new NIBRS system will allow WASPC to provide more data-backed analysis to better inform its stakeholders within the annual *Crime in Washington* report.

Our understanding of your goals

It is our understanding that WASPC seeks to replace their existing NIBRS system with a new and improved system to enhance and improve its data collection and reporting capabilities. The solution must adhere to all data entry, capture, quality, editing, validation, submission, preservation and reporting requirements detailed by FBI NIBRS. The solution must adhere to all state-level Incident-Based Reporting (IBR) requirements. In addition, the solution must generate reports that achieve both State and FBI certification.

- Meet all FBI NIBRS technical and user guideline requirements
- Meet all State of Washington Incident-Based Reporting data collection requirements
- Generate reports that meet Washington State and FBI NIBRS certification
- Help reduce crime and increase public safety

Our solution

IBM proposes to use its existing COPLINK on Cloud system hosted within a CJIS compliant facility to ingest data from contributing agencies and consolidate information within a single data warehouse. Information within the data warehouse would be sent on a schedule determined by the WASPC for integration into the FBI NIBRS system and would comply with all state-level and FBI NIBRS technical and user guideline requirements with the aid of IBM's COGNOS reporting solution.

- Proposed solution would meet all FBI NIBRS technical and user guideline requirements
- Proposed solution would meet all State of Washington Incident-Based Reporting data collection requirements
- Enhanced mapping of threats and incidents for enhanced reporting capabilities for WASPC's annual report
- Cloud environment within a CJIS compliant facility offering a highly available, secure, flexible and scalable solution.
- User access for one concurrent user license per agency; additional concurrent licenses are available at additional cost.
- Development costs for the COPLINK/NIBRS solution are substantially reduced. We would like to engage WASPC as a Sponsor User to assist in the WASPC COPLINK/NIBRS development and to provide a reference for future implementations in other states.

Our value proposition for Washington Association of Sheriffs & Police Chiefs (WASPC)

IBM can offer WASPC a state-of-the-art solution that exceeds requirements while providing a CJIS compliant cloud platform hosted at Nlets for purposes of resiliency, scalability and flexibility as the needs of the State of Washington shift. The proposed solution is comprised of our Commercial off the Shelf (COTS) product. While custom development work is required, the existing COTS product provides approximately 80 percent of the required functionality, thus reducing the need for customization that can cause unforeseen complications and delays in deployment. IBM brings a wealth of experience gained through our fifty COPLINK implementations across the nation serving to deliver peace of mind to the WASPC and its stakeholders.

Section 2 Technical solution and description

2.2 Preferences

A. Administrators and Users

1. Local System Administrator and Users

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

Local administrators will have access privileges as defined by the system administrator(s). The COPLINK Migration reporting service has a near-real time capability of reporting data ingest errors. The migration service error messages will be sent to the specified local administrator as it is generated.

Reason for the failure of the data migration are part of the reporting service.

Duplicate files, based on agency ORI and report number, will be rejected.

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.
- 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.
- c. The SSAs must have the ability to produce standard, ad hoc, and crime mapping reports, charts, and graphs.
- 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.
- e. The SSAs must be able to manage local user accounts, including the set-up or disabling of user profiles and re-setting passwords.

The Source Reporting Service is a stand-alone application that allows a system administrator to view and control the following data migration information:

- View the refresh status of all data sources including when source records are received and processed (system journal).
- Set source refresh expiration time outs. Source refresh status is monitored by a heartbeat between each data source and the node.
- Source errors are sent to the node where they can be forwarded to the System Administrator.
- Control who is notified of status changes and how notifications are directed.
- Monitor logged in users for cloud licensing compliance.

- Monitor the COPLINK database and Search API application for availability. If unavailable, emails are sent to Cloud and Dev Operations.
- Cognos Workspace Advanced provides Ad-Hoc Query and Analysis interface for business users
- Provides a consistent, simplified, and rich interface for self-service reporting and analysis

Blurry

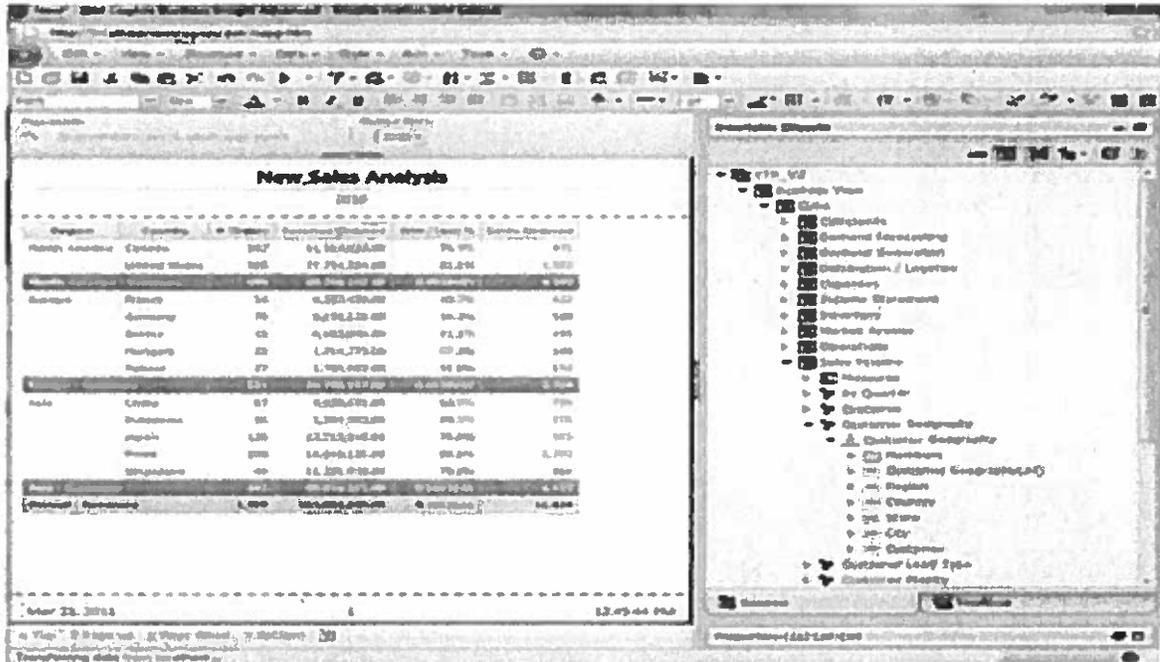


Figure 1. A sample Cognos Workspace Advanced report builder

B. Data Entry and File Upload

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

This portion of the proposed solution does not exist today would require development work by the Safer Planet Lab services unit. The proposal to meet this requirement is that we would create a distinct user interface allowing for the ingestion of the NIBRS Data into the central COPLINK Database.

- The individual incident entry (IIE) must have data validation on each data field
 - Data entry should be user friendly with drop-down tables relevant to either the incident or arrest data being entered.

IBM COPLINK makes maximum use of drop down tables to ensure consistency in data entry. The example below is the criminal intelligence data entry screen. The proposed NIBRS data entry screen would follow a similar paradigm.

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

Missing mandatory fields will generate an error in the migration reporting service. Invalid data entry will be minimized through the use drop-down tables. Mandatory fields that are not completed will not allow the user to submit the file.

- c. The mandatory fields should highlight according to the offense.
In the screen capture, the mandatory fields have a beige background.
- d. The user should not be able advance to next screen without completing mandatory fields.
Missing data will not allow the user to progress, as is shown in the error message below the data entry screen capture. The error message can be modified to reflect the specific situation.
- e. When the IIE is complete, the NIBRS check should list errors and return the user to screen and highlight the error(s)
Errors in the IIE will not allow the user to progress, so this requirement is redundant.
- f. Any field with a date entry should allow the option to type the date or use a calendar.
The COPLINK program data entry fields have this feature.
- g. It is desirable that hot keys be available to facilitate data entry.
The <TAB> key will advance the user through the data screens.

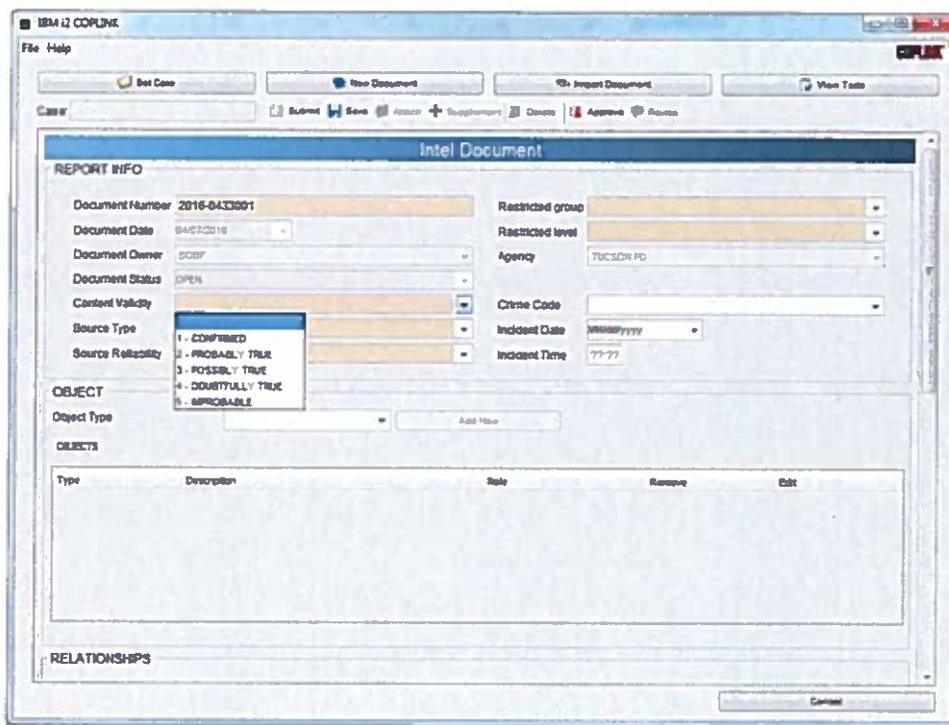


Figure 2: Example of COPLINK data entry capability showing drop-down pick lists and mandatory fields.

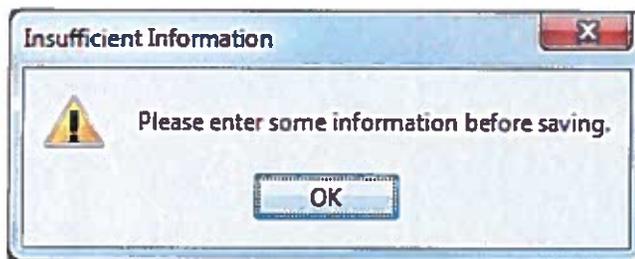


Figure 3: Example of COPLINK error screen.

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

The proposed data entry screen will follow the desired sequence.

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.

The COGNOS system provides the following

- More functionality for power users to perform analysis and exploration directly from Cognos Workspace
- One place for all reporting (OLAP, Relational, Financial)
- Bridge gap between power users and professional report authors
- Integrate external data for filtering and/or supplementary data
- Compatibility with Report Studio
- The User Interface exposes the most commonly used controls needed for building a report including business view of data, formatting objects and properties.
- The types of reports are user defined and customized to fit requirements.

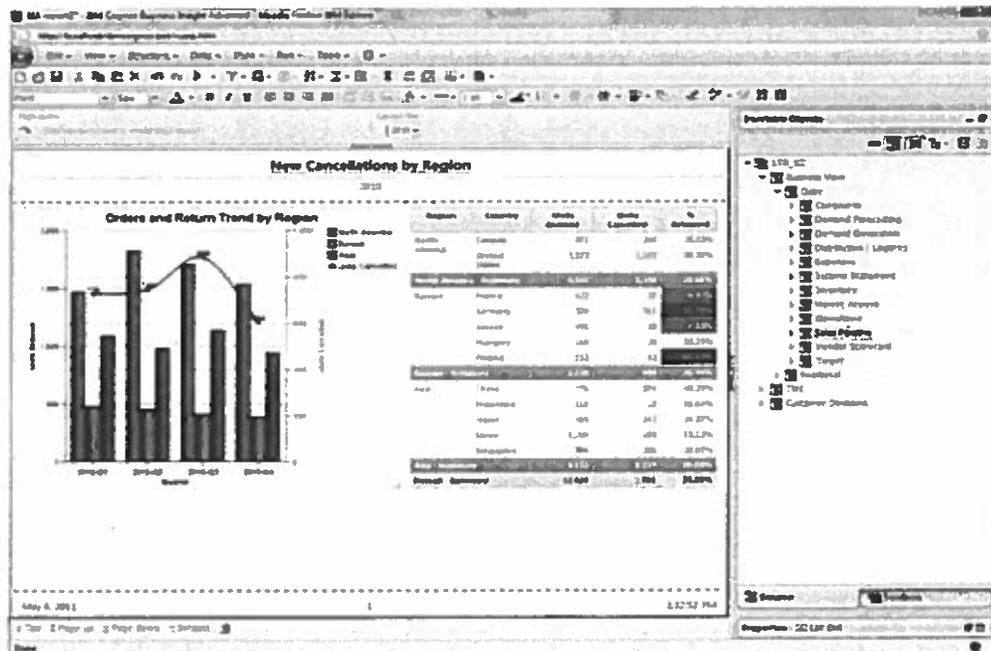


Figure 4. Sample COGNOS Report

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

COPLINK allows export as a csv file Microsoft Excel, Word, and PDF. COPLINK does not support export to Microsoft Access.

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

COPLINK provides a data repository that is searchable by all authorized users.

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

The IBM COGNOS reporting system meets all of these requirements.

D. Data Validation and Error Notification

1. The system must meet all FBI and Washington State data validation edits, perform thorough error-checking, and automatically send electronic error reports back to the submitting agency.
 - a. The State System must perform data validations and locate errors before the file goes to the FBI.

As stated previously, the data migration process used for both batch file load and manual data entry checks for errors and rejects any submissions that do not conform to the NIBRS submission standards. The Migration report service records these errors and makes them available to the system administrator.

- 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

The reporting service output can be made available to a user authorized to view the data.

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).

IBM COGNOS Workspace Advanced permits users to create custom reports. The above parameters are simply selected by the user at the time the report is built.

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

Error message format must be determined at the time the program is configured. However, requirements from WASPC will be incorporated into the error message text during development and IBM will work with WASPC to ensure the error messages are clear and user-friendly. There is no mechanism to allow user editing of the error text messages. This is done to maintain the program integrity.

4. There should not be a Time Windows error.

The program will not include a time-window error as part of the reporting service.

5. The Error Report list

- a. Should not include "outside of base date" comment (unable to correct, so don't display)
- b. Should not include errors without case number (unable to access, so don't display)

The reporting service allows filtering of messages by error code.

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).

COPLINK uses group membership to establish user profiles, which then have access as determined by the system administrators.

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

COPLINK uses group membership to establish user profiles, which then have access as determined by the system administrators.

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

The current COPLINK paradigm allows a reviewer to modify the inputted data. This will be configured to enable the SSAs to modify a record, however, the original record will be held in the repository in the event a data corruption error occurs.

4. There must be at least two (2) databases available:

- a. Training database, a duplicate of the Production database with data field descriptions available when hovering.
- b. When files, incidents, or arrests are uploaded or entered to the Training database for certification or test purposes, the SSAs should have the ability to transfer the files, incidents, or arrests to the Production database.
- c. Production database, with permanent statistical archive ability.

COPLINK currently has no capability to enable the transfer of files from the "training" database to the "production" database. This will require custom development.

F. System Features

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

The COPLINK migration process may be scheduled as desired by the State and the individual agencies. As the batch files are loaded by the user agencies to a specified folder in the COPLINK system, the migrator will load any new files on the defined schedule. This is an automated process that will ingest new records at the prescribed time and record the events in the migration reporting service.

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

Batch file submission will be loaded by user agencies to specified folder in the COPLINK system and then migrated into the database on user-defined schedule. IBM proposes to develop a data entry screen to allow data entry directly into the system with appropriate constraints and checks.

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).

If the data migrated passes all NIBRS data checks, it is immediately available in the COPLINK data repository.

4. The Domestic Violence (DV) indicator is mandatory, relevant to all offenses, and should be associated with the Victim.
 - a. It is desirable that the DV indicator default based on certain victim relationships to offender, for example, "Spouse".
 - b. If a default is triggered, a desirable feature for users would be a pop-up window asking, "Are you sure ...?"

This requirement will be addressed through a custom attribute. The default confirmation screen is a custom development and is included in the proposed system cost.

5. The Gang Involvement indicator is mandatory.

This requirement will be addressed through a custom attribute.

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.

COPLINK paradigm is that data in the repository that is migrated automatically requires a change in the data source contributing the data or an updated batch file. Direct data entry cannot be deleted, only supplemented. The program does have the ability to hide a deleted case from view using the data restriction function.

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.

This requirement will be addressed through a custom attribute.

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.

COPLINK includes a transaction log that records all of the required information.

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

This requirement will be addressed through a custom attribute.

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.

The COPLINK Migration Reporting Service meets these requirements.

11. The Zero Report function

- a. Should allow an agency to enter a Zero Report even if the file contains a correction or update from a previous month's case.
- b. Should allow an agency to override a Zero Report month if an incident is now available for that month.

This requirement will be addressed through a custom attribute.

- 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.

This would require a translation table, which COPLINK does have to convert NIBRS data to UCR data and *vice versa*, however, implementation is custom development work and it is NOT included in the system cost.

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

IBM COPLINK has four COPLINK systems that are submitting data to the FBI N-DEX system. While not NIBRS data, the similarities in error-checking and submission protocols are similar. IBM has worked closely with the FBI on this endeavor since 2010.

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

IBM will ensure that the system will be IBM submission capable. IBM has worked closely with the FBI in migrating data from local COPLINK repositories to the FBI N-DEX system and has experience with the error check required to ensure the submitted data meets the FBI requirements.

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

The COPLINK system in Kansas City (KC-ETAC) displays data in the NIBRS format. This system has been operational since 2010.

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

This requirement will be addressed through a custom attribute.

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

The IBM COPLINK database schema is proprietary intellectual property and is not disclosed except under an agreement to exchange confidential information. Sample COGNOS reports are show in the Figure 1 and Figure 4.

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

- a Customer Service includes a process for Work Order Number assignment
- b It is desirable that the State System Administrators have the ability to check the status of a work order via an on-line tracking system

Included in your IBM Subscription and Support is the ability to request support either by phone or electronically, and meets the above requirements. This is further described in Section 3.6.

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

- a The Vendor should establish a desired protocol for notification to the Vendor when there is an update of the FBI and/or State technical specifications

This would be handled by the filing of a support request and would be treated as part of our ongoing support.

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

IBM Services will schedule the installation of any new releases of upgrades or enhancements with the client.

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

The COPLINK program includes context sensitive on-line help.

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

IBM offers a number of training options that can be discussed at contract negotiation.

11. Vendors are responsible for specifying each hardware component necessary to satisfy the requirements of this RFP; however, all required hardware and system software will be procured by WASPC. Specifications are to be detailed enough to allow WASPC to provide the necessary equipment.

- a. Server storage capacity should be estimated for five years of use.
- b. The server operating system must be compatible with Windows Server 2008 or higher.
- c. The server database software must be compatible with Windows SQL Server 2010 or higher

General hardware/software requirements for the COPLINK solution are available, however, our offering presumes that WASPC will be make use of IBM's Software as a Service on the NLETS hosted cloud. Thus, WASPC need not supply or maintain hardware or third-party software.

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.

IBM COPLINK supports Microsoft Internet Explorer v.11 and above, Microsoft Edge, Google Chrome and Mozilla Firefox web browsers.

- 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.

IBM COPLINK supports Esri ArcGIS Server. Part of the data migration process is a geo-location service that provides GIS-coordinates if the submitted data contains the correct information. The program includes the COPLINK Map Analyzer, which displays the data in the repository to the user on a graphical map.

- 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.

This is an ETL process which is part of the COPLINK program solution. The cost of migrating the data from the current state repository is included in the system cost.

Section 3 Project management description

3.1 Project Plan

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

IBM project delivery methodology covers all stages of a business and technology transformation program to provide a global, integrated set of capabilities to support a complete delivery solution.

IBM has developed a comprehensive Project Management System that provides our clients with unparalleled project management services. Our well-trained, qualified professionals are equipped with integrated methods and tools, and are backed by IBM's broad knowledge and experience in delivering successful projects. Our efforts have been recognized throughout our history by industry and with awards.

Four fundamental tenets underlie IBM's approach to managing projects:

1. **Project management process** – The project team focuses on defining and planning to ensure the client understands and accepts the scope, coverage and depth of the project (see Figure 1) and its accompanying risk factors to achieve their required business objectives.
2. **Project organization and responsibilities** – Members of the project team define and agree the key project team members and their roles and responsibilities including appropriate sponsorship so that project results are met.
3. **Project phases** - Work is phased to provide the opportunity to reassess risks at key points through the project.
4. **Project management system** - A management system is established that will define and apply the appropriate governing processes for all project activities (see Figure 2).

These tenets, which require early coordination between IBM and our clients, provide the basic structure of the project and establish the roadmap for successful project completion.

To provide our teams with consistent methods for implementing project management worldwide, IBM has developed:

- Worldwide Project Management Method (WWPMM), which establishes and provides guidance on the best project management practices for Defining, Planning, Delivering, and controlling a wide variety of projects. IBM's PM Method, WWPMM now extends to support Program Management: WWPgMM.

The goal of IBM's methods is to provide proven, repeatable means of delivering solutions that ultimately result in successful projects and satisfied clients.

Projects and related activities are managed according to established project management principles, documented in the Project Management Institute's A Guide to the Project Management Body of Knowledge and incorporated in IBM's Worldwide Project Management Method (WWPMM). WWPMM is IBM's core project management method. It is the one consistent project management method for use by all project management professionals at IBM and was in response to a corporate executive direction to establish a single, common project management method for IBM projects worldwide.

WWPMM and WWPgMM describe the way projects and programs are managed in IBM. It consists of a number of interrelated components:

Practices

The project management practices group the tasks, work products and guidance needed to support a particular area of knowledge divided into 11 different subject areas.

- **Change Management:** includes the activities, work products and associated guidance required to manage the unforeseen changes that inevitably arise during the course of a project.
- **Communications Management:** includes the activities, work products and associated guidance required to:
 - Ensure the timely and appropriate collection, generation, dissemination, storage and disposition of project information.
 - Provide the critical links among people, ideas and information that are necessary for success.
- **Event Management:** includes the activities, work products and associated guidance used to resolve issues that arise during the course of the project, analyze particular situations, handle compliance incidents and manage the completion of actions.
- **Financial Management:** includes the tasks, work products and associated guidance required to effectively plan, track, and reconcile project budgets and financial information.
- **Human Resource Management:** includes the tasks, work products and associated guidance required to effectively coordinate human resources on a project, including those needed to plan, obtain, orient, assign, and release staff over the life of the project.
- **Quality Management:** includes what is required to ensure that the project satisfies the stated or implied quality criteria for which it was undertaken. It addresses quality from the perspective of both the management of the project and the products and services that are to be produced.
- **Risk Management:** includes the activities, work products and associated guidance required to identify, analyze and respond to risk throughout the life of the project.
- **Schedule Management:** defines the work (activities) that are performed to create the work products that comprise the project's scope. It also describes tracking progress against the plans to execute the work.
- **Scope Management:** includes the activities, work products, and guidance for transforming a business need into a clearly defined strategy for providing a solution which meets the business need.
- **Sponsor Agreement Management:** includes the activities, work products and associated guidance used to develop, negotiate, maintain and, finally, close the agreement with the sponsor. It also covers managing the acceptance of the deliverables, including the correction of defects.
- **Supplier Management:** includes the activities, work products and associated guidance used to acquire goods and services from outside the delivery organization.

The program management practices group the tasks, work products and guidance needed to support a particular area of knowledge divided into 4 different subject areas:

- **Benefits Management:** describes the process, activities, techniques and work products used to manage program benefits.

- **Program Governance:** describes the process, activities, techniques and work products used to establish and maintain program governance.
- **Stakeholder Engagement:** describes the process, activities, techniques and work products used to engage stakeholders, manage relationships and communication.
- **Strategy Alignment:** describes the process, activities, techniques and work products used by a program to ensure it meets the program's strategic objectives.

Activities

The project management activities arrange the tasks defined in the PM practices into a series of executable steps designed to meet particular project management goals or in response to particular project management situations.

1. **Defining:** Gain a thorough understanding of the sponsor's business needs, and outline what will be delivered to meet those needs, and an approach for how to deliver it. Also includes, defining the context and setting objectives of the project.
Initiating: Confirm the current scope and kick-off the associated work effort.
2. **Planning:** Outline plans describing the means that will be necessary to carry out an iteration, phase, sub-project or project.
3. **Starting/Developing:** Expand the project plans to an operational level and get project execution underway.
4. **Delivering:** Perform the project work, such as, refining the plan for the next set of planned work, accepting deliverables from the supplier, handing off deliverables to the sponsor, and assessing the accomplishments of the project to date.
 - **Perform Project Work:** This activity is a placeholder for the actual work to be done to deliver the project. The content for this work comes from the technical methods.
 - **Accepting Deliveries:** Receive, validate and accept deliverables from suppliers.
 - **Handling Deliveries:** Ensure that deliverables are ready, and track their release through formal acceptance.
 - **Confirming:** Assess the accomplishments of the project in regards to strategic milestones or checkpoints. Discuss with the sponsor and make any necessary adjustments or refinements to the project/program tactical plans to align with any potential adjustments in the sponsor's business or IT strategies.
 - **Monitoring:** Perform any on-going work necessary to track and report on progress, as well as make periodic updates to key measures of project health.
 - **Handling Exceptions:** The activities in this group are intended to resolve exceptions that will occur during the life of the project. These activities respond to unplanned project events, therefore cannot be scheduled in advance.
5. **Closing:** Perform the necessary tasks to properly close out a project phase or the project itself.
 - The program management activities arrange the tasks defined in the program practices into a series of executable steps designed to meet particular program management goals or in response to particular program management situations. The program management extends WWPPM activities to include.

- **Handling Transition:** This activity encompasses the development and management of a transition plan to ensure that program components are transitioned to ongoing/operational functions and/or new programs to ensure the achieved benefits continue to be realized.
- **Sustaining Benefits:** This activity monitors and provides ongoing support after transition of program components to ensure that intended benefits continue to be realized until such time as that support ends.

Work Products

Project management work products are the verifiable outcomes that are used to manage projects and programs.

- **Templates for the PM System**
- The project management system is the way in which a particular project is managed. It is documented as a collection of plans and procedures that direct all project management activity, and records that provide evidence of their implementation.

IBM uses WWPM to estimate, plan and manage application development projects. The key activities involved with this process include:

- Defining, planning and estimating each aspect of the project;
- Organizing, controlling and managing multiple types of projects (standalone, cross-functional, and matrix-based);
- Delivering projects in a common fashion across all platforms;
- Capturing, tracking and reporting performance-based information;
- Managing exceptions including risks, issues, changes and dependencies;
- Communicating, on an on-going basis, with constituencies that are involved in the project, and reporting status and issues to the client's executive management; and
- Analyzing the project after implementation to verify that standard processes have been followed and identifying process improvement activities for future projects.

These key activities are supported by tools and techniques for project planning, work plan generation, estimating costs and schedules, time tracking and status reporting.

IBM's approach also incorporates a quality and client focus, assuring that project managers deliver quality on their respective projects. IBM's approach to project management provides for the following:

- Confirming and clarifying client involvement
- Managing client expectations
- Calculating, analyzing and reporting the key performance indicators for projects
- Assuring client acceptance of deliverables
- Measuring client satisfaction
- Reporting benefits that are realized at project completion

IBM's management team is responsible to verify that any solution project follows the methodology and related processes consistently. In addition, IBM's Software Quality Assurance process verifies

that WWPMM is followed throughout the life cycle of a project through a variety of reviews appropriate to the size and complexity of the project. The work activities and products within the Execution and Control phase verify that project plans are tracked and the project status is reviewed with the appropriate project sponsors on an appropriate schedule. The use of formal status reports and meetings with the project sponsors provides for a clear understanding of the project status and the opportunity to review any required risk avoidance or remediation steps.

We work iteratively as a team until we can complete the project successfully and satisfactorily through the Closing Phase including all work products and documentation and acceptance.

Therefore, tasks and project schedule are as follows in hours and are roughly estimated at this time and will be confirmed upon negotiation and further discussion and discovery with the WASPC Project Team.

Activity	Hours
Starting/Initiating/ Planning	140 hours
Designing/ Developing	1280 hours
Testing/ UAT	200 hours
Deployment & Integration	280 hours
Training & Documentation	456 hours
Closing & Go Live	80 hours

3.2 Project Schedule

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

The Estimated Project Schedule is included in a Gantt chart below. This is estimated only, as we will need to work with WASPC in an "Initiation/Planning Phase" as described above in the Project Process and Methodology to review and confirm the requirements and scope. From there we can confirm the schedule and work breakdown tasks (WBS) and schedule accordingly.

Below provides a rough estimate of how we might proceed:

Task Mode	Task Name	Duration	Start	Finish	Predecessors
	Phase 1 - Project Initiation & Planning	21 days	Mon 6/6/16	Tue 7/5/16	
	Contract Signed	1 day	Mon 6/6/16	Tue 6/7/16	
	Client Scope Questionnaire & Sample Documentat	1 day	Tue 6/7/16	Wed 6/8/16	2
	Provide customer questionnaires regarding project requirements	1 day	Tue 6/7/16	Wed 6/8/16	
	Request sample reports	1 day	Tue 6/7/16	Wed 6/8/16	
	Request customization requirements	1 day	Tue 6/7/16	Wed 6/8/16	
	Request customer network infrastructure and connectivity information	1 day	Tue 6/7/16	Wed 6/8/16	
	Schedule Kick Off Meeting	1 day	Tue 6/7/16	Wed 6/8/16	
	Project Meeting Kickoff and Planning Session	1 day	Wed 6/8/16	Thu 6/9/16	3
	Review Architecture and Requirements - Team	3 days	Mon 6/6/16	Thu 6/9/16	
	Draft Solution Design Documentation	5 days	Thu 6/9/16	Thu 6/16/16	10
	Submit Draft Design to Client for Review and Feedb	1 day	Thu 6/16/16	Fri 6/17/16	11
	Revise and Complete Solution and Design Documentation	5 days	Fri 6/17/16	Fri 6/24/16	12
	Customer Acceptance Design Documentation	2 days	Fri 6/24/16	Tue 6/28/16	13
	Complete Project Plan & Schedule	5 days	Tue 6/28/16	Tue 7/5/16	14
	Phase 2 - Solution Build Configuration	222 days	Tue 7/5/16	Thu 5/11/17	
	COPLINK Node Deployment, Configuration and Testing	10 days	Tue 7/5/16	Tue 7/19/16	15
	Data Migrator	2 days	Tue 7/19/16	Thu 7/21/16	17
	Deploy Intel Lead	5 days	Thu 7/21/16	Thu 7/28/16	18

Task Mode	Task Name	Duration	Start	Finish	Predecessors
	Customization Development of Intel Lead/COPLINK Input Screens	60 days	Thu 7/28/16	Thu 10/20/16	19
	Integrate and Load Historical Data	15 days	Thu 10/20/16	Thu 11/10/16	20
	Batch Update Database	60 days	Thu 11/10/16	Thu 2/2/17	21
	Deploy Cognos	5 days	Thu 2/2/17	Thu 2/9/17	22
	Design Custom Reports (based on 4 complex report	30 days	Thu 2/9/17	Thu 3/23/17	23
	Model & Build Reports (based on 4 complex report	35 days	Thu 3/23/17	Thu 5/11/17	24
	Phase 3 - Testing	25 days	Thu 5/11/17	Thu 6/15/17	25
	Test COPLINK Set up & Deployment	5 days	Thu 5/11/17	Thu 5/18/17	22
	Test Intel Lead	10 days	Thu 5/11/17	Thu 5/25/17	25
	Test Cognos Reports	5 days	Thu 5/11/17	Thu 5/18/17	25
	Phase 4 - Integrate Solution Components	20 days	Thu 5/18/17	Thu 6/15/17	29
	Implement COGNOS Views in live DB	10 days	Thu 5/18/17	Thu 6/1/17	29
	Recreate the data connection within COGNOS	5 days	Thu 6/1/17	Thu 6/8/17	31
	Retest all Reports	5 days	Thu 6/8/17	Thu 6/15/17	32
	Phase 5 - Training & Documentation	41 days	Thu 6/15/17	Fri 8/11/17	33
	COPLINK Training (3 days) x 2	6 days	Thu 6/15/17	Fri 6/23/17	33
	Cognos Report Training	1 day	Thu 6/15/17	Fri 6/16/17	33
	Information Exchange; Documentation	10 days	Fri 6/23/17	Fri 7/7/17	35,36
	User Acceptance Testing (UAT) Final Test	15 days	Fri 7/7/17	Fri 7/28/17	37
	Phase 6 - Closing & Go Live	10 days	Fri 7/28/17	Fri 8/11/17	38
	Project Closing Documentation & Acceptance	10 days	Fri 7/28/17	Fri 8/11/17	38

3.3 Roles and Responsibilities

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

WASPC Personnel Role	Description	Estimate on Project
Key Business Stakeholders	Business Decision Makers – responsible to sign Contract, Purchase orders, Change Orders, assign personnel to various roles, responsible to business owners. Some of these signing authority tasks, such as Change orders may be assigned to PM, but only through effective communication plans with business owners and with effective plans in place for review.	50%
Project Manager	Project Manager is responsible for overseeing the implementation of the project from start to finish and will communicate with IBM PM throughout the project and be responsible for all communications to your business stakeholders. S/he will coordinate and facilitate all discussions, technical or otherwise.	100%
Technical Lead	Will be the lead for all technical discussion and references for any IT or technical decisions on the project.	75%
Trainers	Trainer the Trainer leaders to learn the system and then be able to teach the user community how to use system effectively after IBM deploys the system going forward.	25%
User Testers	Testers available that will work with trainers and IBM staff to learn the solution during training and then test the end-to-end solution for acceptance testing and advise any issues as well as iterative provide resolution feedback and completion.	25%
IBM Personnel Role	Description	Estimate on Project
Project Manager	Project Manager is responsible for overseeing the implementation of the project from start to finish. S/he will coordinate and facilitate all discussions, technical or otherwise. Your IBM PM will be your point of contact in all matters, and where necessary will engage other IBM resources to assist with answering questions or taking action to resolve any project issues. PM will be point of contact for all business issues for the project, including communications, invoicing, and change control and risk management throughout each phase of the project.	100%
Delivery Manager	Is an escalation resource for the project as necessary and helps to manage the technical resources for the project. The DM is an additional resource and assists the PM with any issues or requirements with team members and skills assessments to ensure the project is resourced effectively to be successful.	As required
Solution Architect	The solution architect will assist the team in ensuring the requirements are understood and defined in an effective and complete design document that is fully understood. He/she will be able to create the necessary documents that the team will need to create the solution to develop and implement the	Start 25% and as required.

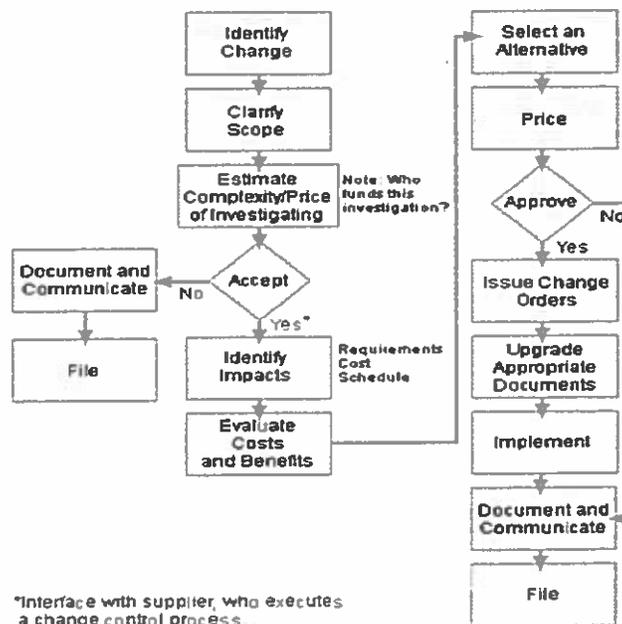
	<p>solution. This role is integral to the overall effectiveness of the solution.</p>	
<p>Technical Lead</p>	<p>A Technical Lead is a senior consultant who assists the Project Manager with technical questions. The Technical Lead for your project is also aware of any technical business rules that may apply to your project. He or she will also be intimate with every aspect of the technical solution and design and communicates with the team to ensure that any questions are addressed quickly and efficiently and can communicate these to the project manager and the stakeholders to ensure rapid risk mitigation as necessary.</p>	<p>50% of time but throughout the life cycle of the project.</p>
<p>Data Integration Analyst (DIA)</p>	<p>Each data source (RMS, CAD, Mug.) provided by your agency is assigned a Data Integration Analyst Engineer (DIA). DIA's analyze, map, and migrate an agency's data source into internal COPLINK databases for testing and verification purposes. Before inserting your data into the live environment, the DIA will also conduct thorough testing and verification of the refresh/ synchronization mechanism of your data source. All communication between the DIAE and the agency is facilitated through the Project Manager.</p> <p>There could be a number of DIA/ Consultants based on the number of integration sources on the project.</p>	<p>100%</p>
<p>Production Systems Administrator (PSA)</p>	<p>The Production Systems Administrator deploys software, and ensures that all the licenses are deployed correctly and configured on the correct machines and connected as expected. He'll work closely with your IT departments to gain access to the necessary machines, hardware or VMs to configure and deploy and connect as necessary all the various components so that the engineers can gain access to begin development. He'll assist in any configurations as necessary to ensure all configurations work as expected through test and Go Live.</p>	<p>25% Implementation and as Necessary</p>
<p>Production Support Engineer (PSE)</p>	<p>Each client is assigned a PSE Installation Engineer to assist the Agency configure network communications and installations between all the various configurations, VPN, VMs etc. This is the role of the PSE.</p>	<p>25% for Implementation Phase 3 Only</p>
<p>QA</p>	<p>Quality Assurance / Testers will work to test the mapping and integration in our internal systems prior to implementation and testing with the client system and doing any UAT. This will allow us to do some iterative testing and bug fixes internally.</p>	<p>50% on the latter half of the project.</p>
<p>Trainers</p>	<p>Trainers will be engaged to facilitate Training Classes as described in the Training Plan attached further in this document.</p>	<p>As required.</p>

3.4 Project Change Control

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

- A Project Change Request (PCR) will be the vehicle for communicating change. The PCR must describe the change, the rationale for the change and the effect the change will have on the project.
- The designated Project Manager of the requesting party will review the proposed change and determine whether to submit the request to the other party.
- Both Project Managers will review the proposed change and agree to implement it, recommend it for further investigation, or reject it.
- IBM will specify any charges for such investigation. A PCR must be signed by authorized representatives from both parties to authorize investigation of the recommended changes. IBM will invoice you for any such charges per the terms of the project and the Agreement. The investigation will determine the effect that the implementation of the PCR will have on price, schedule and other terms and conditions of the Agreement.
- A PCR must be accepted by authorized representatives from both parties to authorize implementation of any agreed changes to the SOW and the Agreement. Until a change is agreed to, both parties will continue to act in accordance with the latest agreed version of the project plan.
- A PCR that has been signed by authorized representatives from both parties constitutes a change authorization for purposes of this SOW and the Agreement.
- IBM Project Manager will keep a PCR Control Log as part of the Project Tracking and Reporting, and make updates to other affected project documents, such as the Project Plan, Requirements Document, etc., to incorporate the approved changes.

The Change Management Process



3.5 Testing

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

1. Application testing – acceptance testing of the basic functionality and operation of the application.
 - a. It is desirable that WASPC project team members have access to the software for comprehensive testing of data elements and validations during RFP evaluation

IBM has extensive quality assurance testing processes that will ensure that the program components are operating correctly. The program will operate on a hosted system (SaaS) and IBM has existing processes to manage these services.
2. Acceptance testing – Upon completion of application testing, WASPC will run system for a minimum of 60-days to ensure the system meets the functional and performance requirements stated in the RFP.

IBM will support the acceptance testing by WASPC

3. FBI re-certification.

IBM will work with WASPC to gain FBI certification.

3.6 System Maintenance and Support

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

IBM Subscription and Support includes the ability to request support either by phone or electronically. The process is governed by the IBM Passport Advantage agreement, where WASPC would name a Primary Contact, a Technical Contact and an Administrative Contact. Users who wish to contact IBM Support would simply self-nominate themselves within the system and WASPC's Contact would grant access to that individual.

The support services include a 1-800 number, electronic support, 7/24 online help and technical resource information, skilled Level 1 to 4 resources with access to development as required. When an incident is reported, a unique incident number is created and WASPC can follow the progress online through secure access provided with your IBM credentials and site information. An escalation process with access to duty managers. IBM also has a Crit/Sit process which engages executives at senior levels. For those situations declared a Severity 1, IBM provides support during business hours and non-business hours is prepared to provide weekend support assuming WASPC resources required are also available during these times. As noted in previous sections, the IBM Software Support Handbook includes details on the policies, procedures and resources available to our clients.

IBM provides an 800 # for phone support that routes customers to their product support team.

- IBM posts all user guides, troubleshooting, configuration, Readmes, release notes, etc. to the IBM Support Portal available 24/7.
- IBM utilizes Severity 1 issues via the Support Portal which comes with a guaranteed one-hour response time 24x7 – this begins the escalation process Support team to Manager to Executive should the need arise.
- The ILE and Coplink Support managers are always available to customers to assist in ensuring Support requirements are met.

- IBM Support collaborates with customers to resolve issues no matter the severity, in the event of a Sev. 1 – escalated processes engage. A severity 1 is defined as a 'system down' or 'critical function' is offline.
- IBM Services can use our monitoring program, "RAM" to monitor all Services across the solution.
- Product Support 'owns' the triage and resolution status for all issues, noted within Service Requests.
- IBM Services will schedule the installation of any new releases of upgrades or enhancements with the client.
- Product Support provides ongoing status within Severity 1 tickets as long as the effort to resolve is ongoing between IBM and the customer.
- Standard IBM Product Support operating procedure for an incident report is to issue a unique incident number and to provide authorized technical contacts with updates until the contact confirms that the incident has been resolved.

3.7 Training

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

The Train the Trainer training will be offered to selected Department users to acquire the necessary information, skills, and proficiencies of the Software Solution to allow those users to train other typical Department users how to use the Software Solution to its fullest potential.

COPLINK Train the Trainer

Overview

Duration: 3 Days

Instructor-led classroom course provides public safety instructors with the background information, instructional tools, learning activities and facilitation skills necessary to present the IBM i2 COPLINK Detect Course. Designed with the end-learner in mind, instructors who have completed this course are able to provide you with the knowledge and skills necessary to generate investigative leads using IBM i2 COPLINK Detect, as well as gain a working knowledge of how to participate in law enforcement information sharing, generate tactical leads, detect relationships among people, places, and things.

This training will assist future instructors in acquiring a working familiarity with IBM i2 COPLINK functions in relation to student duties. A high level of your participation is required. You will gain a working knowledge of how to develop teaching scenarios, utilize proper teaching methods, and work with available course resources. During training, you will develop scenarios and deliver presentations from their own data for use in IBM i2 COPLINK Detect training. You will work with both a fully functioning IBM i2 COPLINK Detect anonymized database and their client agency's live data.

General information

Delivery method: Instructor-led Classroom

Audience: This course is designed for Police Managers, Police Supervisors, Investigators, Officers, Training Officers, Records Managers, and Communications Personnel responsible for training end users in the use of IBM i2 COPLINK Detect.

Topics: During the course the following topics will be covered:

- IBM i2 COPLINK Detect Administration
- IBM i2 COPLINK Detect User Interface and Functionality
- IBM i2 COPLINK Detect Scenario Development
- IBM i2 COPLINK Detect Course Facilitation Techniques

Learning objectives: After completing this course, students should be able to:

- Understand the principles of information sharing and the normalization of records data.
- Discuss the basic functions of IBM i2 COPLINK Detect.
- Explain the function of each of the IBM i2 COPLINK Detect add on components.
- Understand how IBM i2 COPLINK Detect is deployed.
- Access the application, change user settings, and set query preferences.
- Navigate the Graphical User Interface and understand screen structure.
- Construct and initiate basic queries.
- Construct and initiate basic and refined association searches.
- Have a working knowledge of the IBM i2 COPLINK Detect add-on modules Incident Analyzer, Active Agent, and Visualizer.
- Instruct users on the function of IBM i2 COPLINK Detect and add on modules Incident Analyzer, Active Agent, Administration and Visualizer.
- Design, develop, and present IBM i2 COPLINK scenarios and learning activities.

Prerequisites: Before taking this course, students should have a basic knowledge of:

- Basic computing concepts.
- Procedures for the management and handling of sensitive materials.
- Police regulations and investigative procedures.

Duration: 3 days

Skill level: Advanced

Overview of IBM COGNOS Business Intelligence

Recommended duration: 1 Day or 8 Hours

Overview of IBM Cognos BI (V10.2.2) provides participants with a high level overview of the IBM Cognos BI suite of products and their underlying architecture. Participants will examine each BI component as it relates to the comprehensive Smarter Analytics solution, and will be shown a range of resources to access additional information on each product.

3.8 Documentation

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

Both IBM program components have extensive help files and documentation that covers the functionality of the programs.

3.9 Vendor Issues and Concerns

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

Not Applicable

Section 4 Vendor section for additional information

This section asks you to provide information about your company to us. Please adhere to the following format in responding:

4.1 Qualifications and Experience

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

Please visit the following website for the IBM Annual Report and financial information:
<http://www.ibm.com/annualreport/>

4.2 Vendor Information

1. Full legal name

International Business Machines Corporation (IBM)

2. Year started

Incorporated: June 16, 1911

3. State and location of headquarters

1 New Orchard Road
Armonk, NY 10504-1722

4. Tax identification number

IBM Federal Employer ID and Tax Payer ID Number is 13-0871985.

5. Brief history

IBM History

International Business Machines Corporation (IBM), incorporated in the State of New York on June 16, 1911, is a widely held, publicly traded company listed on the New York Stock Exchange. Originally called the Computing Tabulating Recording Company (C-T-R), manufacturing products ranging from commercial scales and industrial time recording equipment to tabulators and punched cards, it was renamed International Business Machines Corporation on February 14, 1924.

6. Current number of employees

IBM is one of the world's largest information technology companies operating in more than 175 countries with approximately 380,000 employees in 2015. IBM releases employee data in its Annual Report and considers further detail of its personnel resources data proprietary and confidential.

7. Type of entity

IBM is a publicly traded corporation.

3. Disclose if your company is aware of any potential claims, investigation, or is involved in any disputes or litigation where an adverse decision may result in a material change to Vendor's financial position or future viability.

IBM does not make the details of past, pending or current litigation publicly available. However, IBM represents that there is no pending litigation that would prevent IBM from discharging its obligations under a contract finally awarded to IBM, including all obligations related to the provisions of IBM Products and Services thereunder. Information that does exist is in Form 10-K, Part I, Item 3 - Legal Proceedings in the annual report filed with the Securities and Exchange Commission. Please refer to the following website for more information:
www.ibm.com/annualreport.

9. Disclose if your company has ever filed for bankruptcy protection, reorganization, or had a receiver appointed for it.

IBM has not filed for bankruptcy.

10. Audited Vendor financial data for the last three years (use appendices).

Please see Appendix B.

11. Most recent annual report, if public (use appendices).

Please visit the following website for the IBM Annual Report and financial information:
<http://www.ibm.com/annualreport/>

4.3 Current Customer Base and References

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

Please see table below.

2. Vendors shall provide at least two reference agencies where the Vendor's NIBRS repositories are installed. WASPC will contact these agencies regarding Vendor's technical capabilities, project management skills, and ongoing support after installation. A reference may be chosen for a site visit by our evaluation team. To warrant consideration for this contract, Vendors must successfully pass reference checks. The reference account information must be given in the format listed below:

IBM COPLINK does not have experience in extracting data for submission to the FBI NIBRS system. We have extensive experience in managing criminal justice information and our current customers have over 1.5 billion sharable documents housed in various COPLINK systems in 22 states. Our COPLINK database can support NIBRS data elements with no customization required. Our Software as a Service offering is hosted by Nlets in a CJIS compliant secure environment and is a fully managed solution, relieving WASPC of any hardware and support costs. We believe our 20 plus years of experience dealing with a wide variety of law enforcement data makes IBM eminently qualified to bid on this proposed solution.

- A. Agency name
- B. Street address, city, zip code
- C. Contact name
- D. Contact telephone number.
- E. Contact e-mail address

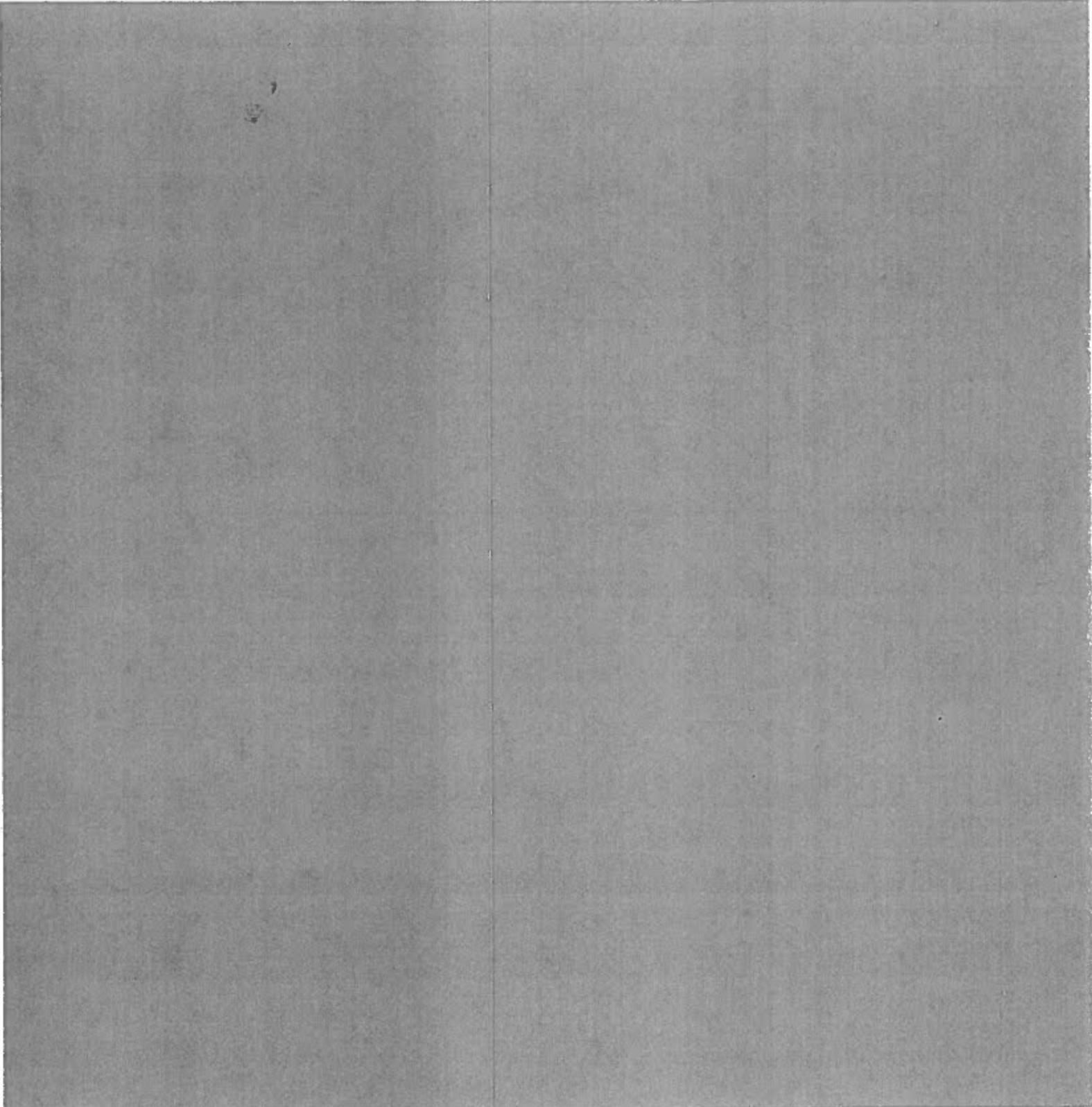
- F. Summary of project
- G. Number of users
- H. Date system implementation started
- I. Date system was certified by FBI (N/A if not certified)
- J. Approximate cost.

Agency Name	Street address/city/zip code	Contact name	Contact telephone number	Contact e-mail address	Summary of project	Number of users.	Date system implementation started	Date system was certified by FBI (N/A if not certified)	Approximate cost
Jefferson Parish Sheriff's Department	1233 Westbank Expy Bldg B 5th Fl, Harvey, LA 70058	Darla Margiolta	504-363-5730	margiolta_dc@psd.com	Integration of seven separate law enforcement agency data systems in the greater New Orleans metropolitan area.	3,215 users	December 2009	N/A	IBM cannot share this confidential customer information due to our Business Conduct Guidelines.
Massachusetts State Police	124 Acton Street, Maynard, MA 01754	Lt. Col. Dermot Quinn	978-451-3751	dermot.quinn@state.ma.us	Integration of 45 Massachusetts law enforcement agencies into a COPLINK data repository.	5,545 authorized users	April 2005	N/A	IBM cannot share this confidential customer information due to our Business Conduct Guidelines.
Spokane Police Department	1100 W Mallon Ave, Spokane WA 99260	Richard Cain	509-625-4197	rcain@spokanepolice.org	Integration of six law enforcement agencies in the Spokane metro area. System in addition has Idaho agencies contributing data.	660 users	2004	N/A	IBM cannot share this confidential customer information due to our Business Conduct Guidelines.

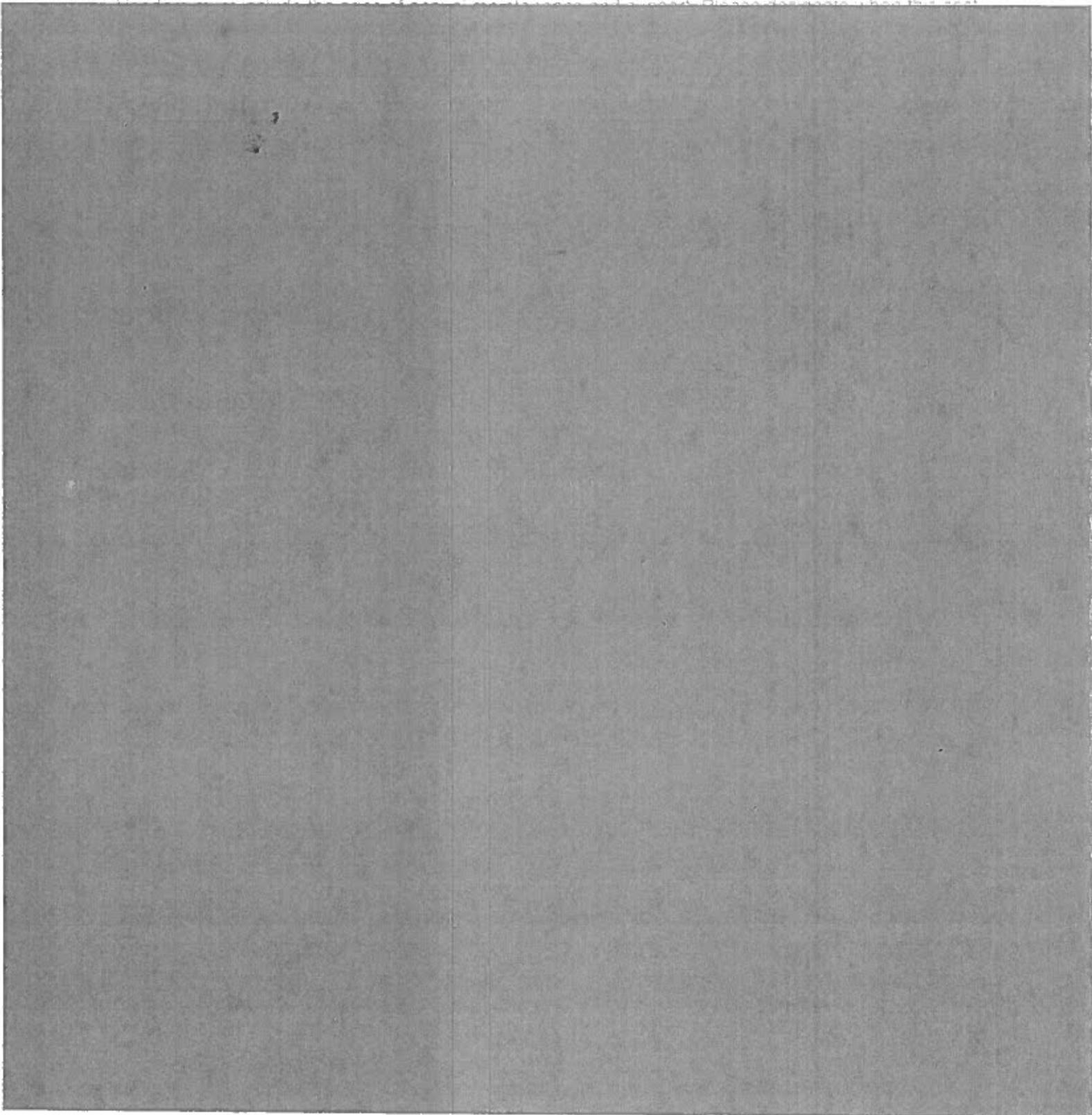
Vendors' Section

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

Section 5 Pricing section



5.4 Maintenance and Support



5.10 General Liability Insurance

The Vendor must secure and maintain insurance and bond coverage acceptable to WASPC. The insurance must be issued by companies, which are duly licensed, admitted, with a Best rating of 'A' and authorized to do business in the state of Washington and Vendor must provide the necessary evidence to substantiate these criteria. Copies of the requisite proof of coverage must be provided to WASPC within five (5) business days after contract execution and must remain in force during the life of the Contract. The proof of insurance must reflect whether the required limits of liability will be offset by prior claim payments, provide evidence that the proper endorsements have been issued to the policy, and provide that the insurance carrier must notify WASPC upon the policy's cancellation or material changes.

Notwithstanding any other requirement of this Section, WASPC reserves the right to consider reasonable alternative methods of insuring the Contract in lieu of the above-stated general liability insurance. Respondent has sole responsibility for recommending to WASPC alternative methods of insuring the Contract. Any alternatives proposed by a respondent must be accompanied by a detailed explanation regarding respondent's inability to obtain insurance coverage as described above. WASPC reserves the right, in its sole discretion, to determine the adequacy of any substitute form of insurance coverage.

WASPC shall be named as an Additional Insured in each required insurance contract. The required insurance contract must remain in effect throughout the term of the Contract. Work under the Contract will not begin until after Vendor has submitted, in a timely manner, evidence of the required insurance coverage in a form acceptable to WASPC. Notwithstanding any other provision of this RFP, failure to timely submit acceptable evidence of the required coverage may be considered a breach of the Contract, in which case WASPC may avail itself of all remedies in equity or at law for such breach. Without limitation on the foregoing, upon failure to submit the insurance contract on a timely basis, WASPC reserves the right, in its sole discretion, to immediately revoke the award.

IBM maintains a corporate Global Risk and Insurance Management program that is designed protect IBM against losses wherever IBM does business throughout the world. We are confident that we can meet requirements for insurance coverage which are acceptable to WASPC.

Appendix A Supplemental and Collateral Material

N/A

Appendix B Vendor financial qualifications and annual reports

Five-Year Comparison of Selected Financial Data

Five-Year Comparison of Selected Financial Data					
International Business Machines Corporation and Subsidiary Companies					
(Dollars in millions except per share amounts)					
For the year ended December 31:	2015	2014	2013	2012	2011
Revenue	\$ 81,741	\$ 92,793	\$ 98,367	\$102,874	\$105,056
Income from continuing operations	\$ 13,364	15,751	16,881	16,999	16,108
Loss from discontinued operations, net of tax	\$ (174)	(3,729)	(398)	(395)	(253)
Net income	\$ 13,190	12,022	16,483	16,604	15,855
Operating (non-GAAP) earnings*	\$ 14,659	16,702	18,356	18,022	16,571
Earnings/(loss) per share of common stock:					
Assuming dilution					
Continuing operations	\$ 13.60	15.59	15.30	14.71	13.27
Discontinued operations	\$ (0.18)	(3.69)	(0.36)	(0.34)	(0.21)
Total	\$ 13.42	\$ 11.90	\$ 14.94	\$ 14.37	\$ 13.06
Basic:					
Continuing operations	\$ 13.66	15.68	15.42	14.88	13.46
Discontinued operations	\$ (0.18)	(3.71)	(0.36)	(0.35)	(0.21)
Total	\$ 13.48	\$ 11.97	\$ 15.06	\$ 14.53	\$ 13.25
Diluted operating (non-GAAP)*	\$ 14.92	16.53	16.64	15.60	13.65
Cash dividends paid on common stock	\$ 4,897	4,265	4,058	3,773	3,473
Per share of common stock	5.00	4.25	3.70	3.30	2.90
Investment in property, plant and equipment	\$ 3,579	3,740	3,623	4,082	4,108
Return on IBM stockholders' equity	101.1%	72.5%	83.8%	81.6%	71.2%
AT DECEMBER 31:	2015	2014	2013	2012	2011
Total assets	\$110,495	\$117,271* * +	\$125,641** +	\$119,213	\$116,128** +

Net investment in property, plant, and equipment	\$ 10,727	10,771	13,821	13,996	13,883
Working capital	\$ 8,235	7,797**	9,610**	5,807	7,347**
Total debt	\$ 39,890	\$ 40,722+	\$39,637+	\$33,269	\$31,265+
Total equity	\$ 14,424	\$ 12,014	\$ 22,929	\$18,984	\$20,236

* Refer to the "GAAP Reconciliation," on pages 63 and 151 of the company's 2014 Annual Report for the reconciliation of non-GAAP financial information for 2012 and 2011, respectively. Also see "GAAP Reconciliation," on pages 41 and 59 for the reconciliation of non-GAAP financial information for 2015, 2014 and 2013.

** Reclassified to reflect adoption of the FASB guidance on deferred taxes in consolidated financial statements. Refer to note B, "Accounting Changes," for additional information.

+ Reclassified to reflect adoption of the FASB guidance on debt issuance costs in consolidated financial statements. Refer to note B, "Accounting Changes," for additional information.

Appendix C Vendor purchase contract

IBM's Services are offered under the terms and conditions of the IBM Client Relationship Agreement (CRA).

[IBM Rationale: The CRA:

- Enables a client to acquire hardware, software, and services from IBM under a concise set of base terms and conditions.
- Is an ongoing relationship agreement (that remains in place until terminated by either party) for use on this and future projects, enabling WASPC and IBM to do business together more easily.]

Appendix D Vendor software license agreements

WASPC is an existing IBM Passport Advantage customer. As such, the software license agreements under the Passport Advantage program govern the acquisition and use of the licensed software. The attached document is the base ILPA.

Nondisclosure Agreement

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

- Please note that changes were made within this NDA by IBM Legal Team

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

1. The Confidential Information may only be used by Vendor to assist Vendor in its Contract with WASPC
2. Vendor will not, at any time, use the Confidential Information in any fashion, form, or manner except in its capacity as a Vendor to WASPC.
3. Any exchange of Confidential Information shall be handled under the terms and conditions of the IBM Agreement for Exchange of Confidential Information (AECI), a copy of which is attached below.

[IBM Rationale: The AECI is a bilateral confidentiality agreement that allows either party to disclose confidential information. It is an ongoing relationship agreement, so the AECI remains in place until terminated by either party, allowing WASPC and IBM to do business together more easily on this and future projects.]

By:



Title Director, IBM Safer Planet

Date 4/22/2016



Attachments

Please see attachments:

- Agreement for Exchange of Confidential Information
- Client Relationship Agreement
- International Passport Advantage Agreement



© International Business Machines Corporation 2016

All Rights Reserved

IBM Corporation

Unless otherwise provided by law, the information in this proposal shall not be duplicated, used or disclosed in whole or in part for any purpose other than to evaluate the proposal, provided that if a contract is awarded to IBM as a result of or in connection with the submission of this proposal, Washington Association of Sheriffs & Police Chiefs (WASPC) shall have the right to duplicate, use or disclose the information to the extent provided in the contract. This restriction does not limit the right of WASPC to use information contained in the proposal if it is obtained from another source without restriction.

Please note that:

- IBM's proposal is valid for 120 days, unless extended in writing by IBM*
- IBM's proposal is offered solely under the terms and conditions shown in Appendix C, Appendix C, and the Nondisclosure Agreement section above.*
- The terms "partner", "partnership", "partnering" and similar terms as used herein are intended to convey a spirit in which the parties seek mutual benefit, and do not mean a legal relationship of any type, or any responsibility by one party for the other's acts, omissions or liabilities. Any legal relationship between the parties regarding the subject matter of this proposal will exist solely as a result of contractual arrangement, if any, that may be agreed upon by the parties in connection with such subject matter.*
- "Ensure", whether capitalized or not, shall mean to use reasonable efforts designed/intended to ensure.*
- Should IBM be selected as the Apparent Successful Bidder, IBM looks forward to working closely with the State to promptly finalize a contract that is mutually agreeable to the State and IBM, utilizing the results of the Sample Contract terms negotiation.*

The IBM home page can be found at: <http://www.ibm.com>

Agreement for Exchange of Confidential Information



This Agreement protects confidential information (Information) while maintaining each party's ability to conduct its respective business activities. The following terms apply when one party (Discloser) discloses Information to the other (Recipient).

Disclosure

Information disclosed orally or not marked with a restrictive legend must be identified as confidential at the time of disclosure. Each disclosure of Information is subject to this Agreement for five years following the initial date of disclosure.

Obligations

Recipient will use Information only for the purpose for which it was disclosed or for the benefit of Discloser, and will use reasonable care to avoid disclosure of the Information other than to Recipient's:

- a) employees and employees of any legal entity that it controls, controls it, or with which it is under common control, who have a need to know. Control means to own or control, directly or indirectly, over 50% of voting shares; or
- b) subcontractors, financial and legal advisors, and then only to those who have a need to know.

Before disclosure to any party in (a) or (b), Recipient will have a written agreement with such party sufficient to require that party to treat Information substantially the same as described in this Agreement.

If required to disclose Information by law or court order, Recipient will endeavor to give Discloser prompt notice to allow Discloser a reasonable opportunity to obtain a protective order.

Disclaimers

Discloser provides Information without warranties of any kind and is not liable for any damages arising out of Recipient's use of Information disclosed under this Agreement.

This Agreement does not require either party to disclose or to receive Information, perform any work, or enter into any license, business engagement or other agreement. Neither this Agreement nor any disclosure of Information under it creates any joint or fiduciary relationship or grants Recipient any right or license under any trademark, copyright or patent, now or subsequently owned or controlled by Discloser.

The receipt of Information under this Agreement does not preclude Recipient from:

1. developing, manufacturing, marketing or providing products or services which may be competitive with products or services of Discloser, or entering into any business relationship with any other party; or
2. assigning its employees in any way it may choose.

Any Information is subject to change or withdrawal without notice.

Recipient may disclose, disseminate, and use Information that is already in its possession without obligation of confidentiality, developed independently, obtained from a source other than Discloser without obligation of confidentiality, publicly available when received or subsequently becomes publicly available through no fault of the Recipient, or disclosed by Discloser to another without obligation of confidentiality.

General

Assignment. Neither party may assign, or otherwise transfer, its rights or delegate its duties or obligations under this Agreement without prior written consent of the other except as part of the divestiture of a business line where the acquirer agrees to be bound by the terms of this Agreement. Any attempt to do so is void.

Termination. Either party may terminate this Agreement by providing at least one month's written notice to the other. Any terms of this Agreement which by their nature extend beyond its termination remain in effect until fulfilled, and apply to respective successors and assignees.

Modification. Only a written agreement signed by both parties can modify this Agreement.

Choice of Law. Both parties agree to the application of the laws of the State of New York to govern, interpret, and enforce all of the parties' respective rights, duties, and obligations arising from, or relating to, the subject of this Agreement, without regard to conflict of law principles.

Import/Export Compliance. Each party will comply with all applicable export and import laws and associated embargo and economic sanction regulations, including those of the United States.

This Agreement, including any applicable supplements, is the complete agreement regarding the exchange of Information, and replaces all prior oral or written communications, representations, warranties, covenants, and commitments between Company and IBM regarding the exchange of Information. Each party accepts the terms of this Agreement by signing this Agreement (or another document that incorporates it by reference) by hand or electronically. Once signed, any reproduction of this Agreement or a supplement made by reliable means is considered an original.

Agreed to:

<Company Full Legal Name> ("Company")

By _____

Authorized Signature

Name (type or print):

Date:

Identification number:

Address:

Agreed to:

International Business Machines Corporation ("IBM")

By _____

Authorized Signature

Name (type or print):

Date:

Agreement number:

IBM address:

International Passport Advantage Agreement

Under this Agreement, Client may order Eligible Products (EPs) from IBM. Details regarding EPs are provided in Attachments, Service Descriptions, Terms of Use and Transaction Documents, collectively TDs. This Agreement and applicable TDs are the complete agreement regarding transactions by which Client acquires EPs. Client Originating Company (also identified as the Originating Site in the Passport Advantage Enrollment Form) and the IBM Originating Company that accepts the Client Originating Company's orders agree to coordinate the administration of this Agreement within their respective Enterprises, which includes the set of legal entities that, by more than 50%, owns, are owned by, or are under common ownership with the Originating Company. The Client Originating Company is responsible for compliance with the terms for all Client sites assigned a Passport Advantage Site Number (Site(s)) under this Agreement. If there is a conflict, a TD prevails over the terms of this Agreement.

1. General

1.1 Acceptance of Terms

The Client Originating Company and thereafter each of its participating Enterprise companies accept this Agreement by submitting an IBM International Passport Advantage Enrollment Form to IBM or Client's chosen reseller(s). This Agreement is effective on the date IBM accepts the initial order under this Agreement (the Effective Date) and remains in effect until the Client Originating Company or the IBM Originating Company terminates it under this Agreement.

An EP is subject to this Agreement when IBM accepts Client's order by i) sending an invoice or a Proof of Entitlement (PoE) including the level of authorized use, ii) making the Program or IBM SaaS available, iii) shipping the Appliance, or iv) providing the support, service, or solution.

1.2 Changes to Agreement Terms

Because this Agreement may apply to many future orders, IBM reserves the right to modify it by providing Client at least three months' written notice. Changes are not retroactive; they apply, as of the effective date, only to new orders and renewals. Client accepts changes by placing new orders after the change effective date or allowing transactions to renew after receipt of the change notice. Except as otherwise provided in this Agreement, all changes must be in writing, signed by both parties.

1.3 Payment and Taxes

Client agrees to pay all applicable charges specified by IBM, charges for use in excess of authorizations, any customs or other duty, tax, levy, or fee imposed by any authority resulting from Client's acquisitions under this Agreement, and any late payment fees. Amounts are due upon receipt of the invoice and payable within 30 days of the invoice date to an account specified by IBM. Prepaid services must be used within the applicable period. IBM does not give credits or refunds for any prepaid, one-time charges, or other charges already due or paid.

Client agrees to: i) pay withholding tax directly to the appropriate government entity where required by law; ii) furnish a tax certificate evidencing such payment to IBM; iii) pay IBM only the net proceeds after tax; and iv) fully cooperate with IBM in seeking a waiver or reduction of such taxes and promptly complete and file all relevant documents.

1.4 IBM Business Partners and Resellers

IBM Business Partners and resellers are independent from IBM and unilaterally determine their prices and terms. IBM is not responsible for their actions, omissions, statements, or offerings.

1.5 Liability and Indemnity

IBM's entire liability for all claims related to this Agreement will not exceed any actual direct damages incurred by Client up to the amounts paid (if recurring charges, up to 12 months' charges apply) for the product or service that is the subject of the claim, regardless of the basis of the claim. This limit applies collectively to IBM, its subsidiaries, contractors, and suppliers. IBM will not be liable for special, incidental, exemplary, indirect, or economic consequential damages, or lost profits, business, revenue, goodwill, or anticipated savings.

The following amounts, if a party is legally liable for them, are not subject to the above cap: i) third party payments referred to in the paragraph below; ii) damages for body injury (including death); and iii) damages to real property and tangible personal property; and iv) damages that cannot be limited under applicable law.

If a third party asserts a claim against Client that an IBM Product acquired under this Agreement infringes a patent or copyright, IBM will defend Client against that claim and pay amounts finally awarded by a court against Client or included in a settlement approved by IBM, provided that Client promptly (i) notifies IBM in writing of the claim, (ii) supplies information requested by IBM, and (iii) allows IBM to control, and reasonably cooperates in, the defense and settlement, including mitigation efforts.

IBM has no responsibility for claims based, in whole or part, on Non-IBM Products, items not provided by IBM, or any violation of law or third party rights caused by Client's content, materials, designs, specifications, or use of a non-current version or release of an IBM Product when an infringement claim could have been avoided by using a current version or release. Each Non-IBM Program is governed by the terms of the third party end user license agreement that accompanies it. IBM is not a party to the third party end user license agreement and assumes no obligations under it.

1.6 General Principles

Parties will not disclose confidential information without a separate, signed confidentiality agreement. If confidential information is exchanged, the confidentiality agreement is incorporated into, and subject to, this Agreement.

IBM is an independent contractor, not Client's agent, joint venturer, partner, or fiduciary, and does not undertake to perform any of Client's regulatory obligations, or assume any responsibility for Client's business or operations. Each party determines the assignment of its personnel and contractors, their direction, control, and compensation.

Client is responsible for obtaining all necessary permissions to use, provide, store and process content in any services, maintenance, or support, and grants IBM permission to do the same. Some of Client's content may be subject to governmental regulation or may require security measures beyond those specified by IBM for an offering. Client will not input or provide such content unless IBM has first agreed in writing to implement additional required security measures.

Client is responsible to pay communications charges associated with accessing SaaS, Appliance Services, IBM Software Subscription and Support, and Select Support unless IBM specifies otherwise in writing.

IBM and its subcontractors may process the business contact information of Client, its employees and contractors worldwide for our business relationship, and Client has obtained the necessary consents. IBM will comply with requests to access, update, or delete such contact information. IBM may use personnel and resources in locations worldwide and third party suppliers to support the delivery of products and services.

Neither party may assign this Agreement, in whole or in part, without the prior written consent of the other. EPs are for use within Client's Enterprise only, and may not be assigned, resold, rented, leased, or transferred to third parties. Any attempt to do so is void. Lease-back financing of Appliances is permitted. Assignment of IBM rights to receive payments and by IBM in conjunction with the sale of the portion of IBM's business that includes the product or service is not restricted.

All notices under this Agreement must be in writing and sent to the address below, unless a party designates in writing a different address. The parties consent to use electronic means and facsimile transmissions for communications as a signed writing. Any reproduction of this Agreement made by reliable means is considered an original. This Agreement supersedes any course of dealing, discussions or representations between the parties.

No right or cause of action for any third party is created by this Agreement or any transaction under it. Neither party will bring a legal action arising out of or related to this Agreement more than two years after the cause of action arose. Neither party is responsible for failure to fulfill its non-monetary obligations due to causes beyond its control. Each party will allow the other reasonable opportunity to comply before it claims the other has not met its obligations. Where approval, acceptance, consent, access, cooperation or similar action by either party is required, such action will not be unreasonably delayed or withheld.

1.7 Governing Laws and Geographic Scope

Each party is responsible for complying with: i) laws and regulations applicable to its business and content, and ii) import, export and economic sanction laws and regulations, including those of the United States that prohibit or restrict the export, re-export, or transfer of products, technology, services or data, directly or indirectly, to or for certain countries, end uses or end users. Client is responsible for its use of IBM and Non-IBM Products.

Both parties agree to the application of the laws of the country where the transaction is performed (or for services, the laws of the country of Client's business address) to this Agreement, without regard to conflict of law principles. The rights and obligations of each party are valid only in the country where the transaction is performed or, if IBM agrees, the country where the product is placed in productive use, except all licenses are valid as specifically granted. If any provision is invalid or unenforceable, the remaining provisions remain in full force and effect. Nothing in this Agreement affects statutory rights of consumers that cannot be waived or limited by contract. The United Nations Convention on Contracts for the International Sale of Goods does not apply to transactions under this Agreement.

1.8 Agreement Termination

After expiration or termination of its obligations under this Agreement, the Client Originating Company may terminate this Agreement without cause on one month's notice to the IBM Originating Company, and the IBM Originating Company may terminate this Agreement on three months' notice to the Customer Originating Company.

If Client acquired or renewed IBM Software Subscription and Support, Selected Support, IBM SaaS, or if Client acquired or renewed a Program's license prior to the notice of termination, IBM may either continue to provide such services or allow Client to use the Program for the remainder of the current term(s), or give Client a prorated refund.

The Client Originating Company will be considered to have terminated this Agreement if neither it nor any of its participating Enterprise companies have placed orders for EPs for 24 consecutive months nor have Software Subscription and Support or Selected Support in effect, nor have any outstanding quotes for EPs.

Either of us may terminate this Agreement if the other does not comply with any of its terms, provided the one not complying is given written notice and reasonable time to comply.

Client agrees to promptly discontinue use of and destroy all of Client's copies of a Program upon termination of a license grant.

Any terms that by their nature extend beyond termination remain in effect until fulfilled, and apply to respective successors and assignees.

1.9 Eligible Products

IBM determines EPs, and assigns each EP a point value. IBM can add or withdraw EPs (including in CEO Product Categories), change PA point values, or add or withdraw a license metric for an EP at any time. EPs may not be used to provide commercial hosting or other commercial information technology services to third parties.

For an EP, IBM may withdraw a Fixed Term license, IBM Software Subscription and Support, and Select Support, Monthly Licensing (ML) in its entirety, or a SaaS or an Appliance Service in its entirety (collectively Options) on 12 months' written notice to all then current Clients by published announcement, letter, or e-mail.

If IBM withdraws an Option, Client understands that as of the effective date of such withdrawal, Client may not increase its level of use beyond the authorizations already acquired without IBM's written consent, renew or purchase that Option; and if Client renewed the Option prior to the notice of withdrawal, Client may either (a) continue to use/receive that Option until the end of the then current term or (b) obtain a prorated refund.

1.10 Renewal

The term for a Fixed Term License, Token License, IBM Software Subscription and Support, Selected Support or Appliance Services automatically renews at then current charges, unless Client provides written notice of termination prior to expiration of the term.

IBM may pro-rate charges for IBM Software Subscription and Support, Selected Support, Fixed Term Licenses of six months or more, and Appliance Services to align with Client's PA Anniversary.

To reinstate any expired Software Subscription and Support coverage, Selected Support, a Fixed Term License or Appliance Services, Client may not renew and must acquire Software Subscription and Support Reinstatement, Selected Support Reinstatement, Appliance Services Reinstatement or a new initial Fixed Term License.

For an ML, Client selects a renewal option at the time of order.

1.11 Relationship Suggested Volume Price (RSVP) Level and Suggested Volume Pricing (SVP)

An RSVP level is determined by aggregating points for all EPs ordered during Client's Term (described below). The point value of Client's initial EP order determines Client's initial RSVP level. Client may attain a higher RSVP Level by placing additional EP orders. The higher RSVP level will apply to orders placed after the higher RSVP level is attained. An SVP level is also calculated for each order, and is based on the point value for that order. If the SVP level for a particular order is higher than Client's current RSVP level, the SVP level will apply to that order.

The initial Term commences with Client's first order after enrollment and continues until the last day of the twelfth full month thereafter (i.e., the initial PA term includes 12 full months, plus if the order was not placed on the first day of a month, the remainder of the first month). On the first day of the month following the end of the prior Term (the Anniversary), the next 12 month Term begins. For each Term after the initial Term, Client's RSVP Level is reset on the Anniversary, based on EP acquired by all participating Client Sites during the prior Term. The RSVP Level for a new Term will not be lowered by more than one level below Client's RSVP level at the end of the prior Term.

RSVP/SVP Level Table:

RSVP/SVP Level	BL	D	E	F	G	H
Points	<500	500	1,000	2,500	5,000	10,000

1.12 Compliance Verification

Client will i) maintain, and provide upon request, records and system tools output, and access to Client's premises, as reasonably necessary for IBM and its independent auditor to verify Client's compliance with this Agreement, including Machine Code and Program licenses and metrics, such as sub-capacity usage, and ii) promptly order any required entitlements and pay additional charges at IBM's then current rates, (including uses in excess of Client's authorizations or entitlements, and associated IBM Subscription and Support and Selected Support), and other liabilities determined as a result of such verification. These compliance verification obligations remain in effect during the term of this Agreement and for two years thereafter. Client is responsible for retaining adequate records. If Client's records are inadequate to determine IBM Subscription and Support or Selected Support charges, IBM's charges for any excess usage will include two years of associated maintenance and IBM Subscription and Support or Selected Support.

1.13 Programs in a Virtualization Environment (Sub-Capacity Licensing Terms)

EPs that meet the operating system, processor technology, and virtualization environment requirements for sub-capacity usage may be licensed based on processor value units (PVUs) under Sub-Capacity Licensing terms (an Eligible Sub-Capacity Product) <http://www-01.ibm.com/software/passportadvantage/subcaplicensing.html>. Product deployments that cannot meet Sub-Capacity Licensing requirements must be licensed using Full Capacity terms.

PVU based licenses for Eligible Sub-Capacity Products must be acquired for the total number of PVUs associated with the virtualization capacity available to the Eligible Sub-Capacity Product as measured at <https://www-112.ibm.com/software/howtobuy/passportadvantage/valueunitcalculator/vucalc.wss>.

Prior to an increase in an Eligible Sub-Capacity Product's virtualization capacity, Client must first acquire sufficient licenses, including IBM Software Subscription and Support, if applicable, to cover that increase.

1.14 Client's Reporting Responsibilities

For Sub-Capacity usage of EPs, Client agrees to install and configure the most current version of IBM's license metric tool (ILMT) within 90 days of Client's first Sub-Capacity based Eligible Sub-Capacity Product deployment, to promptly

install any updates to ILMT that are made available, and to collect deployment data for each such EP. Exceptions to this requirement are i) when ILMT does not yet provide support for the Eligible Sub-Capacity Product, ii) if Client's Enterprise has fewer than 1,000 employees and contractors, Client is not a Service Provider (an entity that provides information technology services for end user customers, either directly or through a reseller), and Client has not contracted with a Service Provider to manage Client's environment in which EPs are deployed, iii) if the total physical capacity of Client's Enterprise servers measured on a full capacity basis, but licensed under Sub-Capacity terms is less than 1,000 PVUs, or iv) when Client's servers are licensed to full capacity.

For all instances where ILMT is not used, and for all non PVU based licenses, Client is required to manually manage and track Client's licenses as described in the Compliance Verification section above.

For all PVU based EP licenses, reports must contain the information in the example Audit Report available at <http://www.ibm.com/software/lotus/passportadvantage/subcaplicensing.html>. Reports must be prepared at least once per quarter. Failure to generate Reports or provide Reports to IBM will cause charging under full capacity for the total number of physical processor cores activated and available for use on the server.

Client will assign a person in Client's organization with authority to manage and promptly resolve questions on Audit Reports or inconsistencies between report contents, license entitlement, or ILMT configuration; and promptly place an order with IBM or Client's IBM reseller if reports reflect EP use over Client's authorized level. IBM Software Subscription and Support and Selected Support coverage will be charged as of the date Client exceeded Client's authorized level.

2. Warranties

Unless IBM specifies otherwise, the following warranties apply only in the country of acquisition.

The warranty for an IBM Program is stated in its license agreement.

IBM warrants it provides IBM Software Subscription and Support, Selected Support and Appliance Services using reasonable care and skill.

IBM warrants that a Machine Component of an Appliance used in its specified operating environment conforms to its official published specifications. The warranty period for an IBM Machine Component of an Appliance is a fixed period commencing on its date of installation (also called "Warranty Start Date") specified in a TD. If a Machine Component does not function as warranted during the warranty period and IBM is unable to either i) make it do so or ii) replace it with one that is at least functionally equivalent, Client may return it to the party from whom Client acquired it for a refund.

The warranty for IBM SaaS is stated in its TD.

IBM does not warrant uninterrupted or error-free operation of an EP or that IBM will correct all defects or prevent third party disruptions or unauthorized third party access to an EP. These warranties are the exclusive warranties from IBM and replace all other warranties, including the implied warranties or conditions of satisfactory quality, merchantability, non-infringement, and fitness for a particular purpose. IBM warranties will not apply if there has been misuse, modification, damage not caused by IBM, failure to comply with instructions provided by IBM, or if otherwise stated in an Attachment or TD. Non-IBM Products are sold under this Agreement as is, without warranties of any kind. Third parties may provide their own warranties to Client.

IBM will identify IBM EPs it does not warrant.

Unless otherwise specified in an Attachment or TD, IBM provides non-IBM EPs, **WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND**. Third parties provide and license products and services directly to Client under their own agreements.

3. Programs and IBM Software Subscription and Support

IBM Programs acquired under this Agreement are subject to IBM's International Program License Agreement IPLA, including its LI.

A Program may include the following, including the original and all whole or partial copies: 1) machine-readable instructions and data, 2) components, 3) audio-visual content (such as images, text, recordings, or pictures), 4) related licensed materials, and 5) license use documents or keys, and documentation.

With the exception of certain Programs that IBM designates as platform or operating system specific, Client may use and install Programs in any commercially available national language for any platform or operating system available from IBM up to the level of Client's authorizations.

3.1 Money-back Guarantee

The IPLA's "money-back guarantee" only applies the first time Client licenses the IBM Program under this Agreement or any other valid agreement. If an IBM Program license is for a Fixed Term subject to renewal or for an initial Commitment Term, Client may obtain a refund only if Client returns the Program and its PoE within the first 30 days of this initial term. The IPLA's "money-back guarantee" does not apply to Appliances.

3.2 Conflict between this agreement and the IPLA

If there is a conflict between the terms of this Agreement, including its Attachments and TDs, and those of the IPLA, including its LI, the terms of this Agreement prevail. The IPLA and its LIs are available on the Internet at <http://www.ibm.com/software/sla>.

3.3 IBM Trade-ups and Competitive Trade-ups

Licenses for certain Programs that replace qualifying IBM Programs or qualifying Non-IBM Programs may be acquired for a reduced charge. Client agrees to terminate Client's use of the replaced Programs when Client installs the replacement Programs.

3.4 Monthly Licenses

Monthly License Programs (ML Programs) are IBM Programs provided to Client for a monthly license charge. Monthly Licenses have a term that begins on the date that Client's order is accepted by IBM and continues for a period Client commits to pay IBM (a Commitment Term) as specified in the TD.

3.5 Fixed Term Licensing

Fixed Term Licenses have a term that begins on the date that Client's order is accepted by IBM; on the calendar day following the expiration of a prior Fixed Term; or on the Anniversary date. A Fixed Term License is for the definite time specified by IBM in a TD.

3.6 Token Licenses

EPs which are Eligible Token Products or ETPs are assigned a Token Value. As long as the total Tokens required for all ETPs used concurrently does not exceed the number of Tokens authorized in Client's PoE(s), Client may use Token(s) for a single ETP or for a combination of ETPs.

Prior to exceeding current Token authorizations or using an Eligible Token Product not authorized, Client must acquire sufficient additional Tokens and authorizations.

ETPs may contain a disabling device that will prevent them from being used after the end of the Fixed Term. Client agrees not to tamper with this disabling device and take precautions to avoid any loss of data.

3.7 CEO Product Categories

Collections of EPs may be offered by IBM on a per user basis subject to a minimum initial user quantity (a CEO Product Category). For Client's first (primary) CEO Product Category, Client must acquire licenses for all users in their Enterprise who have been assigned a machine capable of accessing any Program in the CEO Product Category. For each additional (secondary) CEO Product Category, Client must meet the applicable minimum initial order quantity requirement.

Any installs of any component of a CEO Product Category can only be made and used by or for users for whom licenses have been obtained. All client-side Programs (used on an end user device to access a Program on a server) must be acquired from the same CEO Product Category as the server Program they access.

3.8 IBM Software Subscription and Support

IBM provides IBM Software Subscription and Support with each IBM Program licensed under the IPLA.

IBM Software Subscription and Support begins on the date of IBM Program acquisition and ends on the last day of the corresponding month in the following year, unless the date of acquisition is the first day of the month, in which case coverage ends on the last day of the month, 12 months from acquisition.

IBM Software Subscription and Support includes defect corrections, restrictions, bypasses, and any new versions, releases, or updates IBM makes generally available.

IBM provides Client assistance for Client's i) routine, short duration installation and usage (how-to) questions; ii) code-related questions (together "Support"). Consult the IBM Software Support Handbook for details at <http://www.ibm.com/software/support>. Support for a particular version or release of an IBM Program is available only until IBM withdraws Support for that IBM Program's version or release. When Support is withdrawn, Client must upgrade to a supported version or release of the IBM Program to continue to receive Support. The IBM "Software Support Lifecycle" policy is available at <http://www.ibm.com/software/info/supportlifecycle>.

If Client elects to continue IBM Software Subscription and Support for an IBM Program at a designated Client Site, Client must maintain IBM Software Subscription and Support for all uses and installations of the IBM Program at that Site.

If Client requests to renew expiring IBM Software Subscription and Support at a lesser quantity of IBM Program uses and installations than the expiring quantity, Client must provide a report that verifies current IBM Program usage and installation, and may be required to provide other compliance verification information.

Client shall not use IBM Software Subscription and Support benefits for IBM Programs for which Client has not fully paid for IBM Software Subscription and Support. If Client does, Client must acquire IBM Software Subscription and Support reinstatement sufficient to cover all such unauthorized use at then current IBM prices.

3.9 Selected Support

Selected Support may be available for (i) Non-IBM Programs or for (ii) Programs licensed under the IBM License Agreement for Non-Warranted Programs (together "Selected Programs").

The IBM Software Subscription and Support section above applies to Selected Programs under Selected Support except that 1) IBM may provide Client with assistance in designing and developing applications based on Client's subscription level; 2) the IBM "Software Support Lifecycle" policy does not apply; and 3) no new versions, releases or updates are provided by IBM.

IBM does not provide licenses under this Agreement for Selected Programs.

4. Appliances

An Appliance is an EP which is any combination of Program Components, Machine Components (MCs) and any applicable Machine Code Components offered together as a single offering and designed for a particular function. Unless otherwise provided, terms that apply to a Program apply to the Program Component of an Appliance. Client shall not use an Appliance component independently of the Appliance of which it is a part

Each Appliance is manufactured from parts that may be new or used, and in some cases, an Appliance or its replacement parts may have been previously installed. Regardless, IBM's warranty terms apply.

For each Appliance, IBM bears the risk of loss or damage up to the time it is delivered to the IBM-designated carrier for shipment to Client or Client's designated location. Thereafter, Client assumes the risk. Each Appliance will be covered by insurance, arranged and paid for by IBM for Client, covering the period until it is delivered to Client or Client's designated location. For any loss or damage, Client must i) report the loss or damage in writing to IBM within 10 business days of delivery and ii) follow the claim procedure.

When Client acquires an Appliance directly from IBM, IBM transfers title to a MC to Client or, if applicable, Client's lessor, upon payment of all the amounts due except in the United States where title transfers upon shipment. For an upgrade acquired for an Appliance, IBM reserves transfer of title of the MC until IBM receives payment of all the amounts due and receives all removed parts, which then become IBM's property.

If IBM is responsible for installation, Client will allow installation within 30 calendar days of shipment or additional charges may apply. Client will promptly install or allow IBM to install mandatory engineering changes. Client installs a Client-set-up Appliance according to instructions provided with it.

A Machine Code Component is computer instructions, fixes, replacements and related materials, such as data and passwords relied on, provided, used with or generated by MC, that permit the operation of the MC's processors, storage or other functionality as stated in its Specifications. Client acceptance of this Agreement includes acceptance of IBM's Machine Code license agreements provided with the Appliance. A Machine Code Component is licensed only for use to enable a Machine Component to function under its Specifications and only for the capacity and capability for which Client has acquired IBM's written authorization. The Machine Code Component is copyrighted and licensed (not sold).

4.1 IBM Appliance Services

IBM provides Appliance Services for Appliances consisting of Machine maintenance and IBM Software and Support as a single offering as further described in the Appliance Support Handbook at <http://www.ibm.com/software/appliance/support>.

One year of Appliance Services, starting on the Warranty Start Date specified in a TD, is included with the purchase of an Appliance. Thereafter, automatic renewal terms apply. All renewals will be fulfilled with Appliance Services offered at the same level of service, if available, that Client was entitled to during that first year. Parts removed or exchanged for upgrade, warranty service, or maintenance are IBM property and must be returned to IBM within thirty days. A replacement assumes the warranty or maintenance status of the replaced part. When Client returns an Appliance to IBM, Client will remove all features not supported under Appliance Services, securely erase all data, and ensure that it is free of any legal restrictions that would prevent its return.

Appliance Services cover undamaged and properly maintained and installed Appliances used as authorized by IBM with unaltered identification labels. Services do not cover alterations, accessories, supply items, consumables (such as batteries), structural parts (such as frames and covers), or failures caused by a product for which IBM is not responsible.

5. IBM SaaS

IBM Software as a Service (IBM SaaS) is an EP offering IBM provides to Client remotely through the Internet providing access to (i) functionality of Programs, (ii) infrastructure, and (iii) technical support. IBM SaaS is not a Program but may require Client to download enabling software to use it.

Client acknowledges that International Business Machines Corporation and its subsidiaries do not control the transfer of data over telecommunications facilities, including the Internet. IBM will only provide access and use of Client's proprietary content to IBM employees and contractors as needed to deliver IBM SaaS. IBM will not disclose Client's proprietary content and will return or destroy it upon the expiration or cancellation of IBM SaaS. IBM will provide Client notice of any unauthorized third party access to Client's content of which IBM becomes aware and will use reasonable efforts to remediate identified security vulnerabilities.

Client may access and use IBM SaaS only to the extent of authorizations acquired by Client. Client is responsible for use of IBM SaaS by any party who accesses the IBM SaaS with Client's account credentials. An IBM SaaS may not be used for unlawful, obscene, offensive or fraudulent content or activity, in any jurisdiction for any user, such as advocating or causing harm, interfering with or violating the integrity or security of a network or system, evading filters, sending unsolicited, abusive or deceptive messages, viruses or harmful code, or violating third party rights. If there is a complaint or notice of violation, use may be suspended until resolved, and terminated if not resolved promptly. Unless expressly provided in a TD, Client is not authorized to use IBM SaaS to provide hosting or timesharing services to any third party.

The terms of a specific IBM SaaS offering are provided in its TD and may include without limitation, definitions, description of subscription and services, charge metrics, renewal and restrictions. TDs can be viewed at <http://www-03.ibm.com/software/sla/sladb.nsl/sla/saas/>.

An IBM SaaS Subscription Period begins on the date that IBM notifies Client that Client has access and ends the last day of the month specified in the TD.

During an IBM SaaS Subscription Period, Client may increase Client's subscribed level of an IBM SaaS, but may only decrease the subscribed level at the end of a Subscription Period when renewing.

During an IBM SaaS Subscription Period IBM provides assistance, as specified in the TD, for Client's offering-specific, task-oriented questions regarding IBM SaaS. IBM SaaS technical support is available only for the currently supported versions of IBM SaaS, Client operating systems, Internet browsers, and software. IBM technical support for SaaS is available during the normal business hours (published prime shift hours) of the IBM SaaS support center.

International Passport Advantage Agreement - Country Required Terms (CRTs)

AMERICAS

Governing Laws and Geographic Scope – Replace the phrase, “the laws of the country where the transaction is performed (or for internet delivered Services, the laws of the country of Client’s Business Address)” with:

Canada: the laws of the Province of Ontario.

United States, Anguilla, Antigua/Barbuda, Aruba, British Virgin Islands, Cayman Islands, Dominica, Grenada, Guyana, Saint Kitts and Nevis, Saint Lucia, Saint Maarten, Saint Vincent and the Grenadines: the laws of the State of New York, United States.

General – Replace the first sentence of paragraph two with:

Latin America (all countries): Client accepts the terms in Attachments and Transaction Documents by signing the Attachments and Transaction Documents.

General – Add, where required.

Canada, in Province of Quebec add: Both parties agree to write this document in English. Les parties ont convenu de rédiger le présent document en langue anglaise.

ASIA PACIFIC

Governing Laws and Geographic Scope – Replace the phrase, “the laws of the country where the transaction is performed (or for internet delivered Services, the laws of the country of Client’s Business Address)” with:

Cambodia, Laos: the laws of the State of New York, United States;

Australia: the laws of the State or Territory in which the transaction is performed;

Hong Kong SAR, Macau SAR: the laws of Hong Kong Special Administrative Region (“SAR”);

Korea: the laws of the Republic of Korea;

Taiwan: the laws of Taiwan.

Governing Laws and Geographic Scope– Add as a new paragraph:

Cambodia, India, Laos, Philippines, Vietnam: Disputes will be finally settled by arbitration, held in Singapore, in accordance with the Arbitration Rules of the Singapore International Arbitration Center (“SIAC Rules”) then in effect.

Indonesia: Disputes will be finally settled by arbitration, held in Jakarta, Indonesia, in accordance with the rules of the Board of the Indonesian National Board of Arbitration (Badan Arbitrase Nasional Indonesia or “BANI”) then in effect.

Malaysia: Disputes will be finally settled by arbitration held in Kuala Lumpur in accordance with the Arbitration Rules of the Kuala Lumpur Regional Centre for Arbitration (“KLRC Rules”) then in effect.

People’s Republic of China: Either party has the right to submit the dispute to the China International Economic and Trade Arbitration Commission in Beijing, the PRC, for arbitration in accordance with arbitration rules in force at the time.

Governing Laws and Geographic Scope – Add as a new paragraph:

Hong Kong SAR, Macau SAR, Korea and Taiwan:

All rights and obligations are subject to the courts of the country in which the transaction is performed except that in the countries identified below, all disputes will be brought before and subject to the exclusive jurisdiction of the following courts of competent jurisdiction:

Hong Kong SAR, Macau SAR: the courts of Hong Kong Special Administrative Region (SAR);

Korea: the Seoul Central District Court of the Republic of Korea;

Taiwan: the courts of Taiwan.

EMEA

Appliances – Replace the fourth paragraph with:

Spain, Switzerland, and Turkey: When IBM accepts Client’s order, IBM transfers title to Client or, if applicable, Client’s lessor when the Appliance is shipped to Client or its designated location. However, IBM reserves a purchase money security interest in the MC until IBM receives the amounts due.

Warranties – Add to all countries in Western Europe, after paragraph 4:

The warranty for Machines acquired in Western Europe will be valid and applicable in all Western European countries, provided the Machines have been announced and made available in such countries. For purposes of this paragraph, “Western Europe” means Andorra, Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Monaco, Netherlands, Norway, Poland, Portugal, Romania, San Marino, Slovakia, Slovenia, Spain, Sweden, Switzerland, United Kingdom, Vatican State, and any country that subsequently joins the European Union, from date of accession.

Liability and Indemnity

France, Germany, Malta, Portugal, Spain – Insert after “exceed” and before “the amount”. **the greater of €500,000 (five hundred thousand euro) or**

Ireland, UK - *Replace the phrase "up to the amounts paid" with: up to 125% of the amounts paid*

Governing Laws and Geographic Scope – *Replace the phrase: "the laws of the country where the transaction is performed" or "or internet delivered Services: the laws of the country of Client's Business Address" with:*

Albania, Armenia, Azerbaijan, Belarus, Bosnia-Herzegovina, Bulgaria, Croatia, Former Yugoslav Republic of Macedonia, Georgia, Hungary, Kazakhstan, Kyrgyzstan, Moldova, Montenegro, Romania, Serbia, Tajikistan, Turkmenistan, Ukraine, and Uzbekistan: the laws of Austria;

Algeria, Andorra, Benin, Burkina Faso, Burundi, Cameroon, Cape Verde, Central African Republic, Chad, Comoros, Congo Republic, Djibouti, Democratic Republic of Congo, Equatorial Guinea, French Guiana, French Polynesia, Gabon, Guinea, Guinea-Bissau, Ivory Coast, Lebanon, Madagascar, Mali, Mauritania, Mauritius, Mayotte, Morocco, New Caledonia, Niger, Reunion, Senegal, Seychelles, Togo, Tunisia, Vanuatu, and Wallis and Futuna: the laws of France;

Angola, Bahrain, Botswana, Egypt, Eritrea, Ethiopia, Gambia, Ghana, Jordan, Kenya, Kuwait, Liberia, Malawi, Malta, Mozambique, Nigeria, Oman, Pakistan, Qatar, Rwanda, Sao Tome and Principe, Saudi Arabia, Sierra Leone, Somalia, Tanzania, Uganda, United Arab Emirates, the United Kingdom, West Bank/Gaza, Yemen, Zambia, and Zimbabwe: the laws of England;

Estonia, Latvia, and Lithuania: the laws of Finland;

Russia: the laws of the Russian Federation;

South Africa, Namibia, Lesotho and Swaziland: the laws of the Republic of South Africa.

Governing Laws and Geographic Scope– *Add to the end of the first paragraph:*

Albania, Armenia, Azerbaijan, Belarus, Bosnia-Herzegovina, Bulgaria, Croatia, Former Yugoslav Republic of Macedonia, Georgia, Hungary, Kazakhstan, Kyrgyzstan, Moldova, Montenegro, Romania, Serbia, Tajikistan, Turkmenistan, Ukraine, and Uzbekistan: All disputes will be finally settled under the Rules of Arbitration and Conciliation of the Federal Economic Chamber in Vienna (Vienna Rules).

Algeria, Benin, Burkina Faso, Burundi, Cameroon, Cape Verde, Central African Republic, Chad, Comoros, Congo Republic, Djibouti, Democratic Republic of Congo, Equatorial Guinea, Guinea-Bissau, French Guiana, French Polynesia, Gabon, Guinea, Guinea-Bissau, Ivory Coast, Lebanon, Madagascar, Mali, Mauritania, Mauritius, Mayotte, Morocco, New Caledonia, Niger, Reunion, Senegal, Seychelles, Togo, Tunisia, Vanuatu, Wallis and Futuna: Any dispute will be finally settled by arbitration, administered by the ICC International Court of Arbitration, in Paris, in accordance with its arbitration rules in effect at the time of arbitration, except as may be modified herein or by agreement of the parties.

Angola, Bahrain, Botswana, Egypt, Eritrea, Ethiopia, Gambia, Ghana, Jordan, Kenya, Kuwait, Liberia, Libya, Malawi, Malta, Mozambique, Nigeria, Oman, Pakistan, Qatar, Rwanda, Sao Tome and Principe, Saudi Arabia, Sierra Leone, Somalia, Tanzania, Uganda, United Arab Emirates, West Bank/Gaza, Yemen, Zambia, Zimbabwe: Any dispute will be finally settled by arbitration, administered by the London Court of International Arbitration, in accordance with the LCIA arbitration rules in effect at the time of arbitration, except as may be modified herein or by agreement of the parties.

Estonia, Latvia, and Lithuania: All disputes will be finally settled in arbitration to be held in Helsinki, Finland in accordance with the arbitration laws of Finland then in effect.

Russia: All disputes will be settled by Arbitration Court of Moscow.

South Africa, Namibia, Lesotho, and Swaziland: Any dispute will be finally settled by arbitration, administered by the Arbitration Foundation of South Africa Rules (AFSA Rules), in accordance with the ICC arbitration rules in effect at the time of arbitration, except as may be modified herein or by agreement of the parties.

Governing Laws and Geographic Scope – *Add to the end of the second paragraph:*

All disputes will be brought before and subject to the exclusive jurisdiction of the following courts of competent jurisdiction:

Andorra: the Commercial Court of Paris;

Austria: the court of Vienna, Austria (Inner-City);

Greece: the competent court of Athens;

Israel: the courts of Tel Aviv-Jaffa;

Italy: the courts of Milan;

Portugal: the courts of Lisbon;

South Africa, Namibia, Lesotho and Swaziland: the High Court in Johannesburg;

Spain: the courts of Madrid;

Turkey: the Istanbul Central (Çağlayan) Courts and Execution Directorates of Istanbul, the Republic of Turkey;

United Kingdom: the English courts.

Client Relationship Agreement

Using this agreement, Client may order Programs, Cloud and other Services, Machines and Appliances (collectively IBM Products) and third party products and services (Non-IBM Products) available from IBM. Details regarding products, offerings or orders are provided in Attachments and Transaction Documents (TDs). This agreement and applicable Attachments and TDs are the complete agreement (Agreement) regarding transactions under this Agreement.

Programs

A **Program** is an IBM-branded computer program and related material available for license from IBM subject to the payment of charges. Program details are described in an Attachment called License Information (LI) available at <http://www-03.ibm.com/software/sla/slabd.nsf>. Programs do not include Machine Code or Project Materials. Programs are copyrighted and licensed (not sold). When IBM accepts an order for a Program, IBM grants Client a nonexclusive license to: a) use the Program only up to its authorizations and subject to its LI; b) make and install copies to support such authorized use; and c) make a backup copy. Programs may be used by Client, its authorized employees and contractors only within Client's Enterprise, and not to provide hosting or timesharing services to any third party. Client may not sublicense, assign, or transfer the license for any Program. Additional rights may be available from IBM for additional fees or under different terms. IBM does not grant unrestricted rights to use the Program nor has Client paid for all of the economic value of the Program. Certain Programs may contain third party code licensed under separate agreements identified in the LI.

The license granted for a Program is subject to Client:

- reproducing copyright notices and other markings;
- ensuring anyone who uses the Program does so only for Client's authorized use and complies with the license;
- not reverse assembling, reverse compiling, translating, or reverse engineering the Program; and
- not using any of the elements of the Program or related licensed material separately from the Program.

The metric applicable to a Program license is specified in an Attachment or TD. All licenses on a server or capacity based metric must be licensed to the full capacity of the server on which the Program is installed, unless sub-capacity usage is available from IBM and Client complies with the applicable sub-capacity requirements.

Services - Cloud Services

A **Cloud Service** is an IBM branded offering hosted or managed by IBM and made available via a network. Each Cloud Service is described in a TD or an Attachment called a Service Description. When IBM accepts Client's order, IBM provides Client the entitlements specified in the TD. Cloud Services are designed to be available 24/7, subject to maintenance. Client will be notified of scheduled maintenance. Service level commitments, if applicable, are specified in an Attachment or TD.

Client may access and use a Cloud Service only to the extent of authorizations acquired by Client. Client is responsible for use of Cloud Services by any party who accesses the Cloud Service with Client's account credentials. A Cloud Service may not be used for unlawful, obscene, offensive or fraudulent content or activity, in any jurisdiction for any user, such as advocating or causing harm, interfering with or violating the integrity or security of a network or system, evading filters, sending unsolicited,

abusive or deceptive messages, viruses or harmful code, or violating third party rights. If there is a complaint or notice of violation, use may be suspended until resolved, and terminated if not resolved promptly. Unless expressly provided in a TD, Client is not authorized to use a Cloud Service to provide hosting or timesharing services to any third party.

Each Cloud Service is designed to protect the proprietary content that Client inputs into the Cloud Service and to provide for access and use only as part of the Cloud Service. Except as otherwise specified in a TD, IBM will only provide access and use of Client's proprietary content to IBM employees and contractors as needed to deliver the Cloud Service. IBM will not disclose Client's proprietary content and will return or destroy it upon the expiration or cancellation of the Cloud Service, or earlier upon Client's request. IBM may charge for certain activities performed at Client's request (such as delivering content in a specific format).

The description for each Cloud Service includes the security functions and features applicable to the Cloud Service. IBM will provide Client notice of any unauthorized third party access to Client's content of which IBM becomes aware and will use reasonable efforts to remediate identified security vulnerabilities. If Client's content is lost or damaged, IBM will assist Client in restoring it to the Cloud Service from Client's last available backup copy in compatible format.

The term, including any renewal term, for a Cloud Service is described in an Attachment or TD. IBM may withdraw a Cloud Service on 12 months' notice, unless otherwise stated in an Attachment or TD. IBM will either continue to provide the Cloud Service for the remainder of Client's unexpired term or work with Client to migrate to another IBM Service. IBM may suspend, revoke or limit Client's use of a Cloud Service if IBM determines there is a material breach of Client's obligations, a security breach, or violation of law. Charges will continue to accrue for the Cloud Service during any suspension. If the cause of the suspension can reasonably be remedied, IBM will provide notice of the actions Client must take to reinstate the Cloud Service. If Client fails to take such actions within a reasonable time, IBM may terminate the Cloud Service.

Any changes to the Service Description by IBM will be effective upon the next agreed renewal or extension. IBM may modify the computing environment used to provide a Cloud Service, without degrading its functionality or security features.

Services - Other Services

IBM provides consulting, installation, customization and configuration, maintenance, and other services as detailed in an Attachment or TD. Client will own the copyright in works of authorship that IBM develops for Client under a Statement of Work (SOW) (Project Materials). Project Materials exclude works of authorship delivered to Client, but not created, under the SOW, and any modifications or enhancements of such works made under the SOW (Existing Works). Some Existing Works are subject to a

separate license agreement (Existing Licensed Works). A Program is an example of an Existing Licensed Work and is subject to the Program terms. IBM grants Client an irrevocable (subject to Client's payment obligations), nonexclusive, worldwide license to use, execute, reproduce, display, perform and prepare derivatives of Existing Works that are not Existing Licensed Works. IBM retains an irrevocable, nonexclusive, worldwide, paid-up license to use, execute, reproduce, display, perform, sublicense, distribute, and prepare derivative works of Project Materials.

Either party may terminate a Service if a material breach concerning the Service is not remedied within a reasonable time. IBM will provide at least 90 days' notice prior to withdrawal of Service. Client will pay charges for Services provided through the effective date of termination. If Client terminates without cause or IBM terminates for breach, Client will meet all minimum commitments and pay termination or adjustment charges specified in the SOW or TD and any additional costs IBM reasonably incurs because of early termination, such as costs relating to subcontracts or relocation. IBM will take reasonable steps to mitigate any such additional costs.

Machines and Appliances

A **Machine** is an IBM-branded device including its features, upgrades, and accessories. An **Appliance** is a Program and Machine combination designed for a particular function. Unless otherwise provided, terms that apply to a Program apply to the Program component of an Appliance and terms that apply to a Machine apply to the Machine component of an Appliance. Client may not use or transfer an Appliance's Program component independently of the Appliance.

When IBM accepts Client's order, IBM transfers title to Machines and non-IBM machines to Client or Client's lessor upon payment of all amounts due, except in the United States where title transfers upon shipment. IBM bears risk of loss until delivery to the carrier for shipment. IBM pays for insurance on Client's behalf until delivery to Client's location. Client must report any loss in writing to IBM within 10 business days of delivery and follow the claim procedure. If IBM is responsible for installation, Client will allow installation within 30 calendar days of shipment or additional charges may apply. Client must follow instructions provided to install Client set up Machines.

Machines and parts removed or exchanged for upgrade, warranty service, or maintenance are IBM property and must be returned to IBM promptly. A replacement assumes the warranty or maintenance status of the replaced part. A Machine may include parts that are not new and in some instances Machines may have been previously installed. Regardless, IBM's warranty terms apply. Client will promptly install or allow IBM to install mandatory engineering changes. Client may only acquire Machines for use within Client's Enterprise in the country where acquired and not for resale, lease, or transfer. Lease-back financing is permitted.

Machine Code and Built in Capacity

Machines may include **Machine Code (MC)** and **Built in Capacity (BIC)**. MC is computer instructions, fixes, replacements and related materials, such as data and passwords relied on, provided, used with or generated by MC, that permit the operation of the machine's processors, storage or other functionality. MC is copyrighted and licensed (not sold). IBM only provides copies, fixes or replacements for MC for Machines under warranty or IBM

maintenance, or under a separate written agreement which may be subject to additional charges. Client agrees that all copies, fixes or replacements for MC will be obtained solely as authorized by IBM. IBM grants Client a nonexclusive license to use MC only (i) on the Machine for which IBM provided it, and (ii) to access and use BIC only to the extent paid for by Client, activated by IBM and subject to the Attachment called IBM Authorized Use Table for Machines (AUT) available from IBM and at http://www.ibm.com/systems/support/machine_warranties/machine_code/aut.html. BIC is computing resource (e.g., processors, storage and other functionality) that IBM provides for a Machine. Use of BIC may be restricted by contract, technological or other measures. Client agrees to IBM's implementation of technological and other measures that restrict, monitor and report on use of BIC or MC, and to install any changes IBM provides. Client may not alter, reverse assemble, reverse compile, translate or reverse engineer the MC, or circumvent or interfere, by any means, with IBM's contractual, technological or other measures that restrict, monitor or report on use of BIC or MC. Client may transfer possession of MC only with transfer of the Machine. Client may not transfer its license to MC; the transferee must acquire a license directly from IBM. This Agreement governs MC and BIC on Machines acquired from another party. Use of BIC in excess of authorizations from IBM is subject to additional charges.

Warranties and Post Warranty Support

IBM warrants that Programs used in their specified operating environment conform to their official published specifications. The warranty period for a Program (not the Program component of an Appliance) is one year, or the initial license term if less than one year, unless another warranty period is specified in an Attachment or TD. During the Program warranty period, IBM provides Software Subscription and Support (S&S), entitling Client to defect correction information, restrictions, bypasses, and new releases and versions IBM makes generally available. Unless Client elects to discontinue S&S, annual S&S automatically renews at then-current charges until S&S for a version or release is withdrawn. If Client elects to continue S&S for a Program at a designated Client site, Client must maintain S&S for all uses and installations of the Program at that site.

IBM warrants that it provides Cloud and other Services using commercially reasonable care and skill in accordance with the applicable Attachment or TD, including any completion criteria, and that Project Materials will comply with the Attachment or TD at the time of delivery. The warranty for a Service ends when the Service ends.

IBM warrants that Machines used in their specified operating environment conform to their official published specifications. For a Machine or Appliance, the warranty period is specified in the Attachment or TD. During its warranty period, IBM will repair or exchange the Machine without charge, as specified in the Attachment. Client may purchase warranty service upgrades and post warranty support where available. For Appliances, post warranty support includes maintenance and S&S.

If a Machine or Program does not function as warranted during its warranty period and IBM is unable to repair or replace it with a functional equivalent, Client may return it to IBM for a refund of the amount Client paid (for recurring charges, up to twelve months' charges) and Client's license or right to use it terminates.

IBM does not warrant uninterrupted or error-free operation of an IBM Product or that IBM will correct all defects or prevent third party disruptions or unauthorized third party access to an IBM Product. These warranties are the exclusive warranties from IBM and replace all other warranties, including the implied warranties or conditions of satisfactory quality, merchantability, non-infringement, and fitness for a particular purpose. IBM warranties will not apply if there has been misuse, modification, damage not caused by IBM, failure to comply with instructions provided by IBM, or if otherwise stated in an Attachment or TD. Non-IBM Products are sold under this Agreement as-is, without warranties of any kind. Third parties may provide their own warranties to Client.

Charges, Taxes, Payment and Verification

Client agrees to pay all applicable charges specified by IBM, charges for use in excess of authorizations, any customs or other duty, tax, levy, or fee imposed by any authority resulting from Client's acquisitions under this Agreement, and any late payment fees. Amounts are due upon receipt of the invoice and payable within 30 days of the invoice date to an account specified by IBM. Prepaid Services must be used within the applicable period. IBM does not give credits or refunds for any prepaid, one-time charges, or other charges already due or paid.

Client agrees to: i) pay withholding tax directly to the appropriate government entity where required by law; ii) furnish a tax certificate evidencing such payment to IBM; iii) pay IBM only the net proceeds after tax; and iv) fully cooperate with IBM in seeking a waiver or reduction of such taxes and promptly complete and file all relevant documents. Where taxes are based upon the location(s) receiving the benefit of the Cloud Service, Client has an ongoing obligation to notify IBM of such location(s) if different than Client's business address listed in the applicable Attachment or TD.

IBM may change recurring charges, labor rates and minimum commitments on three months' notice. A change applies on the invoice date or the first day of the charging period on or after the effective date IBM specifies in the notice. IBM may change one-time charges without notice. However, a change to a one-time charge does not apply to an order if i) IBM receives the order before the announcement date of the increase and ii) within three months after IBM's receipt of the order, the product is shipped or made available to Client.

Client will i) maintain, and provide upon request, records, system tools output, and access to Client's premises, as reasonably necessary for IBM and its independent auditor to verify Client's compliance with the Agreement, including MC and Program licenses and metrics, such as sub-capacity usage, and ii) promptly order and pay for required entitlements (including associated S&S or maintenance) at IBM's then current rates and for other charges and liabilities determined as a result of such verification, as IBM specifies in an invoice. These compliance verification obligations remain in effect during the term of any TD and for two years thereafter.

Liability and Indemnity

IBM's entire liability for all claims related to the Agreement will not exceed the amount of any actual direct damages incurred by Client up to the amounts

paid (if recurring charges, up to 12 months' charges apply) for the product or service that is the subject of the claim, regardless of the basis of the claim. This limit applies collectively to IBM, its subsidiaries, contractors, and suppliers. IBM will not be liable for special, incidental, exemplary, indirect, or economic consequential damages, or lost profits, business, value, revenue, goodwill, or anticipated savings.

The following amounts, if a party is legally liable for them, are not subject to the above cap: i) third party payments referred to in the paragraph below; ii) damages for body injury (including death); iii) damages to real property and tangible personal property; and iv) damages that cannot be limited under applicable law.

If a third party asserts a claim against Client that an IBM Product acquired under this Agreement infringes a patent or copyright, IBM will defend Client against that claim and pay amounts finally awarded by a court against Client or included in a settlement approved by IBM, provided that Client promptly (i) notifies IBM in writing of the claim, (ii) supplies information requested by IBM, and (iii) allows IBM to control, and reasonably cooperates in, the defense and settlement, including mitigation efforts.

IBM has no responsibility for claims based, in whole or part, on Non-IBM Products, items not provided by IBM, or any violation of law or third party rights caused by Client's content, materials, designs, specifications, or use of a non-current version or release of an IBM Product when an infringement claim could have been avoided by using a current version or release.

Termination

Either party may terminate this Agreement: a) without cause on at least one month's notice to the other after expiration or termination of its obligations under this Agreement; or b) immediately for cause if the other is in material breach of this Agreement, provided the one who is not complying is given notice and reasonable time to comply. Failure to pay is a material breach. Any terms that by their nature extend beyond the Agreement termination remain in effect until fulfilled, and apply to successors and assignees.

Termination of the Agreement does not terminate TDs, and provisions of this Agreement and Attachments as they relate to such TDs remain in effect until fulfilled or otherwise terminated in accordance with their terms. IBM may terminate Client's license to use a Program or MC if Client fails to comply with this Agreement. Client will promptly destroy all copies of the Program or MC after either party has terminated the license.

Governing Laws and Geographic Scope

Each party is responsible for complying with: i) laws and regulations applicable to its business and content, and ii) import, export and economic sanction laws and regulations, including those of the United States that prohibit or restrict the export, re-export, or transfer of products, technology, services or data, directly or indirectly, to or for certain countries, end uses or end users. Client is responsible for its use of IBM and Non-IBM Products.

Both parties agree to the application of the laws of the state of New York to this Agreement, without regard to conflict of law principles. The rights and obligations of each party are valid only in the country where the transaction is performed or, if IBM agrees, the country where the product is placed in productive use, except all licenses are valid as specifically

granted. If any provision of the Agreement is invalid or unenforceable, the remaining provisions remain in full force and effect. Nothing in the Agreement affects statutory rights of consumers that cannot be waived or limited by contract. The United Nations Convention on Contracts for the International Sale of Goods does not apply to transactions under this Agreement.

General

Parties will not disclose confidential information without a separate, signed confidentiality agreement. If confidential information is exchanged in connection with this Agreement, the applicable confidentiality agreement is incorporated into, and subject to, this Agreement.

Client accepts an Attachment or TD by ordering, enrolling, using, or making a payment for, the product, offering or service. Since this Agreement may apply to many future orders, IBM reserves the right to modify it by providing Client at least three months' written notice. However, changes are not retroactive; they apply, as of the effective date, only to new orders and renewals. For transactions with a defined renewable contract period, Client may request that IBM defer the change effective date until the end of the current contract period. Client accepts changes by placing new orders after the change effective date or allowing transactions to renew after receipt of the change notice. Except as provided above, all changes to the agreement must be in writing signed by both parties. If there is a conflict, an Attachment or TD prevails over the terms of this agreement.

IBM is an independent contractor, not Client's agent, joint venturer, partner, or fiduciary, and does not undertake to perform any of Client's regulatory obligations, or assume any responsibility for Client's business or operations. Each party is responsible for determining the assignment of its personnel and contractors, and for their direction, control, and compensation. IBM Business Partners are independent from IBM and unilaterally determine their prices and terms. IBM is not responsible for their actions, omissions, statements, or offerings.

Client is responsible for obtaining all necessary permissions to use, provide, store and process content in Cloud, other Services, maintenance, or Program support, and grants IBM permission to do the same. Client is responsible for adequate content back-up. Some of Client's content may be subject to governmental regulation or may require security

measures beyond those specified by IBM for an offering. Client will not input or provide such content unless IBM has first agreed in writing to implement additional required security measures.

IBM and its affiliates, and their subcontractors, may process and store business contact information of Client personnel in connection with the performance of this Agreement wherever they do business. IBM may use personnel and resources in locations worldwide and third party suppliers to support the delivery of products and services.

Neither party may assign this Agreement, in whole or in part, without the prior written consent of the other. Assignment of IBM rights to receive payments and by IBM in conjunction with the sale of the portion of IBM's business that includes the product or service is not restricted.

All notices under this Agreement must be in writing and sent to the address below, unless a party designates in writing a different address. The parties consent to the use of electronic means and facsimile transmissions for communications as a signed writing. Any reproduction of the Agreement made by reliable means is considered an original. The Agreement supersedes any course of dealing, discussions or representations between the parties.

No right or cause of action for any third party is created by this Agreement or any transaction under it. Neither party will bring a legal action arising out of or related to this Agreement more than two years after the cause of action arose. Neither party is responsible for failure to fulfill its non-monetary obligations due to causes beyond its control. Each party will allow the other reasonable opportunity to comply before it claims the other has not met its obligations. Where approval, acceptance, consent, access, cooperation or similar action by either party is required, such action will not be unreasonably delayed or withheld.

The Agreement applies to IBM and Client (the signatories below) and their respective Enterprise companies who avail themselves of the Agreement. The signatories shall coordinate the activities of Enterprise companies under this Agreement. Enterprise companies include (i) companies within the same country that Client or IBM control (by owning greater than 50% of the voting shares), and (ii) any other entity that controls, is controlled by or is under common control as Client or IBM and has signed a participation Attachment.

Agreed to:
Client Company Name:

By _____
Authorized signature

Title:
Name (type or print):
Date:
Client number:
Enterprise number:
Client address:

Agreed to:
International Business Machines Corporation

By _____
Authorized signature

Title:
Name (type or print):
Date:
Agreement number:
IBM address:

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*

Vendor Name: **IBM Analytics**

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

	Point Value	Points Given	Comments (Use additional page if necessary)
I Preliminary Evaluation	300	150	
II Technical Solution	100	90	
III Project Management	100	75	
IV Proposal Format	100	100	
V Technical Specifications - Basic Requirements	100	100	
VI Technical Specifications - Preferences	100	93	
VII Add-On Components	100	100	
VIII Management Requirements	100	100	
Sub-Total I - VIII	1,000	808	
References:			
Reference 1	100		
Reference 2	100		
Oral Presentation	200		
Price / Value	500		

Total Points Possible 1,900

Vendor: **IBM Analytics**

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	10
	100	90

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

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

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

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

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

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

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

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

NIBRS RFP Evaluation Total Score

Score 481

Vendor Name: IBM Analytics

Point Value Points Given

Comments (Use additional page if necessary)

	Point Value	Points Given	Comments (Use additional page if necessary)
I Preliminary Evaluation	300		Coplink in other states
II Technical Solution	100	50	
III Project Management	100	75	
IV Proposal Format	100	65	
V Technical Specifications - Basic Requirements	100	75	
VI Technical Specifications - Preferences	100	56	
VII Add-On Components	100	100	
VIII Management Requirements	100	60	
Sub-Total I - VIII		1,000	
References:			
Reference 1	100		
Reference 2	100		
Oral Presentation	200		
Price / Value	500	0	Over grant allotment for Coplink software

Total Points Possible 1,900

Vendor: IBM Analytics

A. Technical Solution		
1. Fulfillment of the requirements as stated in this RFP	20	0
2. Understanding of the work to be performed	20	0
3. Technical approach and methodology to accomplish the work	20	0
4. Completeness and competence in addressing the scope of work	20	0
5. Demonstrated and reliable technology with previous use and success	20	0
	100	0

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

C. Proposal Format		
Cover letter	10	10
Section 1 Proposal executive summary	10	10
Section 2 Technical solution and description	10	5
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	0
Appendix A Supplemental and Collateral Material	10	0
Appendix B Vendor financial qualifications and annual reports	10	10
Appendix C Vendor purchase contract	10	0
Appendix D Vendor software license agreements	10	10
	100	65

D. Technical Specifications - Basic Requirements		
1. Ability to capture and preserve NIBRS data pursuant to current FBI Tech Spec	20	15
2. System allows entry of standard values for each data element	20	10
3. System meets additional WA State IBR data collection requirements	20	15
4. System performs editing and validation of data	20	20
5. System provides capability for submission of NIBRS data	20	15
	100	75

E. Technical Specifications - Preferences		
A. Administrators and Users		
1. Levels of user privileges: administrator, power user, report generator	2	2
2. User receives immediate notification when upload successful or failed	2	2
3. User receives reason in message if a file upload error occurs	2	2
4. System allows user to cancel duplicate file upload	1	0
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	2
7. SSAs have access to standard, ad hoc, crime mapping reports	2	0
8. SSAs are able to monitor system through utilities function	2	2
9. SSAs are able to manage local user accounts	1	0
Sub-Total	15	10
B. Data Entry and File Upload		
1. Submission options include both batch file upload and individual incident entry	2	0
2. Individual incident entry (IIE) has data validation on each field	2	0
3. IIE is user friendly	1	0

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	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	0
12. IIE of domestic violence: DV is associated with the Victim	2	0
13. IIE entry of property: ability to enter immediately with the offense	1	0
14. IIE entry of time: pop-up explaining "00" rule	1	0
Sub-Total	18	5
C. Data Reports		
1. System provides report writing capability; includes standard and ad hoc reports	2	1
2. System allows data output in MS Access, Excel, Word, PDF in report & data form	2	1
3. LEAs have access to other LEA data for report extraction	1	1
4. Data report extraction includes ad hoc, crime mapping, and data quality	2	2
5. Standard reports include:		
a. Summary of offenses	1	1
b. Summary of offenses - Domestic Violence	1	1
c. Offenses by location	1	1
d. Arrests by Offense and Age Category	1	1
e. Hate Crime	1	1
f. Activity Log (by month or year)	1	1
g. Outstanding Errors and Incidents/Arrests Not Checked	1	1
h. Static report (snapshot) of database	1	1
Sub-Total	15	13
D. Data Validation and Error Notification		
1. System meets all FBI and WA State data validation edits and error checks	2	2
2. System sends electronic error reports back to submitting agency	2	0
3. System performs data validations/error checks before FBI file submission	2	0
4. Local and State SA are able to access batch error upload report	2	1
5. Incidents with errors are included in the ad hoc and summary reports	2	2
6. The FBI error messages can be easily edited to make them user friendly	1	0
7. There is no Time-Window Base Date Calculation	2	2
8. The error list does not include errors without a case number	1	1
Sub-Total	14	8
E. State System		
1. The system authenticates access with levels of users	2	2
2. The state system administrators (SSAs) designate roles for local users	2	2
3. The SSAs are able to enter and update data directly through the application	2	0
4. There are two databases: training and production	2	1
a. The training database displays data field descriptions when hovering	1	0
b. SSAs can transfer files from training to production	1	0
c. Production database has permanent archive ability	2	0
Sub-Total	12	5
F. System Features		
1. System discovers NIBRS batch submissions automatically	2	1
2. System provides batch submissions and IIE to repository via web browser	2	1
3. Data are immediately available for reports after State system acceptance	2	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	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		
Sub-Total	14	11
G. Vendor Responsibilities		
1. Vendor has FBI certified state repository in at least one other state	1	0
2. Vendor has system that is FBI submission-capable	2	0
3. Vendor has a minimum of two years' experience with NIBRS repository development	1	0
4. Vendor presents logical solutions and proposed record layouts	1	0
5. Vendor included record layouts and report samples in the technical section	1	0
6. Vendor has customer service available Monday through Friday, 8am-4pm, Pacific Time	1	1
a. Vendor has process for Work Order Number assignment		
b. SSAs are able to check status of work order via on-line tracking system		
7. Vendor will update system per FBI requirements at no additional cost	1	1
8. Vendor will update tables or allow SSAs to update tables in timely manner	1	1
9. Vendor provides user-friendly electronic manuals, error messages, pop-up windows	1	1
10. Vendor provides comprehensive user and technical personnel training	1	0
11. Vendor specified hardware components necessary for proposed repository	1	0
Sub-Total	12	4
Total for Section E. Technical Specifications - Preferences	100	56

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
Sub-Total	100	100

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

NIBRS RFP Evaluation Total Score

Vendor Name: **IBM Analytics**

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	100	
III Project Management	100	77	
IV Proposal Format	100	100	
V Technical Specifications - Basic Requirements	100	92	
VI Technical Specifications - Preferences	100	70.5	
VII Add-On Components	100	100	
VIII Management Requirements	100	70	
Sub-Total I - VIII	1,000		
References:			
Reference 1	100		
Reference 2	100		
Oral Presentation	200		
Price / Value	500	0	

Total Points Possible 1,900

Vendor: IBM Analytics

A. Technical Solution		
1. Fulfillment of the requirements as stated in this RFP	20	20
2. Understanding of the work to be performed	20	15
3. Technical approach and methodology to accomplish the work	20	15
4. Completeness and competence in addressing the scope of work	20	10
5. Demonstrated and reliable technology with previous use and success	20	0
	100	60

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	7
4. Familiarity with NIBRS terminology and requirements	20	15
5. Ability to meet deadlines	15	10
6. Special consideration for detailed project plan	20	15
	100	77

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	17
3. System meets additional WA State IBR data collection requirements	20	20
4. System performs editing and validation of data <i>- saying our data not good?</i>	20	15
5. System provides capability for submission of NIBRS data	20	20
	100	92

E. Technical Specifications - Preferences		
A. Administrators and Users		
1. Levels of user privileges: administrator, power user, report generator	2	1
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	1
5. State system administrators (SSAs) have access to a contact database	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	1
8. SSAs are able to monitor system through utilities function	2	1
9. SSAs are able to manage local user accounts	1	.5
Sub-Total	15	9
B. Data Entry and File Upload		
1. Submission options include both batch file upload and individual incident entry <i>NO IIE</i>	2	1
2. Individual incident entry (IIE) has data validation on each field	2	0
3. IIE is user friendly	1	0

6-3

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	.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	.5
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	1
13. IIE entry of property: ability to enter immediately with the offense	1	.5
14. IIE entry of time: pop-up explaining "00" rule	1	.5
Sub-Total	18	10
C. Data Reports		
1. System provides report writing capability; includes standard and ad hoc reports	2	2
2. System allows data output in MS Access, Excel, Word, PDF in report & data form <small>Access-N</small>	2	1.5
3. LEAs have access to other LEA data for report extraction	1	1
4. Data report extraction includes ad hoc, crime mapping, and data quality	2	2
5. Standard reports include:		
a. Summary of offenses	1	1
b. Summary of offenses - Domestic Violence	1	1
c. Offenses by location	1	1
d. Arrests by Offense and Age Category	1	1
e. Hate Crime	1	1
f. Activity Log (by month or year)	1	1
g. Outstanding Errors and Incidents/Arrests Not Checked	1	1
h. Static report (snapshot) of database	1	1
Sub-Total	15	14.5
D. Data Validation and Error Notification		
1. System meets all FBI and WA State data validation edits and error checks	2	2
2. System sends electronic error reports back to submitting agency	2	2
3. System performs data validations/error checks before FBI file submission	2	2
4. Local and State SA are able to access batch error upload report	2	2
5. Incidents with errors are included in the ad hoc and summary reports	2	2
6. The FBI error messages can be easily edited to make them user friendly	1	.5
7. There is no Time-Window Base Date Calculation	2	2
8. The error list does not include errors without a case number	1	1
Sub-Total	14	13.5
E. State System		
1. The system authenticates access with levels of users	2	2
2. The state system administrators (SSAs) designate roles for local users	2	2
3. The SSAs are able to enter and update data directly through the application	2	1
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	.5
c. Production database has permanent archive ability	2	0
Sub-Total	12	8.5
F. System Features		
1. System discovers NIBRS batch submissions automatically	2	2
2. System provides batch submissions and IIE to repository via web browser	2	1
3. Data are immediately available for reports after State system acceptance	2	2
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

Extra

Extra

Extra

"

"

"

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	.5	Extra
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		—	Extra
10. Journal is available in Utilities for SSAs to track agency information, error rates, and agency	1	1	
11. Zero Report can be entered even if the file contains a correction from previous month	1	.5	Extra
12. Agency can override Zero Report month if an incident is now available for the month	1	.5	"
13. NIBRS data can be converted to Summary format for certification purposes			
Sub-Total	14	9.5	
G. Vendor Responsibilities			
1. Vendor has FBI certified state repository in at least one other state	1	0	
2. Vendor has system that is FBI submission-capable	2	0	
3. Vendor has a minimum of two years' experience with NIBRS repository development	1	.5	Display
4. Vendor presents logical solutions and proposed record layouts	1	.5	Extra
5. Vendor included record layouts and report samples in the technical section	1	0	
6. Vendor has customer service available Monday through Friday, 8am-4pm, Pacific Time	1	1	
a. Vendor has process for Work Order Number assignment		—	
b. SSAs are able to check status of work order via on-line tracking system		—	
7. Vendor will update system per FBI requirements at no additional cost	1	1	
8. Vendor will update tables or allow SSAs to update tables in timely manner	1	1	
9. Vendor provides user-friendly electronic manuals, error messages, pop-up windows	1	.5	
10. Vendor provides comprehensive user and technical personnel training	1	.5	Extra
11. Vendor specified hardware components necessary for proposed repository	1	.5	
Sub-Total	12	5.5	
Total for Section E. Technical Specifications - Preferences	100		

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

Management Requirements		
1. Project Plan:		
a. Comprehensive in scope and detail	10	10
b. Plan includes project tasks, approximate dates, and time in hours	10	5
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	5
b. Product enhancement	10	5
c. Work order number process	10	5
5. Testing:		
a. WASPC project team has access to software for application testing	10	0
b. Minimum 60-day acceptance testing	10	10
c. FBI recertification plan	10	10
Sub-Total	100	70

NIBRS RFP Evaluation Total Score

Score 531.5

Vendor Name: IBM Analytics

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	45	
III Project Management	100	70	
IV Proposal Format	100	80	
V Technical Specifications - Basic Requirements	100	80	
VI Technical Specifications - Preferences	100	68.5	
VII Add-On Components	100	100	
VIII Management Requirements	100	88	
Sub-Total I - VIII	1,000		
References:			
Reference 1	100		
Reference 2	100		
Oral Presentation	200		
Price / Value	500		

Total Points Possible 1,900

Vendor: **IBM Analytics**

A. Technical Solution		
1. Fulfillment of the requirements as stated in this RFP	20	10
2. Understanding of the work to be performed	20	10
3. Technical approach and methodology to accomplish the work	20	10
4. Completeness and competence in addressing the scope of work	20	10
5. Demonstrated and reliable technology with previous use and success	20	5
	100	45

B. Project Management		
1. Completeness and responsiveness of project management plans	15	10
2. Project Team assigned	15	15
3. Experience in development and implementing similar systems	15	5
4. Familiarity with NIBRS terminology and requirements	20	15
5. Ability to meet deadlines	15	15
6. Special consideration for detailed project plan	20	10
	100	70

C. Proposal Format		
Cover letter	10	10
Section 1 Proposal executive summary	10	5
Section 2 Technical solution and description	10	5
Section 3 Project management description	10	10
Section 4 Vendor section for additional information	10	10
Section 5 Pricing section - to include product and maintenance/support pricing	10	10
Appendix A Supplemental and Collateral Material	10	0
Appendix B Vendor financial qualifications and annual reports	10	10
Appendix C Vendor purchase contract	10	10
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	15
2. System allows entry of standard values for each data element	20	10
3. System meets additional WA State IBR data collection requirements	20	15
4. System performs editing and validation of data	20	20
5. System provides capability for submission of NIBRS data	20	20
	100	80

E. Technical Specifications - Preferences		
A. Administrators and Users		
1. Levels of user privileges: administrator, power user, report generator	2	2
2. User receives immediate notification when upload successful or failed	2	2
3. User receives reason in message if a file upload error occurs	2	2
4. System allows user to cancel duplicate file upload	1	1.5
5. State system administrators (SSAs) have access to a contact database	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	1
9. SSAs are able to manage local user accounts	1	0
Sub-Total	15	11.5
B. Data Entry and File Upload		
1. Submission options include both batch file upload and individual incident entry	2	1
2. Individual incident entry (IIE) has data validation on each field	2	1
3. IIE is user friendly	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	—
9. IIE entry of date or calendar option	1	1
10. IIE hot key options are available	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	—
13. IIE entry of property: ability to enter immediately with the offense	1	—
14. IIE entry of time: pop-up explaining "00" rule	1	—
Sub-Total	18	9
C. Data Reports		
1. System provides report writing capability; includes standard and ad hoc reports	2	2
2. System allows data output in MS Access, Excel, Word, PDF in report & data form	2	1
3. LEAs have access to other LEA data for report extraction	1	1
4. Data report extraction includes ad hoc, crime mapping, and data quality	2	2
5. Standard reports include:		
a. Summary of offenses	1	1
b. Summary of offenses - Domestic Violence	1	1
c. Offenses by location	1	1
d. Arrests by Offense and Age Category	1	1
e. Hate Crime	1	1
f. Activity Log (by month or year)	1	1
g. Outstanding Errors and Incidents/Arrests Not Checked	1	1
h. Static report (snapshot) of database	1	1
Sub-Total	15	14
D. Data Validation and Error Notification		
1. System meets all FBI and WA State data validation edits and error checks	2	2
2. System sends electronic error reports back to submitting agency	2	1
3. System performs data validations/error checks before FBI file submission	2	2
4. Local and State SA are able to access batch error upload report	2	2
5. Incidents with errors are included in the ad hoc and summary reports	2	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	2	2
8. The error list does not include errors without a case number	1	1
Sub-Total	14	11
E. State System		
1. The system authenticates access with levels of users	2	2
2. The state system administrators (SSAs) designate roles for local users	2	2
3. The SSAs are able to enter and update data directly through the application	2	1
4. There are two databases: training and production	2	1
a. The training database displays data field descriptions when hovering	1	—
b. SSAs can transfer files from training to production	1	—
c. Production database has permanent archive ability	2	—
Sub-Total	12	6
F. System Features		
1. System discovers NIBRS batch submissions automatically	2	2
2. System provides batch submissions and IIE to repository via web browser	2	1
3. Data are immediately available for reports after State system acceptance	2	2
4. Domestic Violence (DV) indicator is associated with Victim	1	.5
a. DV default is set for based on certain relationships, i.e. Spouse		
b. If default is triggered, a pop-up question asks, "Are you sure?"		
5. Gang Involvement indicator is set as mandatory	1	.5

6. All related cases for Multiple Clearance indicator are displayed	1	.5
a. User is able to delete a case number on the list		
7. Data values not relevant to WA State or utilized by FBI can be "greyed out"	1	.5
8. System journal is available for SSAs to track IIE data entry and updates	1	1
9. Pop-up windows asking "Are you sure?" are available		-
10. Journal is available in Utilities for SSAs to track agency information, error rates, and agency	1	1
11. Zero Report can be entered even if the file contains a correction from previous month	1	.5
12. Agency can override Zero Report month if an incident is now available for the month	1	.5
13. NIBRS data can be converted to Summary format for certification purposes		
Sub-Total	14	10
G. Vendor Responsibilities		
1. Vendor has FBI certified state repository in at least one other state	1	.5
2. Vendor has system that is FBI submission-capable	2	.5
3. Vendor has a minimum of two years' experience with NIBRS repository development	1	.5
4. Vendor presents logical solutions and proposed record layouts	1	-
5. Vendor included record layouts and report samples in the technical section	1	.5
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	.5
10. Vendor provides comprehensive user and technical personnel training	1	.5
11. Vendor specified hardware components necessary for proposed repository	1	1
Sub-Total	12	7
Total for Section E. Technical Specifications - Preferences	100	68.5

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

Management Requirements		
1. Project Plan:		
a. Comprehensive in scope and detail	10	8
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	5
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	5
b. Minimum 60-day acceptance testing	10	10
c. FBI recertification plan	10	10
Sub-Total	100	88

Phase 2 Evaluation

Vendor: IBM

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)		X		
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				
A. Administrators and Users				
1. Levels of user privileges: administrator, power user, report generator		X		
2. User receives immediate notification when upload successful or failed		X		
3. User receives reason in message if a file upload error occurs	inadequate			X
4. System allows user to cancel duplicate file upload				X
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		X		
8. SSAs are able to monitor system through utilities function				X
9. SSAs are able to manage local user accounts				
Comments:				
B. Data Entry and File Upload				
1. Submission options include both batch file upload and individual incident entry		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	optional		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: Willingness to provide what is needed. Team seems to go above and beyond.			
C. Data Reports			
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		
3. LEAs have access to other LEA data for report extraction	X		
4. Data report extraction includes ad hoc, crime mapping, and data quality	X		
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	X		
Comments:			
Cognos seem cumbersome but is learning curve capabilities in Ad hoc very good			
D. Data Validation and Error Notification			
1. System meets all FBI (and WA State) data validation edits and error checks	will	X	
2. System sends electronic error reports back to submitting agency	Automated	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			
5. Incidents with errors are included in the ad hoc and summary reports			X
6. The FBI error messages can be easily edited to make them user friendly		X	
7. There is no Time-Window Base Date Calculation			
8. The error list does not include errors without a case number			
Comments:			

- willing to do what they can to make what we want - system/price
- 24/7 support - critical issues call within hour. status online.
- training + access to multiple people for customer service

IBM

- Willingness to provide exactly what is needed. Team seems to go above and beyond.
- Cognos seems cumbersome but once all data elements are available should be exactly what is needed for reports, ad hoc reports and dashboards.
- Everything was added into total cost.
- 24/7 support – critical issues handled within an hour with online status review.
- Training and access to multiple people for customer service.
- Will build to what state requires and how state wants.
- Reports will be real time or as specified by user.

Vendor: IBM

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>system performs validations as entry is completed</i>				
5. System provides capability for submission of NIBRS data		✓		
Comments:				

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

Comments: entry process was very smooth. The flow was good. The screens are nice & logic behind the screens was great.

C. Data Reports

- 1. System provides report writing capability; includes standard and ad hoc reports ✓
- 2. System allows data output in MS Access, Excel, Word, PDF in report & data form ✓
- 3. LEAs have access to other LEA data for report extraction ✓
- 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:
 Reports will be built to our specifications
 This will require more time to learn

D. Data Validation and Error Notification

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

Comments:

Notes on IBM Analytics System

Manual incident entry into system is user friendly and very intuitive. Background logic in place based on offense. System highlights data fields that are required, such as, method of entry when the offense is a burglary. If the data element is not required, the field is not available to populate.

When a data element may be used more than one time, such as, "weapon/force involve", you have one dropdown and may select up to three choices.

The system allows reports to be generated as soon as data is placed into repository.

Coplink on Cloud

- Housed at NLETS facility
- Secured/Encrypted facility

Cognos Express:

- Dashboards can be placed on website and data will refresh as we require. When data is on the website, it cannot be manipulated by the public.
- Reports will be created for us (as many as we wish) and we will be shown how to create reports as well.
- System will allow for data other than NIBRS data to be ingested into system for reporting. For example, jail statistics.