



Washington State
Department of Social
& Health Services

Operations Support and Services Division
Background Check Central Unit

RFP 1524-577

EXHIBIT D

BUSINESS REQUIREMENTS PACKAGE

REQUIREMENTS, PROCESS FLOWS & BUSINESS RULES

BACKGROUND CHECK SYSTEM PROJECT

November 2015

DOCUMENT INFORMATION AND APPROVALS

VERSION HISTORY			
<u>Version #</u>	<u>Date</u>	<u>Revised By</u>	<u>Reason for change</u>
0.1	06/04/2015	Cindy LaRose-Eatwell	Initial Draft
0.2	6/11/2015	Richelle Glascock	Updated references to Appendixes and format review to deliver for QA Assessment. Updated document name to include version number and date.
0.3	6/25/2015	Cindy LaRose-Eatwell	Updated to incorporate recommendations of QA vendor.
0.4	7/1/2015	Richelle Glascock	Updated Glossary and Constraints
0.5	11/05/2015	Cindy LaRose-Eatwell	Updated flows, requirements, and business rules to reflect recent changes to business process and to address comments from independent QA assessment.

DOCUMENT APPROVALS

This document has been approved as the official Business Requirements Document for the Background Check System Project and accurately reflects the current understanding of business requirements. Following requirements validation with successful vendor, requirement changes will be governed by the project’s change management process, including impact analysis, appropriate reviews and approvals.

TABLE OF CONTENTS

1. Document Purpose 1

2. Document Resources 1

3. Glossary of Terms 1

4. Project Overview 4

 4.1 Project Overview and Background 4

 4.2 Project Dependencies..... 5

 4.3 Stakeholders..... 5

5. Key Assumptions and Constraints..... 5

 5.1 Key Assumptions and Constraints..... 5

6. Business Requirements 6

 6.1 General Functional Business Requirements 6

 6.2 Online Applicant Form 13

 6.3 Submit New Background Check Application 16

 6.4 Match Person of Interest Records 23

 6.5 Search Data Sources..... 26

 6.6 Investigator Review and Determine Results..... 32

 6.7 Thumbprint Process..... 49

 6.8 Legal Review Processes 53

 6.9 Court and Corrections Research (FORS/JIS) 58

 6.10 Initiate Fingerprint Check..... 60

 6.11 Fingerprint Handling 65

 6.12 Documents and Imaging..... 81

 6.13 Quality Assurance..... 84

 6.14 Background Check Update..... 86

 6.15 Records Request 88

 6.16 Audit Review..... 90

 6.17 Department of Health Review Inquiry..... 93

 6.18 Entity Accounts, Users and User Roles..... 97

 6.19 Workload Management..... 107

 6.20 Customer Support..... 109

 6.21 Reconcile Accounts 112

 6.22 Reporting Requirements..... 115

 6.23 Non-Functional Requirements..... 116

 6.24 Technical Requirements..... 118

 6.25 Security Requirements 120

 6.26 Specific Interface Requirements..... 122

1. DOCUMENT PURPOSE

This document defines the functional and non-functional business requirements, future and current state work process flows, and business rules for the Department of Social and Health Services, Background Check System Project. Each section of the document includes a list of supporting documentation that will be provided to the successful vendor at the time of requirements verification. This document will be used as the basis for the following activities:

- Creating solution designs
- Developing use cases
- Developing test plans, test scripts, and test cases
- Determining project completion
- Assessing project success

2. DOCUMENT RESOURCES

The following identifies stakeholders and resources who were involved in gathering requirements.

Name	Business Unit	Role
Cindy LaRose-Eatwell	Background Check Central Unit	Business Lead
Richelle Glascock	Background Check System Project	Project Manager
Lamona Foster	Background Check Central Unit	Office Chief
Jennifer Colley	Background Check Central Unit	Operations
Elizabeth Elder	Background Check Central Unit	Process Improvement
Jessica Ward	Background Check Central Unit	Vendor and Customer Relations
Julie Jarrett	Background Check Central Unit	Subject Matter Expert
Urbano Eijan	Technology Services Division	Lead Developer
David Amyakar	Technology Services Division	Technology Lead
Aaron Mason	Enterprise Technology	Security Analyst
Background Check Advisory Group	DSHS Oversight Programs	Group responsible for coordinating department-wide background check process and policy

3. GLOSSARY OF TERMS

Term/Acronym	Definition
ADSA	Aging and Disability Services Administration (DSHS) – former DSHS administration – split into three separate administrations – AL TSA, BHSIA and DDA
AL TSA	Aging and Long-Term Support Administration (DSHS) – formerly part of ADSA
AOC	Administrative Office of the Courts – provides criminal conviction information through access to public data warehouse.

Term/Acronym	Definition
Applicant	The person of interest who is the subject of the background check
APS	Adult Protective Services
Background Check	Search of a person's criminal history and negative action background, beginning with a request being submitted and ending with results being distributed
BCCU	Background Check Central Unit – the centralized unit that processes background checks on behalf of DSHS oversight programs who are responsible to conduct background checks on internal staff and contracted and licensed providers and their employees.
BHSIA	Behavioral Health and Service Integration Administration (DSHS) – formerly part of ADSA
CA	Children's Administration (DSHS)
CHS	Criminal History System, the current system used by BCCU to process and store background checks
Confidential Information or Data	Information that is exempt from disclosure to the public or other unauthorized persons under RCW 42.56 or other federal or state laws. Confidential Information includes, but is not limited to personally identifiable information.
DDA	Developmental Disabilities Administration (DSHS) – formerly part of ADSA
DEL	Washington State Department of Early Learning
DOH	Washington State Department of Health
DSHS	Department of Social and Health Services
Encrypt	To encode Confidential Information into a format that can only be read by those possessing a "key", a password, digital certificate or other mechanism available only to authorized users.
Entity	An internal DSHS business unit or external contracted or licensed service provider who is approved by a DSHS oversight program to request background checks through BCCU.
ESA	Economic Services Administration (DSHS)
FBI	Federal Bureau of Investigation
Findings	Administrative decisions recorded by an agency, accessed as part of a background check
HCS	Home and Community Services (DSHS) – a division of ALTSA
HRD	Human Resources Division (DSHS)
TSD	Technology Services Division (formerly Information System Services Division) within DSHS
RA	Rehabilitation Administration (formerly Juvenile Justice and Rehabilitation Administration) within DSHS

Term/Acronym	Definition
Name/DOB	Name and date of birth
OCA	Originating Case Agency – also known as BCCU Inquiry ID#. Unique number assigned by background check system to each background check inquiry. Used by WSP and BCCU for tracking and billing reconciliation.
Originating Index # (ORI)	Numbers assigned by the FBI based on the purpose entities are running a fingerprint-based background check. The ORI is also used by the WSP and MT. The ORI is sent to MT and MT sends the ORI with the Fingerprint to the WSP. The WSP uses the ORI when billing DSHS. A federal fingerprint check cannot be run without an ORI.
Person of Interest	Also known as POI. The applicant or the subject of the background check that OCAs are associated with.
Personal Information	Information identifiable to any person, including, but not limited to, information that relates to a person’s name, health, finances, education, business, use or receipt of governmental services or other activities, addresses, telephone numbers, SSNs, driver license numbers, other identifying numbers, and any financial identifiers.
POI	Person of Interest. The person of interest is a person that has undergone a background check through BCCU.
POI#	Person of Interest number – the unique number assigned to each person of interest contained in the background check system.
Quick Return	In the CHS, the process of automatically checking multiple background check data sources for “hits”. If there are no hits in any of the data sources, the system automatically issues a “No Record” result.
Rap-back	A service where an employer may register with the FBI or State so that if an employee is arrested, arraigned or convicted, the employer is notified.
RCS	Residential Care Services (DSHS) – a division of AL TSA
SID	State ID number: fingerprint-based identifier of a person, assigned by WSP and associated with the WSP rapsheet.
TCN	Transaction Control Number – unique number assigned by either the fingerprint vendor or WSP to each set of fingerprints – used by WSP, also used by BCCU for tracking and billing reconciliation.
WSP	Washington State Patrol

4. PROJECT OVERVIEW

4.1 Project Overview and Background

The Department of Social and Health Services (DSHS) is seeking to replace its existing Criminal History System with a web-based solution for the submission and receipt of background checks. This system supports the functions of a centralized Background Check Unit (BCCU) as well as provider and program interaction with the BCCU. The Background Check System must have the flexibility to respond to the dynamic nature of the Department's statutory requirements and business needs of multiple business areas within the Department of Social and Health Services.

The DSHS BCCU processes over 320,000 background checks for over 75 business areas within DSHS and the Department of Early Learning (DEL) annually. Federal and state laws as well as core business needs for the various business areas mandate:

- The type of background check a business area can perform (name/date of birth or fingerprint)
- Recheck requirements and frequency
- Disqualifying crimes/negative actions
- Who makes the suitability determination
- Who can view/receive FBI records

DSHS uses an inquiry type structure that allows us to apply a common set of business rules to business areas that share the same or similar mandates, eliminating the need to write specific business rules for each business area. Additionally, the inquiry type structure is designed to ensure the appropriate funding sources are charged and DSHS programs have the data necessary to oversee background check activities.

To minimize background check costs, the current DSHS system incorporates a number of automated processes that enable BCCU to efficiently process background checks with minimal FTEs. When a new background check request is received in the work flow, the system automatically searches seven integrated data sources to determine possible hits. Currently about seventy-four percent of Name/DOB background checks (no records) are processed by the system with no manual BCCU review. For the background checks not automatically processed by the system, BCCU staff are required to process a background check in less than two minutes.

The Background Check Central Unit is an information pass-through and does not make the final character, competence and suitability decisions. The Background Check System must have the capability to search multiple data sources; store information associated with a person of interest, and push the data and documents to the entity user who is responsible for making the hiring, placement, or contracting decision.

DSHS is mandated by law to pay the cost of the background checks conducted, including those conducted for external providers. DSHS programs spend millions of dollars each year on background checks. The DSHS Background Check System must be able to incorporate business rules to enforce the mandates for numerous business areas, and have a method for ensuring the appropriate funding sources are charged for the costs of background checks. The system must incorporate equivalent automation and workflow efficiencies of the current system to ensure BCCU can continue to process background checks with existing FTE resources. The Background Check System must incorporate validation to ensure unnecessary background checks costs are not incurred.

4.2 Project Dependencies

No known project dependencies exist.

4.3 Stakeholders

The following comprises the internal and external stakeholders whose requirements are represented by this document:

	Stakeholders
1.	All DSHS Oversight Programs who conduct background checks through BCCU
2.	Department of Early Learning
3.	Department of Health
4.	Washington State Patrol
5.	Washington Administrative Office of the Courts
6.	MorphoTrust –fingerprint vendor
7.	Federal Bureau of Investigation
8.	External licensed and contracted providers who are required by DSHS oversight programs to conduct background checks through BCCU
9.	DSHS Information System Services Division

5. KEY ASSUMPTIONS AND CONSTRAINTS

5.1 Key Assumptions and Constraints

#	Assumptions
1.	DEL, ESA, and MT will have sufficient resources to complete the needed system modifications noted in this document or its appendices.
2.	DEL, ESA, and MT will have the resources to test changes to system interfaces.
#	Constraints
1.	The BCS must include equivalent automation to the CHS.
2.	Changes to interface systems (e.g. DEL, WSP) are limited to what specified in this document or its appendices. Additional changes must be agreed to by the affected interface partner.

6. BUSINESS REQUIREMENTS

The following sections document the various functional business requirements, non-functional requirements, and technical requirements of the Background Check System Project. The functional business requirements sections are organized into the main functional areas of the system. Each section contains a requirements table, business rules, and future and current state work process flows (if applicable*). Supporting documents referenced in the requirements or business rules are contained in the document appendices and will be provided to the successful vendor during requirements verification.

* Where the current state and future state process is significantly the same, no current state work process flow is included. Work process flows are only included if a visual representation is beneficial to clarify the requirements/business rules.

Note: Work process flow documents contain a reference number in each object. These numbers do not denote process sequence; they serve as a reference point for discussion only.

Requirements Table Requirement Type Key

- F = Functional Requirement
- NF = Non-Functional Requirement
- T = Technical Requirement
- S = Security Requirement
- I = Interface Requirement

6.1 General Functional Business Requirements

This section describes the functional requirements that apply throughout the Background Check System or to more than one functional area.

Requirements Table 6.1 – General Business Requirements		
Requirement Type (F/NF/T)	Requirement Number	Function/Feature - Requirement
F	1.1	Provide a complete web-based background check system that provides the following components: <ul style="list-style-type: none"> • Web-based method for authorized entities to submit background check applications and receive background check results; • Online form for applicants to complete and print the background authorization form and save applicant information to database for later retrieval; • Centralized repository of background check results, documents, and person of interest information;

Requirements Table 6.1 – General Business Requirements		
		<ul style="list-style-type: none"> Automated processing system with interfaces to data sources, integrated workload management, and automated no-record results processing; Web interfaces with the Department of Early Learning and Economic Services Administration systems for the submission and results of background checks; Background check inquiry lookup for Department of Health licensers to view the results of long-term care background checks. Background check inquiry lookup for internal audit staff and DSHS oversight programs to monitor background check activities. Robust reporting capabilities for various user groups.
F	1.2	Provide the ability to conduct and track in-state name/date of birth and national fingerprint-based background checks.
F	1.3	Provide the capability to create and maintain a person of interest profile, including demographic information for each application.
F	1.4	Provide the ability to store incoming background check application data until the POI matching procedure is completed by the BCS or BCCU staff. See Section 6.4.
F	1.5	Maintain a history of background checks associated with a person of interest.
F	1.6	Provide a method for viewing background check inquiries associated with a person of interest record.
F	1.7	Provide the ability to track the status of a background check based on specific points in the process.
F	1.8	Provide the ability to view submitted background checks at any stage of the process.
F	1.9	Maintain an audit trail of activities related to a background check by recording all associated transactions.
F	1.10	Track multiple parties involved in a background check: the applicant (person of interest), primary entity (the BCCU account holder), and the secondary entity (contracted vendor/employer who is not the account holder).
F	1.11	Provide a method to store criminal history records and access them for viewing/printing.
F	1.12	Provide a method for BCCU user to initiate an e-mail communication to requesting entity user or secondary contact.
F	1.13	Have the ability to track the time elapsed from initiation of a background check request to the result being distributed.
F	1.14	Have the capability to record all of the transactions performed in the course of a background check, such as queries to registries, issuance of result letters, data entry corrections, etc.
F	1.15	Ability to capture notes related to the submission or processing of a background check.
F	1.16	Provide the ability to select pre-defined notes available through a drop-down list or to add custom notes. Pre-defined notes will be categorized by subject area.
F	1.17	Associate notes with the applicable person of interest and OCA.
F	1.18	Provide the ability to sort the list of notes related to a subject area.
F	1.19	Provide the ability to automatically include certain types of notes, called source information or source merge text, in the result notification or result letter.
F	1.20	Track the note type, date, and user who added the note.
F	1.21	Provide a method for authorized entities to create and view notes associated with a background check application.
F	1.22	Ensure entity notes are only viewed by entity users with permission to view notes.
F	1.23	Provide a method for BCCU users to capture and view notes associated with a person of

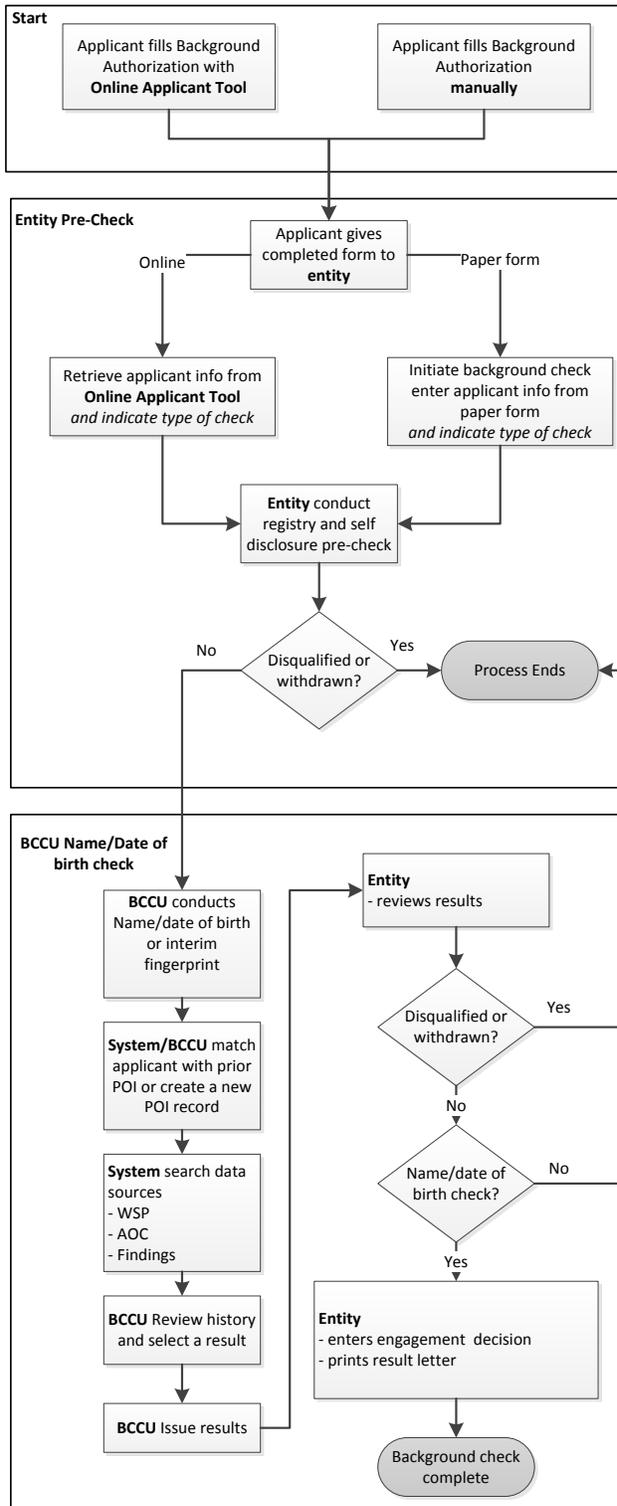
Requirements Table 6.1 – General Business Requirements		
		interest or a specific background check inquiry (OCA).
F	1.24	Ensure BCCU notes are only viewed by BCCU users with permission for viewing notes.
F	1.25	Provide a notification to the requesting user that a background check is complete and the outcome of the check. This may include notifying other systems, such as DEL and ESA web applications.
F	1.26	Provide a means for the requesting user to view completed background checks including: the result type, self-disclosure information, and any associated rap sheets. Exception: Only authorized users may view fingerprint rap sheets.
F	1.27	Provide capability for requesting user to print and mail result letter and associated background check information such as rap sheets, self-disclosures, and negative action information. Exception: The system must prevent the FBI rap sheet from being viewed and printed by unauthorized users.
F	1.28	Retain a history of background check results and result letters.
F	1.29	Provide the capability to run an interim in-state Name/DOB check when a fingerprint-based background check type is submitted. These checks are referred to as interim fingerprint.
F	1.30	Incorporate records retention rules to identify and remove records from the data base when the retention period is past.
F	1.31	Provide a method for BCCU users to review the records scheduled to be deleted and provide a method for BCCU users to approve or decline record deletion.
F	1.32	Provide a method for certain BCCU users to apply a legal hold to a person of interest record, an OCA, or to records associated with a BCCU account # to prevent the records from being deleted. When a record is flagged for a legal hold, notify the BCCU user.
F	1.33	Provide a method for the entity to record an engagement and separation determination for each completed background check on an applicant.
F	1.35	Provide the ability for entities to create a profile for secondary entities and associate a secondary entity to a background check application.
F	1.36	Provide the ability to generate a fingerprint appointment form with BCCU Account #, OCA #, and applicant information populated into the form.
F	1.37	Provide the ability for entity user to print the fingerprint appointment form returned with the interim fingerprint result.
F	1.38	Allow criminal history records from the FBI to be viewed or distributed only to authorized DSHS personnel, Area Agencies on Aging, Department of Early Learning (within certain timeframes), and the Department of Health.
F	1.39	Provide the ability to incorporate a hierarchical inquiry type structure.
F	1.40	Provide the ability to implement a series of rules at the inquiry type level that allows or prohibits certain functions by the entity users.
F	1.41	The system must have the ability to define the type of background check allowed for each inquiry type. Example: Only certain inquiry types may request fingerprint checks.
F	1.42	Provide the ability to track multiple parties involved in the background check.
F	1.43	Ability to create and maintain applicant associations to one or more entities.
F	1.44	Maintain a history of changes to applicant information.
F	1.45	Provide a method for BCCU users to e-mail the entity user who submitted a background check.
F	1.46	Provide a method for BCCU users to manage system administrative tasks through use of system tools.

Business Rules Table 6.1 – General/Global Business Rules	
BR#	Rule Description
1000	Person of Interest Files (including OCAs and associated documents/images) are retained in system for 20 years after the last background check was completed then all records within the POI file are destroyed.
1001	For imaged documents, WA state law mandates that the storage of the original hardcopy scan must be stored as a PNG or a TIFF. Even if the BCS decides to display PDF, it must retain the original TIFF/PNG format.
1002	If a document or file is received electronically it must be stored in the same format as it was received. PDF saved as PDF. TIFF as TIFF etc.
1003	Email must be a valid email with format email@domain.com.
1004	When search or choice options require the user to choose an inquiry type or division, the search will apply the following pick list hierarchy: <ul style="list-style-type: none"> • Users may only select administrations for which they are assigned. • The Division choices display only divisions within the selected Administration. • The Inquiry Type choices display only Inquiry Types within the selected Administration/Division.
1005	The system saves the date/time and user for all activities associated with a POI or an OCA.
1006	The system displays a history for all activities associated with a POI or OCA.
1007	The system tracks all activities by a user for reporting purposes (to show all activities by a selected user for a selected period of time).
1008	POI notes track special handling events, research, or other events associated with a POI/OCA. Active POI notes are considered a data source that requires investigator review when new background checks are processed for the POI.
1009	Investigator will select the type of POI note using drop down list
1010	Investigator can select pre-defined notes through a drop-down list or to add custom notes.
1011	POI notes can be sorted by type.
1012	POI notes can be hidden.
1013	When a POI note is created, the current OCA # is tracked.
1014	Entity notes are not displayed to BCCU users.
1015	BCCU POI/OCA notes are not displayed to entity, audit, DOH, or oversight users.
1016	BCCU will have system tools to manage POI Note and Source Information Entry drop down-lists and system-generated merge text
1017	Notifications that have next steps will include a link to the next step within the Notification Detail.
1018	If there is an interim fingerprint result, and a date received then display “Fingerprint Appointment” form with the following fields populated by data in system: BCCU Account Number, Applicant Name, Address (Mailing Address), BCCU Inquiry ID/OCA Number, Date of Birth, Daytime Phone.
1019	Private Home Care Agency, Adult Family Home, and Assisted Living Facility accounts are

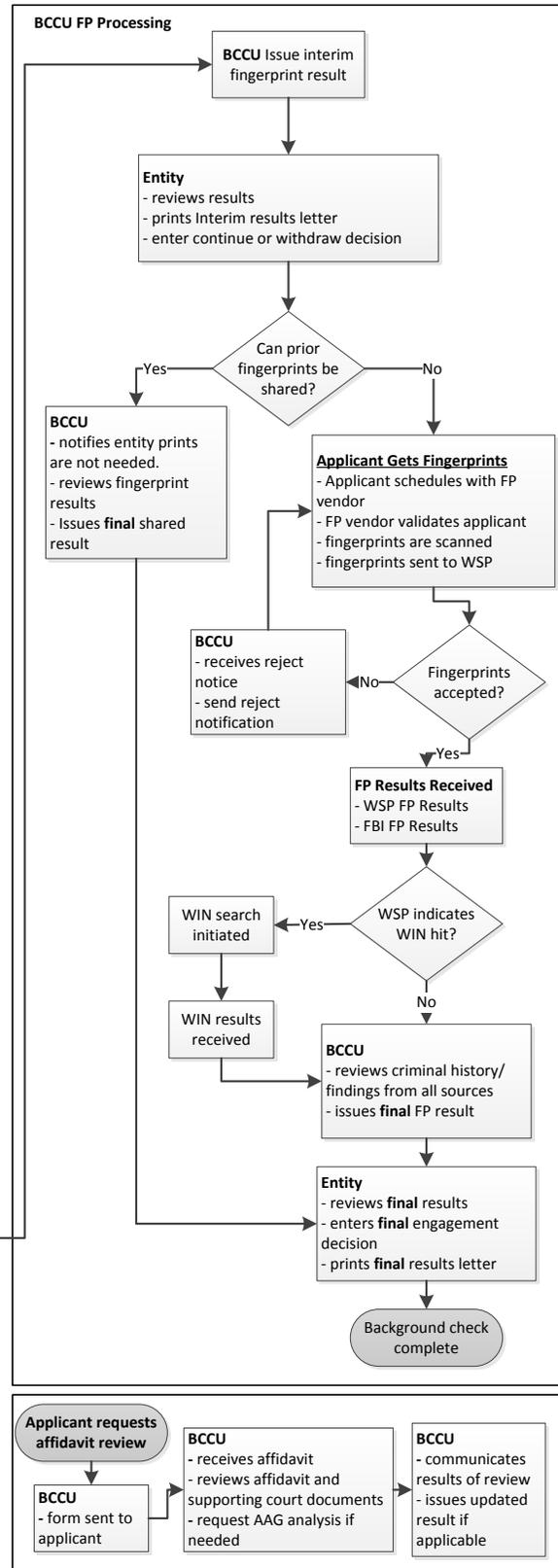
Business Rules Table 6.1 – General/Global Business Rules	
BR#	Rule Description
	limited to one fingerprint check per applicant.
1020	Private Home Care Agency Accounts are prohibited from submitting name/date of birth background checks.
1021	Only authorized accounts can submit a fingerprint-based background check.

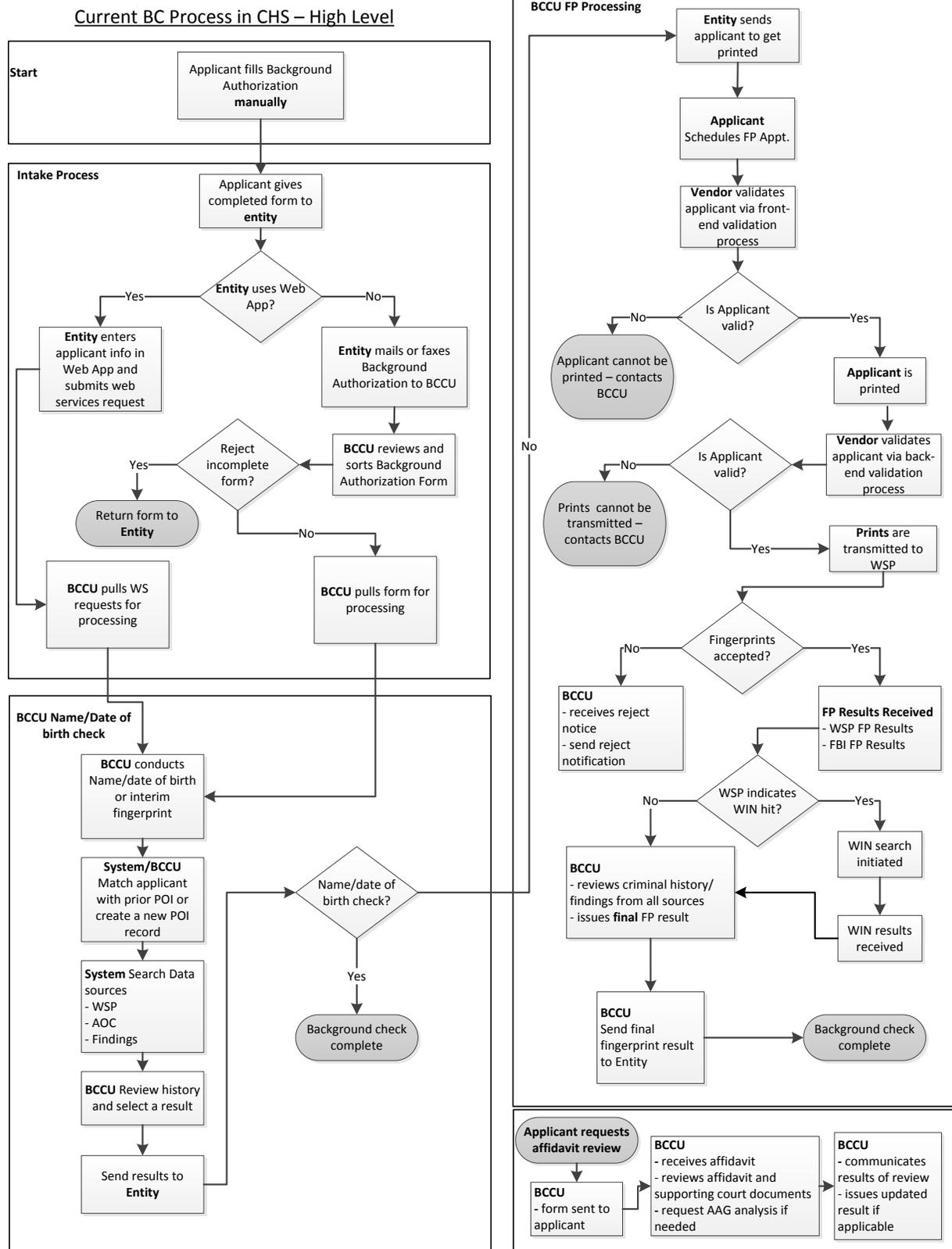
Supporting Documents Table 6.1 – General	
The following supporting documents will be provided to the successful vendor at time of requirements verification:	
Name	Location
Audit Example	Appendix AA
Inquiry Type Table Crosswalk	Appendix L

Future Background Check Process in BCS – High Level



Updated 05/26/2015





6.2 Online Applicant Form

This section describes the functional requirements, business rules and work process flow for creation of an Online Applicant Form. The Online Applicant Form will limit workload impact to DSHS and external entity users by providing a method for the background check applicant to access a web-based application, enter the required information, verify entered information, and print a Background Check Authorization Form with information populated. The Online Applicant Form will save applicant data to the Background Check System database and assign unique form ID # for retrieval of applicant information at the time a background check application is submitted by the entity.

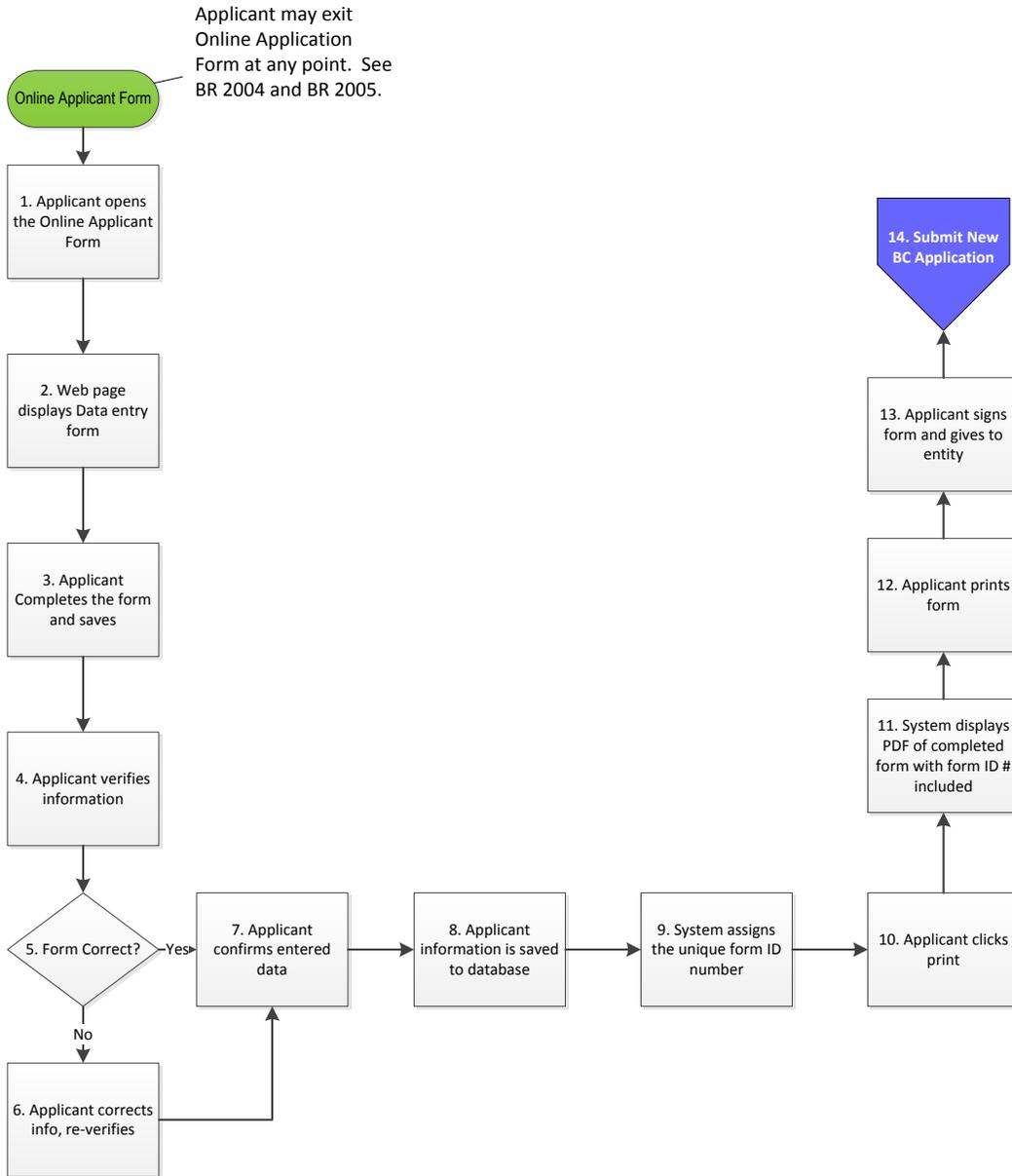
Requirements Table 6.2 – Online Applicant Form		
Requirement Type (F/NF)	Requirement Number	Function/Feature - Requirement
F	2.1	Provide a web-based method for the background check applicant to enter applicant information and print the Background Check Authorization Form.
F	2.2	Include all the necessary fields to complete the applicant information section of the Background Check Authorization Form.
F	2.3	Incorporate data entry rules such as required fields, input validation, date pickers, drop-down lists, etc.
F	2.4	Incorporate predefined business rules such as WA driver's license validation rules, birth date validation rules, and crime disclosure rules.
F	2.5	Include unlimited text fields for the applicant to explain self-disclosed crimes and pending charges.
F	2.6	Provide a method for the applicant to review and correct entered information before it is permanently saved in the system.
F	2.7	Capture and store applicant data for retrieval into the background check system.
F	2.8	Assign a unique identifying confirmation number to each set of applicant data saved in the system that will be used to retrieve applicant data at the time an entity submits a new background check request.
F	2.9	Produce a printable PDF of the DSHS Background Authorization Form in the current official version populated with applicant information and confirmation number. Create supplemental pages to display self-disclosure and alias name details that include confirmation number and applicant name and date of birth.

Business Rules Table 6.2 - Online Applicant Form	
BR#	Rule Description
2000	Uses the same format and data entry rules as the Submit New Application data entry page.
2001	Applicant accesses the form via the Public Landing Page.
2002	Saving the data will create a unique, 8 digit, alpha-numeric Confirmation Number.

Business Rules Table 6.2 - Online Applicant Form	
BR#	Rule Description
2003	The Print Button will create a PDF of the Official DSHS form with the applicant information populated and confirmation number. Will also produce a second page with the applicant Name/DOB and any self disclosure information (including the descriptions).
2004	The applicant may exit the Online Applicant Form from any screen.
2005	The applicant cannot retrieve their saved data after leaving the Online Applicant Form. If the applicant exits the Online Applicant Form prior to printing the completed Background Check Authorization form, they must re-enter their data.

Supporting Documents Table 6.2 – Online Applicant Form	
The following supporting documents will be provided to the successful vendor at time of requirements verification:	
Name	Location
Background Check Authorization Form	Appendix A
Applicant Data - Field Validation Rules	Appendix B

Future State - Online Application Form Workflow



6.3 Submit New Background Check Application

This section describes the functional requirements, business rules and work process flow to enable authorized entities to create a new background check application and submit the background check request to the Background Check Central Unit through a web-based solution. The entity will have the ability to check the Office of Inspector General registry and log the result of the check.

Requirements Table 6.3 – Submit New Background Check Application		
Requirement Type (F/NF)	Requirement Number	Function/Feature - Requirement
F	3.1	The system must provide a web-based method for entity users to initiate a background check request.
F	3.2	Allow the requesting user to retrieve applicant information previously entered using the online applicant information function or to enter applicant information into a data entry screen.
F	3.3	Require the requesting user to confirm receipt of a complete/signed Background Authorization Form or Consent Form.
F	3.4	Provide a method for requesting users to track the status of submitted background checks.
F	3.5	Require the user to indicate the type of background check - fingerprint check or Name/DOB check. Exception: when the BCCU account is limited to Name/DOB or fingerprint checks, the system will default to the applicable background check type.
F	3.6	Require the requesting user to record the applicant type. The applicant type will be a predefined list associated with the inquiry type.
F	3.7	Allow the requesting user to discontinue the background check up to a certain point.
F	3.8	The entity data entry screen for capturing applicant information will have the same the same data entry and validation rules as described in Req. 2.2 through 2.5.
F	3.9	The system must provide the capability for the requesting user to perform a pre-check of the Office of Inspector General and log the results prior to submitting the background check to BCCU for processing.
F	3.10	Provide the capability to search OIG registry using name, date of birth, and alias names and return a list of matching names.
F	3.11	Allow the user to view matching records retrieved through the registry.
F	3.12	Require the user to log the results of a registry pre check (whether the applicant appears in the registry) or indicate that a registry check is not required for the applicant.
F	3.13	Require the user to make a continue/withdraw decision after the registry pre-check.
F	3.14	Prevent the requesting user from submitting the background check application to BCCU unless the pre-check is complete and a continue/withdraw decision has been made.
F	3.15	Retain and make available for viewing the history of registry pre checks for the applicant.
F	3.16	Provide a method for recording the reason the background check was discontinued, such as applicant withdrawing from process or entity withdrawing applicant from consideration

Requirements Table 6.3 – Submit New Background Check Application		
Requirement Type (F/NF)	Requirement Number	Function/Feature - Requirement
		(such as due to disqualifying information.)
F	3.17	If one or more applicant self-disclosure questions have a “yes” response, require the user to make a continue/withdraw decision prior to submitting the background check request to BCCU for processing.
F	3.18	Provide a method to exclude certain inquiry types from the requirement to do a registry pre-check.
F	3.19	Assign a unique OCA# to each new background check application created.
F	3.20	Provide a review page for entity user to review and correct application information before submitting to BCCU for processing.
F	3.21	Associate the applicant to the entity submitting the background check.
F	3.22	Provide the capability to search for applications and entity information for the applicant such as a record of background check requests, background check results, pre-check history, applicant profile, and engagement decisions.
F	3.23	Provide a method for the entity to record the engagement decision for the applicant.
F	3.24	Provide a modified application data entry screen to allow users for an APS Inquiry Type to submit a background check request with limited applicant information (current first and last name, date of birth)
F	3.25	Provide a method for the entity to associate a secondary entity to a new background check application.
F	3.26	Provide the capability to save an incomplete background check application and return to complete at a different time.

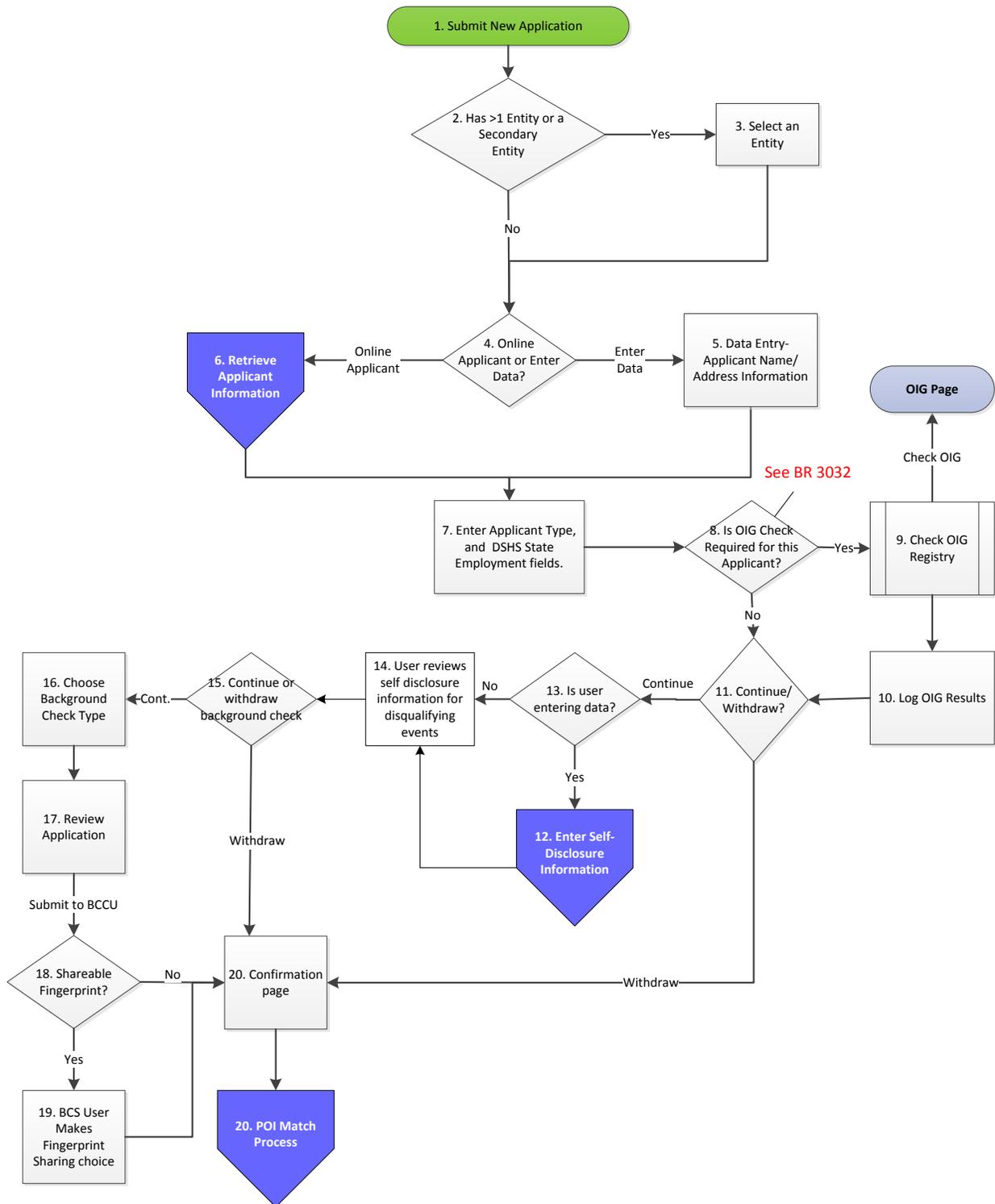
Business Rules Table 6.3 – Submit New Background Check Application	
BR#	Rule Description
3000	If the user has access to more than one Entity account, the user must designate which primary entity account is associated with the new background check application.
3001	The application will always be submitted under the BCCU account for primary entity. Secondary Entities do not submit applications.
3002	If the Confirmation Number/DOB entered do not match a Online Applicant Form, display message: "The Confirmation Number and Date of Birth entered cannot be matched to an application. Verify you have entered the Confirmation Number and Date of Birth exactly as they are printed on the Background Check Authorization form."
3003	If Applicant Information is retrieved from the Online Application Form, display the retrieved applicant data as read only. The entity user may not edit the retrieved data.
3004	If the driver’s license state is WA, enforce the following validation rules: 1. Format check using this Regular Expression – [a-zA-Z*\]{7}[0-9]{3}[a-zA-Z][a-zA-Z0-9] a. 12 characters in length (Ex: TESTERAB421AP) b. First seven characters are alpha (TESTERAB) c. Characters 8 – 10 are numeric (421)

Business Rules Table 6.3 – Submit New Background Check Application	
BR#	Rule Description
	d. Character 11 is alpha (A) e. Character 12 is either alpha or numeric (P) 2. Validate against Birth year: the values in the 8-9 position of driver’s license + the last 2 digits in the birth date year = 100 a. Following the above example, the Birth date year must be 58 for the driver’s license to be valid as the numbers in the 8-9 position is 42 (58 + 42 = 100).
3005	If the inquiry type is a Name/DOB only type or a fingerprint only type, the options for indicating the type of background check will be pre-populated and may not be edited.
3006	When the applicant answers Yes to: Have you lived in any state or country other than Washington State within the last three years (36 months)? <u>and</u> the inquiry type is set to enforce 3-year residency rule, the system will require a new fingerprint check. Name/DOB check will not be allowed. Shared fingerprint check will not be allowed.
3007	Inquiry types must have fingerprint authority to apply the 3-year residency rule.
3008	When the 3-year residency rule is enforced, the system will default to type of check: fingerprint. The system will display the following message next to the type of check: A fingerprint check is required for this applicant.
3009	The Applicant Type field follows rules defined in the Applicant Type Lists and Applicant type by Inquiry Types documents.
3010	If the application is a State Employee Inquiry Type, display the DSHS State Employment section. Otherwise, the section is hidden.
3011	Appointment type dropdown options include: Acting, Non-Permanent (Includes On-call), Volunteer, Work Study, Student Internship
3012	The system sends the Applicant Name and Aliases to the OIG Registry.
3013	At the point in the process where a continue or withdraw decision is required, the continue or withdraw selection must be made before the process can continue.
3014	The response to “Would you like to continue or withdraw this background check?” determines the application status when the application saved: a. “I intend to continue the background check.” sets status to "Data Entry" or “Verify Information” depending on if the Self Disclosure section is complete. b. “I am withdrawing this background check.” sets status to “Withdrawn”. c. “The applicant withdrew the background check.” sets status to “Withdrawn”.
3015	The user may save an application in an incomplete state to be finished and submitted to BCCU in a later session. Save will save the current state of the page.
3016	When the criminal history self-disclosure questions are answered "yes", the user will be required to enter crime details and provide a description of the action. Criminal History SD questions = Have you ever been convicted of a crime and Do you have any charges pending against you for any crime (11A and 11B on Background Check Authorization form)
3017	If the self-disclosure question for crime conviction is answered “yes”, the user will be required to list crime details that include crime name, degree, state, conviction date in mm/dd/yyyy format, and provide a description of the actions that led to the conviction.
3018	If the self-disclosure question for pending charge is answered “yes”, the user will be required to list crime details that include crime name, degree, and state and provide a description of the actions that led to the pending charge.
3019	An applicant may have multiple pending charges or crime convictions to disclose.
3020	When entering crime name, the user will have the option of choosing the crime name from a

Business Rules Table 6.3 – Submit New Background Check Application	
BR#	Rule Description
	drop-down list or entering a crime name.
3021	When the user chooses “crime not in list” from crimes list dropdown, the crime name and degree fields will be active and the user will enter a crime name and degree. The system will prompt the user: “If the crime does not appear on the list, please enter the crime”.
3022	The crimes list in the dropdown will be managed by a system tool and is pre-populated with the Common Crimes List.
3023	The “description” data entry box for pending charge and crime conviction questions will be a free text field with unlimited characters.
3024	Crime degree text box is required if user chooses to enter a crime name. The user will have the option of entering “none” for crimes with no degree.
3025	Clicking "Add a Crime" or "Add a Pending Charge" adds another set of fields for entering additional crimes/pending charges.
3026	An incoming application (OCA) is not associated with a person of interest in the database until the application is submitted to BCCU and the automated or manual POI matching process is complete.
3027	If Inquiry type is APS, Enter New Application page will have the following required fields: First Name, Last Name, and Date of Birth.
3028	If Inquiry type is APS, Enter New Application page will have the following optional fields: Middle Name, Social Security Number.
3029	If Inquiry type is APS, the following applicant information is <u>not</u> collected on the Enter New Application page: Retrieve applicant data from Online Applicant Form, other names used, photo ID information , address, mailing address, previous address, DSHS state employment, OIG check, continue/withdraw background check, applicant self-disclosure, applicant type.
3030	If Inquiry Type is APS, the Review Applicant Information Page will only include: First Name, Middle Name, Last Name, Social Security Number and Date of Birth.
3031	Once an application has been submitted to the BCCU The Applicant Profile cannot be edited other than the applicant phone number and email.
3032	The entity requesting the background check determines if the OIG check is required for the applicant. If an OIG check is not required, the entity user must indicate an OIG check is not required for the applicant. If an OIG check is required, the entity user must log the results of the OIG check.
3033	If any of the self-disclosure questions have a “yes” answer, the user must review the self-disclosure for disqualifying events and make a decision to withdraw the background check or continue the background check.

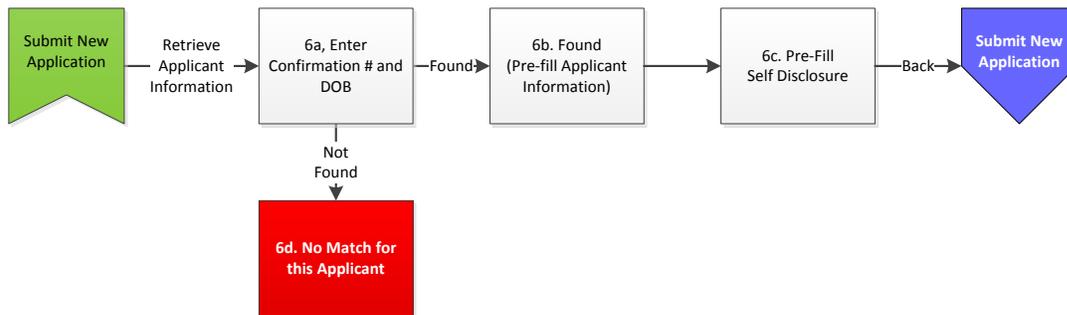
Supporting Documents Table 6.3 – Submit New Background Check Application	
The following supporting documents will be provided to the successful vendor at time of requirements verification:	
Name	Location
Applicant Type Lists	Appendix C
Applicant Type by Inquiry Types	Appendix D
Common Crimes List	Appendix E

Future State - Submit New Application

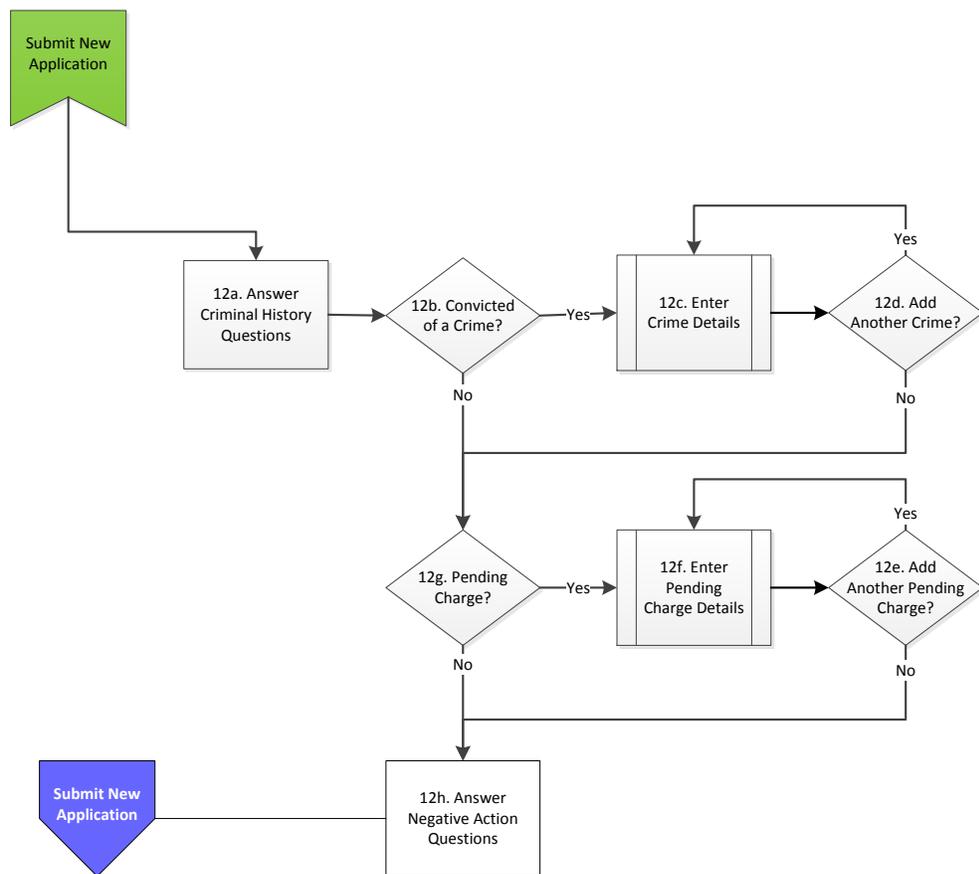


Updated 06/24/2015

Future State – Entity Retrieve Online Applicant Information Sub Process

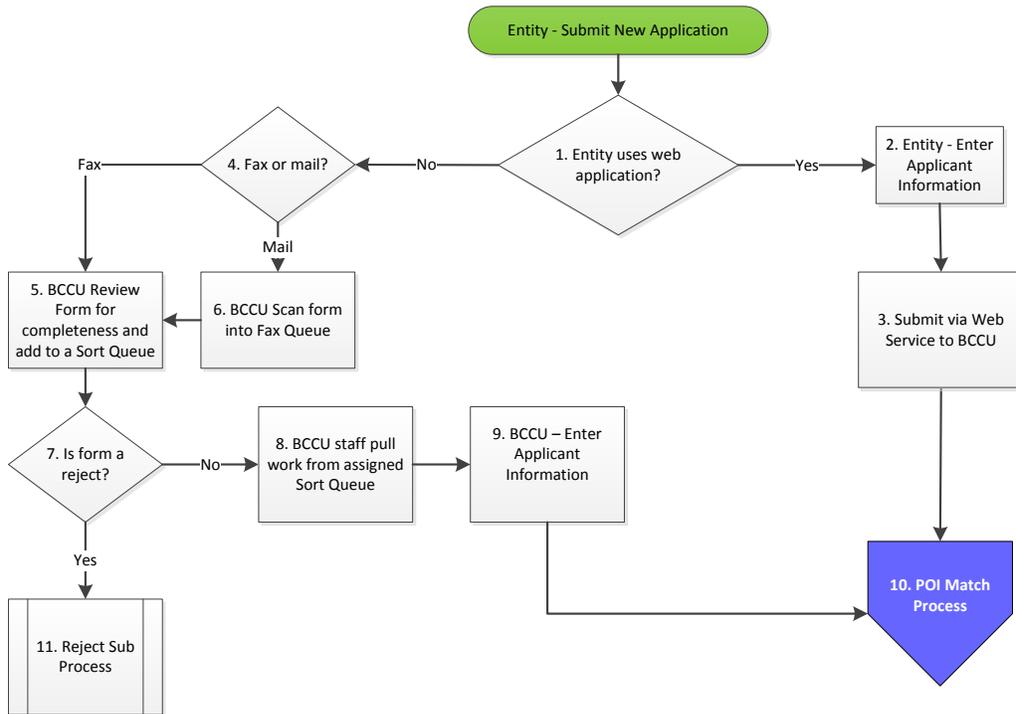


Future State – Entity Enter Self-Disclosure Sub Process

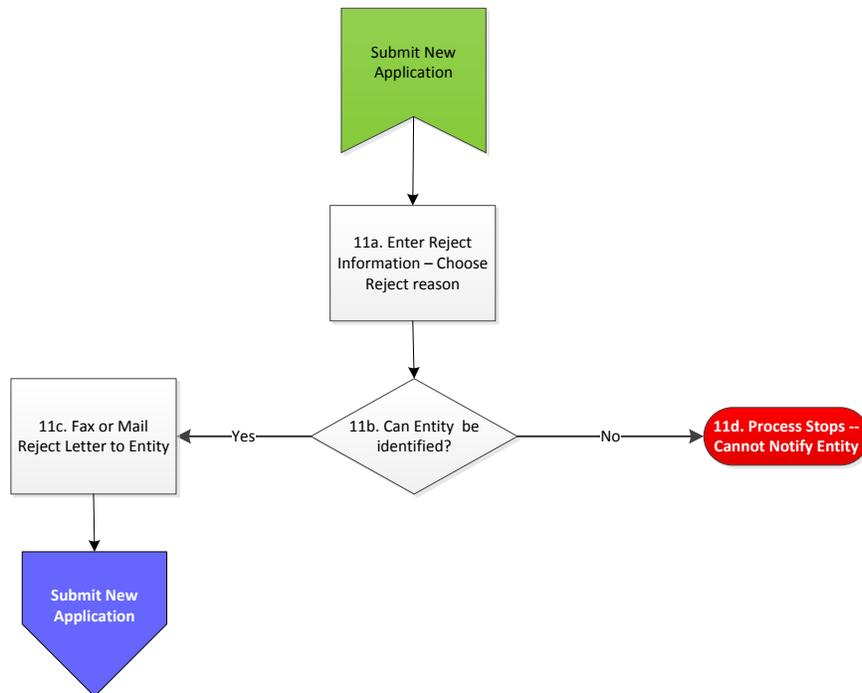


Updated 06/24/2015

Current State - Submit New Application



Current State – Reject Sub Process



Updated 06/01/2015

6.4 Match Person of Interest Records

A person of interest record is the primary record set for every person who has completed a background check through the Background Check Central Unit. This section describes the requirements, business rules and process for determining whether to match incoming applications to an existing person of interest or to create a new person of interest record. Each person of interest has a unique identifying number in the Background Check System database.

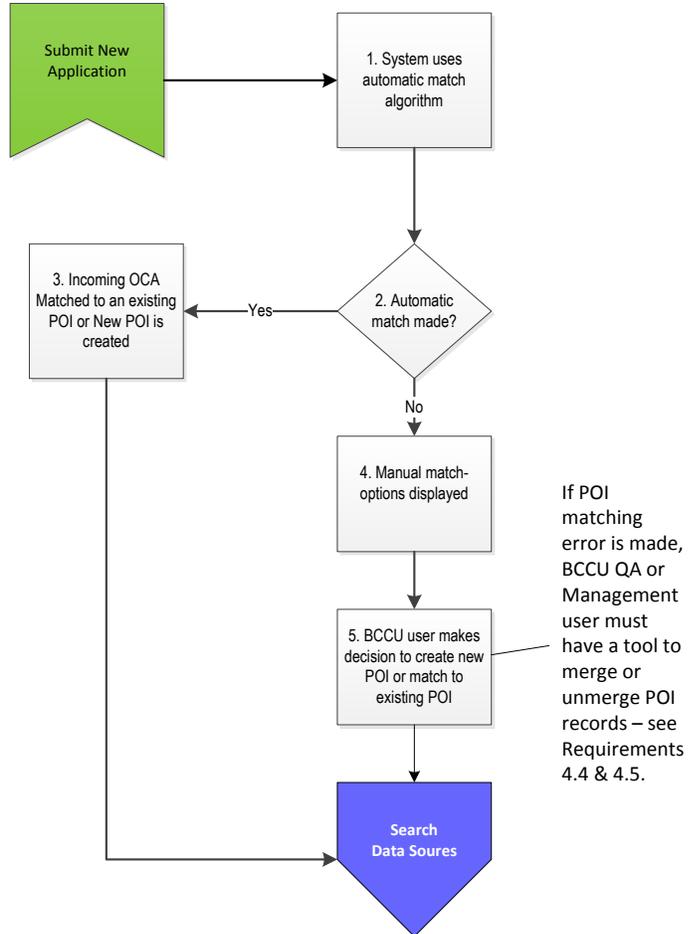
Requirements Table 6.4 – Match Person of Interest Records		
Requirement Type (F/NF)	Requirement Number	Function/Feature - Requirement
F	4.1	Apply an automated procedure that when conditions are met automatically matches an incoming application to an existing person of interest record, creates a new person of interest record, or requires BCCU user to make a manual POI match.
F	4.2	Compare applicant name and date of birth information to existing database records to determine if a person of interest (POI) record exists in the system.
F	4.3	Provide a method for BCCU user to match POI records or create new POI records when the stored procedure requires manual match.
F	4.4	Ability to merge person of interest records when BCCU user determines multiple POI records exist for the same person.
F	4.5	Ability to unmerge person of interest records when POI was merged in error.

Business Rules Table 6.4 - Match Person of Interest Records	
BR#	Rule Description
4000	A Social Security Number cannot be required as a method for matching incoming applicant records to existing database records.
4001	When an applicant is an exact match to an existing person of interest record, the system automatically matches the applicant to the person of interest (POI) record.
4002	The applicant is an exact match to the existing POI record if there is an exact match to an existing person of interest for the applicant's SSN, first name, last name, middle name, and date of birth, AND there is only one matching record.
4003	When there is no SSN, the applicant is an exact match to the existing POI record if there is an exact match to an existing person of interest for the applicant's first name, last name, middle name, and date of birth, AND there is only one matching record.
4004	If there is no match to ALL of the applicant info (SSN, first name, last name, middle name, and date of birth), the system automatically creates a new person of interest record.
4005	If the applicant information is not automatically matched to an existing POI record or if a new POI is not automatically created, BCCU User must review potential matches and either match to an existing POI record or create a new POI record.
4006	When a manual match is required, the system provides a list of possible matches for BCCU User to match to.

Business Rules Table 6.4 - Match Person of Interest Records	
4007	When a manual POI Match is made and there is no existing SSN, but there is an incoming SSN, the system adds the incoming SSN to the POI record.
4008	When the BCCU User manually matches an incoming applicant to an existing POI and the incoming name is different than the existing POI name, the incoming name becomes the primary name for the POI and the existing name becomes an alias.
4009	When the user is viewing possible POI matches, the user can choose to either create a new POI record or match the applicant to an existing POI record.
4010	The automated POI Matching process begins once the entity submits the application to BCCU.
4011	The system must use the rules documented in the referenced stored procedure for the POI Matching.
4012	When a manual POI Match is made and an existing SSN does not match the incoming SSN, the system should overwrite the existing POI SSN with the incoming SSN.
4013	When a manual POI Match is made and the incoming SSN is blank, but there is an existing SSN, retain the existing POI SSN.
4014	BCCU users will be the only users allowed to do the matching with POI or create new POI.
4015	When the incoming SSN matches an existing SSN but the BCCU User determines the Name/DOB are not a match, the BCCU User clears the incoming SSN and either creates a new POI or matches to an existing POI.

Supporting Documents Table 6.4 – Match Person of Interest Records	
The following supporting documents will be provided to the successful vendor at time of requirements verification:	
Name	Location
POI Matching – with Stored Procedure	Appendix F

Future State – POI Matching
(Same as Current State)



Updated 06/25/2015

6.5 Search Data Sources

This section describes the requirements, business rules and process for searching the various internal and external data sources used to complete background checks through the Background Check Central Unit, fingerprint sharing, and the process for completing an automated Name/DOB no record result.

Requirements Table 6.5 – Search Data Sources		
Requirement Type (F/NF)	Requirement Number	Function/Feature - Requirement
F	5.1	Ability to perform an integrated search of multiple internal and external data interfaces and internal database records on a person of interest using name/date of birth/alias name search criteria described in Data Sources and Automated No Record Document.
F	5.2	Ability to search data sources and return a list of possible matches for each of the following data sources: Washington State Patrol WATCH, Administrative Office of the Courts public data mart, internal findings data from AL TSA Adult Protective Services Registry, AL TSA Resident and Client Protection Program, CA Child Protective Services, Department of Health Licensing Data.
F	5.3	Ability to perform an automated process to determine when the criteria for automated no record return is met.
F	5.4	Automatically produce and distribute to the background check requester a Name/DOB or interim fingerprint no record result when the automated no record criteria is met.
F	5.5	Ability to use stored rap sheets, manually entered source information, and applicant self-disclosure information that is associated with a person of interest as a source of data for future background check submissions.
F	5.6	Ability to receive criminal history records from the Washington State Patrol WATCH web service and Administrative Office of the Courts data mart and populate the applicable rap sheet template.
F	5.7	Implement a series of fingerprint sharing rules to avoid unnecessary duplicative fingerprint checks. Sharing rules include specific rules for when fingerprints can/cannot be shared across inquiry types and for specific date ranges and when prior fingerprint results can be used to complete subsequent background checks.

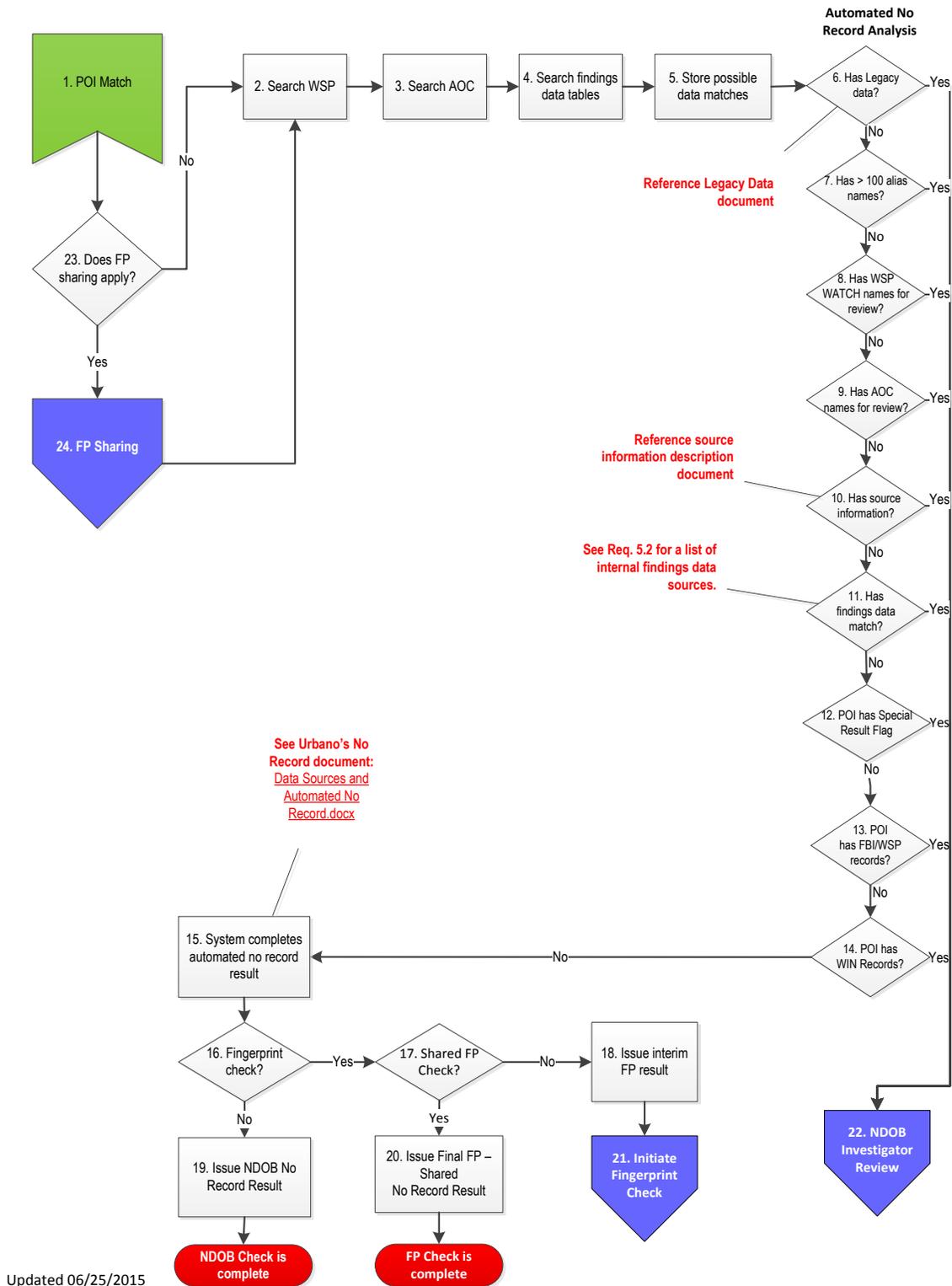
Business Rules Table 6.5 – Search Data Sources	
BR#	Rule Description
5000	Data Source search cannot be initiated until FP sharing decision is made.
5001	All data sources are searched and possible data matches are stored in the database prior to Automated No Record analysis.
5002	System sends search info to WSP WATCH via web service.
5003	System searches AOC data warehouse via linked SQL server.
5004	Findings data sources are APS, CPS, RCPP findings and DOH licensing actions.

Business Rules Table 6.5 – Search Data Sources	
5005	If any point in the automated no record analysis fails (FS Search Data Sources Process Flow Box 6-14 = Yes), the inquiry (OCA) is not eligible for an Automated No Record result.
5006	When the possible alias name combinations for WSP WATCH exceed 100, OCA cannot go through automated no record return.
5007	When WSP WATCH returns one or more possible matches for POI, OCA cannot go through automated no record return.
5008	Source Information is reportable background check information that is entered into the background check system and associated with the POI record. POI information is reported as part of the background check result.
5009	An OCA is not eligible for Automated No Record return when the POI has reportable source information.
5010	The automated no record analysis does not fail for hidden (inactive) source information (self-disclosures, court entries, etc.) or rap sheets.
5011	Findings information from Department of Health, ADSA APS, ADSA RCPP, and CA CPS is limited to an indicator that the individual has a founded finding -- specific information regarding the finding is not included.
5012	If findings data search returns one or more possible findings matches, OCA cannot go through automated no record return.
5013	CA findings data contains names w/DOB of 01/01/1900 – Name/DOB combinations with 01/01/1900 birth date are invalid. Filter out Name/DOB combinations with a 01/01/1900 birth date and do not include as possible matches to POI. Note: The name search criteria provided in Data Sources and Automated No Record document does not enforce this rule - it must be enforced in new system.
5014	If POI is flagged for special result, OCA cannot go through automated no record return.
5015	WSP/FBI record – the OCA is not eligible for automated no record return if the most recent FP OCA for the POI (in progress or finished) has a WSP Record or FBI Record result. Exception: FP Checks conducted under Inquiry Types using ORI WA027A15C, WA021015C, WA034025Y, or WA034019T are not considered as part of the Automated No Record Return analysis.
5016	WIN record – the OCA is not eligible for the automated no record return process if: 1) an in progress FP check for the POI has a WIN hit; or 2) a finished FP check for the POI has WIN Record results from any one or more of the WIN States. Exception: FP Checks conducted under Inquiry Types using ORI WA027A15C, WA021015C, WA034025Y, or WA034019T are not considered as part of the Automated No Record Return analysis.
5017	If OCA is eligible for automated no record result and background check type is Name/DOB, system issues Name/DOB no record letter.
5018	If OCA is eligible for automated no record result and background check type is fingerprint and FP sharing decision is yes, system issues final fingerprint - shared no record letter.
5019	If OCA is eligible for automated no record result and background check type is fingerprint and OCA is not a shared fingerprint, system issues interim fingerprint no record letter.
5020	OIG check is not a data source used in BCCU background check. BCCU investigator will not see the results of the OIG check as part of the investigator review.
5021	Fingerprint sharing is a process for using a prior FBI record or FBI no record result received from the FBI for a completed OCA to complete a new fingerprint request for a POI.
5022	Entities within the fingerprint sharing group may use (share) prior fingerprint rap sheets from a previous OCA to complete a new fingerprint OCA when the fingerprint sharing conditions are met.

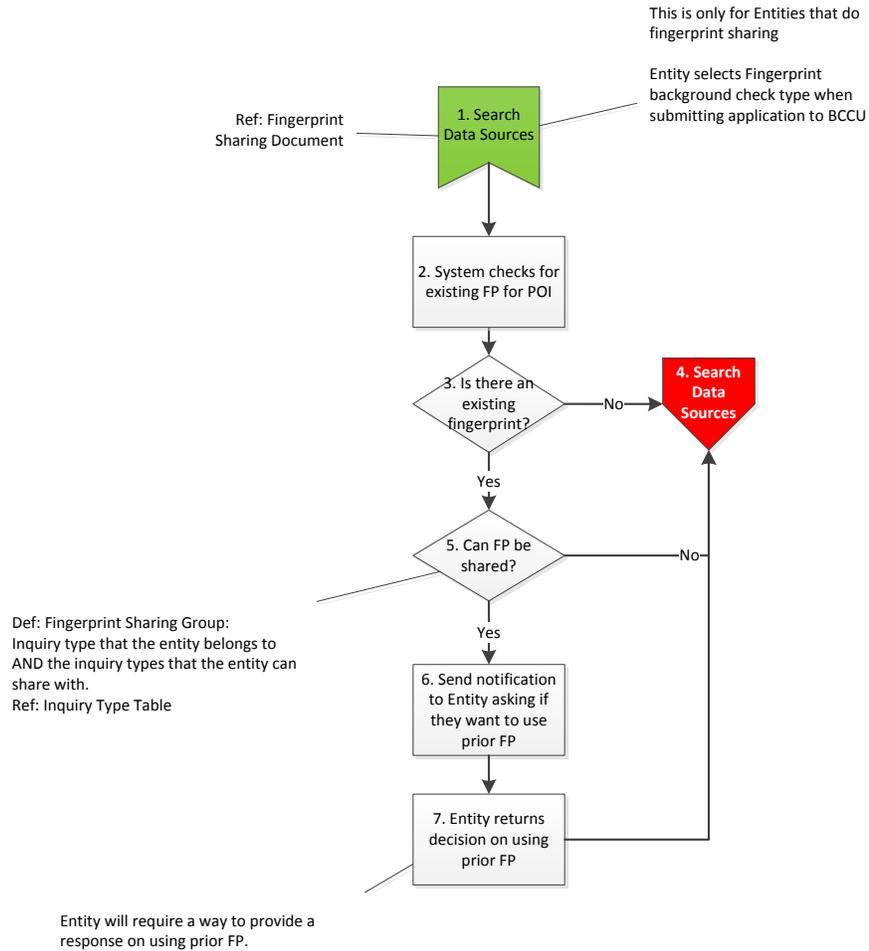
Business Rules Table 6.5 – Search Data Sources	
5023	Fingerprint sharing group is based 1) the participating inquiry types and, 2) the inquiry types for the source of the prior fingerprint rap sheet.
5024	To be eligible for fingerprint sharing, prior FP must be for a source FP inquiry type and have been completed within the last three years.
5025	Only entities with an inquiry type that is part of the FP sharing group are allowed to use prior fingerprint results.
5026	When fingerprint sharing criteria are met, the system will notify the entity user that the applicant has a prior fingerprint check that may be used. The fingerprint sharing notification will include the date of the prior fingerprint background check.
5027	When fingerprint sharing criteria are met, the user will be required to make a decision to use the shared fingerprint or request a new fingerprint check.
5028	When entity indicates decision to share prior FP, system runs Name/DOB data sources to determine if applicant is eligible for automated no record return.
5029	If shared FP is eligible for automated no record return, system issues final fingerprint - shared no record result. (See BR on re not issuing interim)
5030	If shared FP is not eligible for automated no record return, the system moves OCA into BCCU User review
5031	When a shared FP is in investigator review, the system will indicate OCA is a shared FP and will "present" the prior rap sheet that must be reviewed.
5032	An interim result is <u>not</u> issued for OCA's designated as shared fingerprint. The only letter issued is final fingerprint - shared.
5033	Result letter type will indicate Final FP – Shared and list the result such as no record, record, etc.
5034	When the fingerprint is shared, the system will insert FP sharing merge text in the Final fingerprint result letter.
5035	BCCU will have a system tool to manage FP Sharing permissions at the inquiry type level.

Supporting Documents Table 6.5 – Search Data Sources	
The following supporting documents will be provided to the successful vendor at time of requirements verification:	
Name	Location
Data Sources and Automated No Record Document	Appendix G
WATCH and AOC Name Search Technical Summary	Appendix H
Source Information Document	Appendix I
Fingerprint Sharing Description	Appendix J
Inquiry Type Table	Appendix L

Future State – Search Data Sources

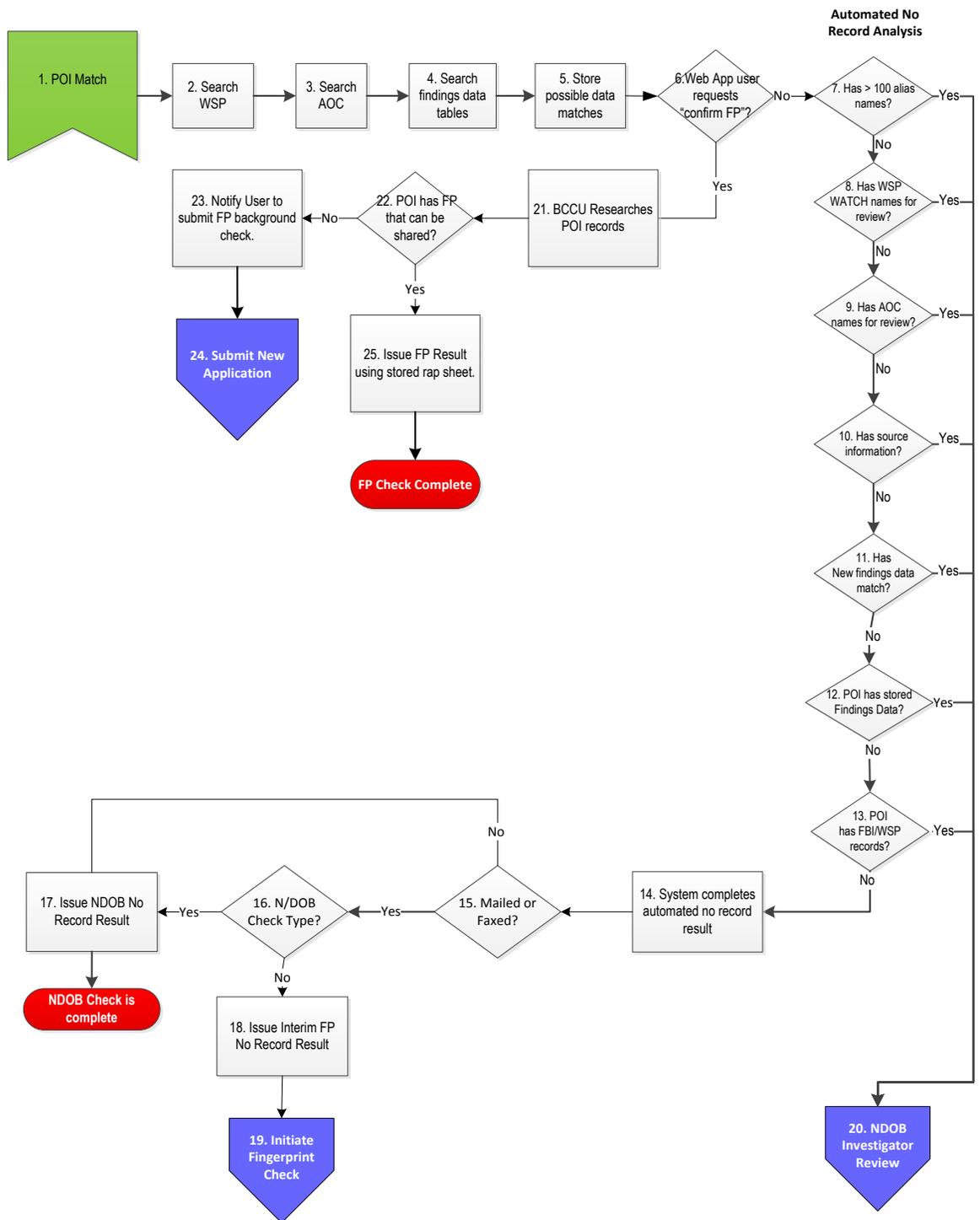


Future State – Fingerprint Sharing



Updated 06/08/2015

Current State – Search Data Sources



Updated 06/02/2015

6.6 Investigator Review and Determine Results

This section describes the requirements, business rules and process for Investigators (BCCU user) in the Background Check Central unit to review background check data returned for the person of interest, match a person of interest to possible data hits when more than one possible match exists, and determine and choose the background check result.

Requirements Table 6.6 – Investigator Review		
Requirement Type (F/NF)	Requirement Number	Function/Feature - Requirement
F	6.1	Return a list of possible matches from all data sources (internal and external) in a consolidated view.
F	6.2	Provide a method for BCCU users to choose matching criminal history records and attach them to the OCA or POI as applicable.
F	6.3	Provide a method for BCCU users to initiate special handling events such as legal reviews in the background check processing workflow.
F	6.4	Provide the ability to initiate a thumbprint request when a positive Name/DOB match to Washington State Patrol records cannot be determined by BCCU user.
F	6.5	Provide a summary of data search results indicating when a data source has information to review, no hit, or requires a match to possible hits.
F	6.6	Retain a history of the results of data search and provide a method for BCCU user to view the Name/DOB/alias combinations searched for each data source and the possible matches returned for each data source.
F	6.7	Provide the ability for BCCU user to indicate when review steps for each data source have been completed.
F	6.8	Record and maintain a history of the results of the final fingerprint check.
F	6.9	Record and maintain a history of the results of the interim fingerprint check.
F	6.10	Record and maintain a history of the results of the Name/DOB background check.
F	6.11	Provide the ability for BCCU to choose a result type and distribute a background check result to the entity.
F	6.12	Provide the ability to flag person of interest for special result. When the POI is flagged for special result, the system will block the auto-generation of the standard result template and prompt BCCU user to use a special result template.
F	6.13	Ability to receive, track, and display the criminal and negative action records returned from each of the various data sources.
F	6.14	Associate criminal history results or negative action data with the Person of Interest (POI) and background check (OCA).
F	6.15	Provide a consolidated view of background search results for BCCU users to view and print rap sheets, self-disclosures, court documents, and other history associated with the background check.

F	6.16	Provide a means for BCCU user to record which disqualifying crimes are reported on the criminal history reports. The system will need to display the appropriate disqualifying crimes list for user to choose from.
F	6.17	Ability for the system to apply the appropriate result template based on the letters used by the inquiry type for the BCCU account, the type of background check conducted, and the result chosen by BCCU.

Business Rules Table 6.6 – Investigator Review	
BR#	Rule Description
6000	The order that data sources are listed in the Name/DOB Investigator Review high-level flow does not dictate the order in which data needs to be reviewed by the investigator.
6001	If the POI has pending legal review (AAG Review, Equivalency Review, or DOH review) or Pending WIN Hit for a different OCA, the current OCA must be placed in a hold queue until the legal review or WIN activities for the previous OCA are complete. The investigator cannot complete the current OCA until the pending analyses or WIN searches are complete.
6002	The system will search all data sources to determine which data sources require investigator review and display a summary of data search results.
6003	For each data source that requires investigator review, the summary will indicate review is needed and provide a link to the data source review page.
6004	When a data source has no information for investigator review, the summary will indicate no action required for investigator.
6005	For each data source that requires investigator review, the investigator will access the data source review page and complete the review steps for that data source.
6006	Active Court and DOC entries will display on the data source review page for investigator review. Hidden Court/DOC entries will not display.
6007	Documents associated with active Court and DOC entries will be available on the data source review page for investigator review.
6008	The investigator will review data and log disqualifying actions (crime or negative action) for the following data sources: Court/DOC, Self-disclosure, stored FP rap sheets, DOH findings, WSP WATCH, and AOC
6009	The investigator will choose the disqualifying actions from the drop-down list of disqualifying crimes associated with the inquiry type.
6010	The crimes list used to log disqualifying actions is dependent on the inquiry type associated with the entity's account#.
6011	The crimes list dropdown will be available for each data source that requires the investigator to log disqualifying action log.
6012	The investigator will be able to remove disqualifying actions from the disqualifying actions log. (i.e. Would need to be able to remove the disqualifying action if it was added in error or if the background check is being updated.)
6013	Disqualifying actions are not logged for inquiry types that receive only record/no record results.
6014	If the self disclosure is "yes" to DSHS Questions 12, 13, or 14, the system will automatically populate the disqualifying action log with the following as applicable: Answered Yes to DSHS #12 Answered Yes to DSHS #13 Answered Yes to DSHS # 14
6015	Active Self-Disclosures will display on the data source review page for investigator review.

Business Rules Table 6.6 – Investigator Review	
	Hidden self disclosures will not display.
6016	New Self-Disclosures submitted with application will be set to active status for investigator review.
6017	Self-Disclosures will be reviewed by investigator to determine if they are duplicates, need additional information, or need legal review.
6018	When the investigator determines a new self-disclosure is a duplicate, the investigator will hide the duplicate entry.
6019	For unclear WA state crime self-disclosures, the investigator will review against AOC rap sheet, JIS, or FORS, and will add note (comment) if research clarifies the SD.
6020	Prior fingerprint rapsheets are used to complete subsequent Name/DOB checks and shared fingerprint checks when certain conditions are met.
6021	When the background check type is fingerprint - shared and there is a prior WSP, FBI, and/or WIN state record rapsheet that meet the FP sharing conditions, the system will display rapsheets for review.
6022	When the background check type is Name/DOB and there is a prior WSP, FBI, and/or WIN state rapsheet that meets the conditions for using prior FP, the system will display the rapsheet for review.
6023	<p>Conditions for using Prior FP rapsheets for Name/DOB:</p> <ul style="list-style-type: none"> - Rap sheets from FP Checks conducted under Inquiry Types using ORI WA027A15C, WA021015C, WA034025Y, or WA034019T cannot be used. - Only the most recent FP with WSP record, FBI record, or WIN state record rap sheets will be displayed - No record and non-conviction rapsheets will not require investigator review - Except as noted above, DSHS and DEL Inquiry types can use prior rapsheets from either agency.
6024	The prior FP result review page will display the following information related to the original FP background check: Administration, division, inquiry type, Entity Name, OCA, completion date.
6025	If an equivalency was not requested for the rap sheet, the investigator will determine if equivalency is needed.
6026	Data review page will have a link to view stored equivalency results. The system will indicate when there are no stored equivalency results for review.
6027	POI notes document legal actions or other events that inform the investigator and may affect the background check result.
6028	Data review page will display possible DOH findings matches for POI.
6029	Investigator determines if POI is a match to DOH finding and associates the finding to the OCA.
6030	Data review page will have a link to view the results of prior DOH legal review. The system will indicate when there are no stored DOH legal reviews.
6031	When a new DOH action is reported and matched to the POI, investigator will initiate DOH legal review.
6032	Based on DOH legal review, the investigator will log if DOH action is disqualifying or a record.
6033	Data review page will display possible APS, CPS, and RCPP findings matches for POI.
6034	Investigator determines if POI is a match to APS, CPS, or RCPP finding and associates the finding to the OCA.
6035	When APS, CPS, or RCPP findings are matched to the POI, the system will automatically log the type of finding in the disqualifying action log.
6036	WSP data review page will be displayed when there are one or more possible Name/DOB

Business Rules Table 6.6 – Investigator Review	
	matches to the POI.
6037	WSP WATCH returns a list of possible Name/DOB matches with associated WSP SID#.
6038	The investigator will have the ability to view the WSP WATCH rapsheet for possible matches to assist in determining if the SID is a match to POI.
6039	The investigator may need to review more than one WSP WATCH rapsheet to determine if one is a match to the POI.
6040	If the investigator cannot determine if POI is a match to one or more SIDs, the investigator will initiate the thumbprint request. Reference Section 6.7 Thumbprint Process Requirements.
6041	If the SID is a match to the POI, the investigator will associate the rapsheet with the OCA. The associated rapsheet will become part of the background check result and be stored in the system.
6042	The investigator will review the rapsheet and may determine additional DOC (FORS) or WA Court (JIS) research is needed. See FORS/JIS Research Process flow.
6043	The investigator will review the rapsheet and may determine legal review is needed. See AAG Review and Equivalency & DOH Review flows.
6044	AOC data review page will be displayed when there are one or more possible Name/DOB matches to the POI.
6045	AOC data search returns a list of possible Name/DOB matches with associated AOC parent keys linked to AOC data rap sheet data.
6046	The investigator will have the ability to view the AOC rapsheet to assist in determining if the AOC Name/DOB and parent key is a match to POI.
6047	The investigator may need to review more than one AOC record to determine if one or more AOC parent keys are a match to the POI.
6048	If any of the AOC parent keys are a match to the POI, the investigator will associate all matching parent keys with the OCA. The associated rapsheet will become part of the background check result and be stored in the system.
6049	The system will populate the AOC rap sheet template with the combined information from all selected parent key records.
6050	The investigator must complete review of all data sources and complete all required actions for each data source before a result can be selected.
6051	The DOH, APS, CPS, RCPP Findings, WSP, and AOC data review pages will display the Name/DOB combinations searched for each data source.
6052	When the investigator determines the POI does not match one of the possible matches, the investigator will indicate no match chosen. (DOH, APS, CPS, RCPP findings, WSP, AOC)
6053	After the investigator has completed review of the data source, the data source summary will display the results of investigator review.
6054	The data source summary will display the disqualifying crimes/negative actions for each data source.
6055	The order that data sources are listed in the Final FP Investigator flow does not dictate the order in which data needs to be reviewed by the investigator.
6056	The system will search all Final FP data sources to determine which data sources require investigator review and display a summary of data search results.
6057	The Final FP data summary will display the result type from the Interim Letter (i.e. Interim No Record, Interim Record, Interim Disqualify) and provide a link to the interim background check summary page.

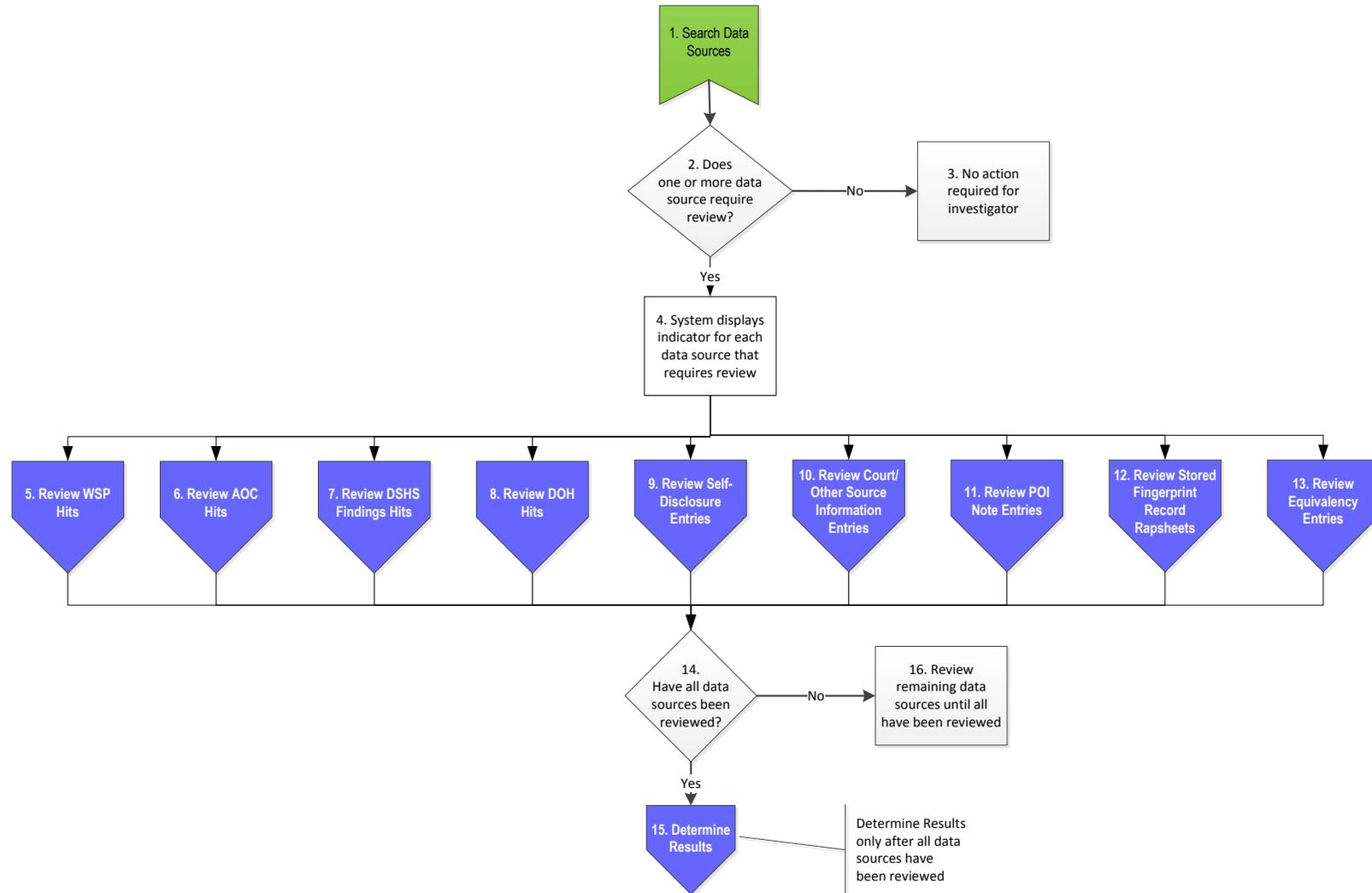
Business Rules Table 6.6 – Investigator Review	
6058	The Final FP data summary will display the WSP or FBI fingerprint result activity (i.e. WSP Record, WSP No Record, FBI Record, FBI No Record) and provide a link to the data review page if the result is a record result.
6059	If the FP result is a no record, investigator review is not required.
6060	The investigator will review the WSP or FBI Record rap sheet to determine if there are disqualifying crimes and will log disqualifying crimes in the crimes box.
6061	When investigator reviews FP record rapsheet and determines the rapsheet contains only non-conviction information, the investigator will change the FP record activity to "non-conviction".
6062	After the investigator has completed review of the Final FP data source, the data source summary will display the results of investigator review.
6063	The Final FP data source summary will display the disqualifying crimes/negative actions for each data source.
6064	All Final FP data sources must be reviewed before investigator can determine result.
6065	If additional information is needed from applicant, the investigator will generate an additional information needed letter.
6066	When investigator chooses additional information needed letter, the investigator enters a note documenting reason additional information is needed and chooses "canned" merge text from drop-down list or enters custom merge text.
6067	When the additional information needed letter is chosen, the system generates an applicant version and entity version of the letter.
6068	The applicant version of the additional information needed result will include merge text chosen/entered by investigator and all associated source information, WSP WATCH, AOC, and FP rap sheets.
6069	The entity version of the additional information needed result will not include merge text chosen/entered by investigator. Letter does not include rapsheets.
6070	When entity additional information needed letter is distributed a notification will be sent to entity indicating BCCU has requested additional information from the applicant.
6071	For inquiry types that are record/no record only, the investigator will not have the option to choose the additional information needed or disqualify letter types.
6072	All result letters have common information that is automatically inserted into the result letter template.
6073	Record and Disqualify letter types will include all associated source information, WSP WATCH and AOC rap sheets. FP rap sheets will only be distributed to entities authorized to receive FP rap sheets.
6074	The system will have a button/method for BCCU to print an applicant copy of the result letter sent to the entity.
6075	The applicant copy of the result letter will include: - Mailing slip sheet with applicant mailing address - Result letter/source information/rap sheets sent to the entity - FP rap sheets if not included in entity result.
6076	The system chooses the appropriate result letter template based on type of background check and whether the FP is in the interim or final stage of the process.
6077	When result decision is complete, the result is distributed to the entity and a notification sent. Exception: If the investigator is in quality assurance status, the OCA is placed in quality assurance review queue. See Quality Assurance flow and BRs.

Business Rules Table 6.6 – Investigator Review	
6078	When NDOB, Final FP - Shared, and Final FP results are distributed, the OCA is placed in finished status.
6079	When Interim FP result is distributed, the Fingerprint Appointment Form with applicant information is active for entity.
6080	The system populates the result letter merge text based on the result type chosen by the investigator.
6081	The source information associated with the OCA is populated on second page of the record and disqualify result
6082	When the additional information requested result is chosen by the investigator, the system will prompt the investigator to choose WIN Nevada, WIN Wyoming, or Information Request. The system will merge the appropriate text based on the selection of the investigator.
6083	When the background check is completed with an information requested result, the investigator will print the Applicant Request for Additional Information Letter. Te system will automatically generate the Entity Notification - Additional Information Needed letter and send a notification to the entity.
6084	System-generated automated no record results are not subject to QA Review.
6085	The application summary will have a link to the background check result and will indicate the type of result. (i.e. no record, record, disqualify, thumbprint, fingerprint reject, etc.)
Special Result	
6086	Special result letter is created and updated outside the system.
6087	Special result letter is imaged into the system and associated with the OCA record.
6088	When POI is flagged for special result letter, system will block automated no record return process.
6089	When POI is flagged for special result letter, system will block auto generating standard letter template.
6090	When POI is flagged for special result letter, system will prompt user to update and attach special result letter.
6091	BCCU user will record the result type (i.e. no record, record, etc.) and complete the check.
6092	System will distribute special result letter to requester along with any associated background check reports (rap sheets and reportable source information, i.e. self-disclosures, etc.). The system-generated result will not be distributed.
Source Information	
6093	Source information entries are a record of crime or negative action reported through a self-disclosure or found by the investigator when researching DOC-FORS, WA Court, or Out of State Court, or another source. Source information entries are part of the POI's background check history stored in the system and are reported on the background check result.
6094	Active (not hidden) source information entries are considered data sources that must be reviewed by the investigator.
6095	When the POI has active (not hidden) source information entries, the OCA is not eligible for automated Name/DOB no record return.
6096	When the investigator hides source information entries, there will be a method to view hidden source information entries.
6097	When the investigator hides a source information entry, they will enter a note (comment) documenting the reason for hiding the source information.
6098	Investigators do not add Self-Disclosure source information entries, and cannot edit the self

Business Rules Table 6.6 – Investigator Review	
	disclosure. The investigator may add and edit information in the Investigator comment field.
6099	Investigators add DOC-FORS, WA Court, and Out-of-State Court entries. Once the entry is saved, the investigator cannot edit it except that an investigator can edit and add to the investigator comment field.
6100	Once a self disclosure has been hidden, the QA and manager users must be able to view and unhide the hidden source information entries.
6101	Certain fields from the Source Information entry merge to the Source Information section of the record or disqualify result letter.
6102	System-generated source information merge text is verbiage that automatically merges into the source information section of the record or disqualify result letter when certain conditions are met.
6103	Legacy source information entries and system generated merge text is used for future background checks.
6104	POI notes do not print on the background check results.

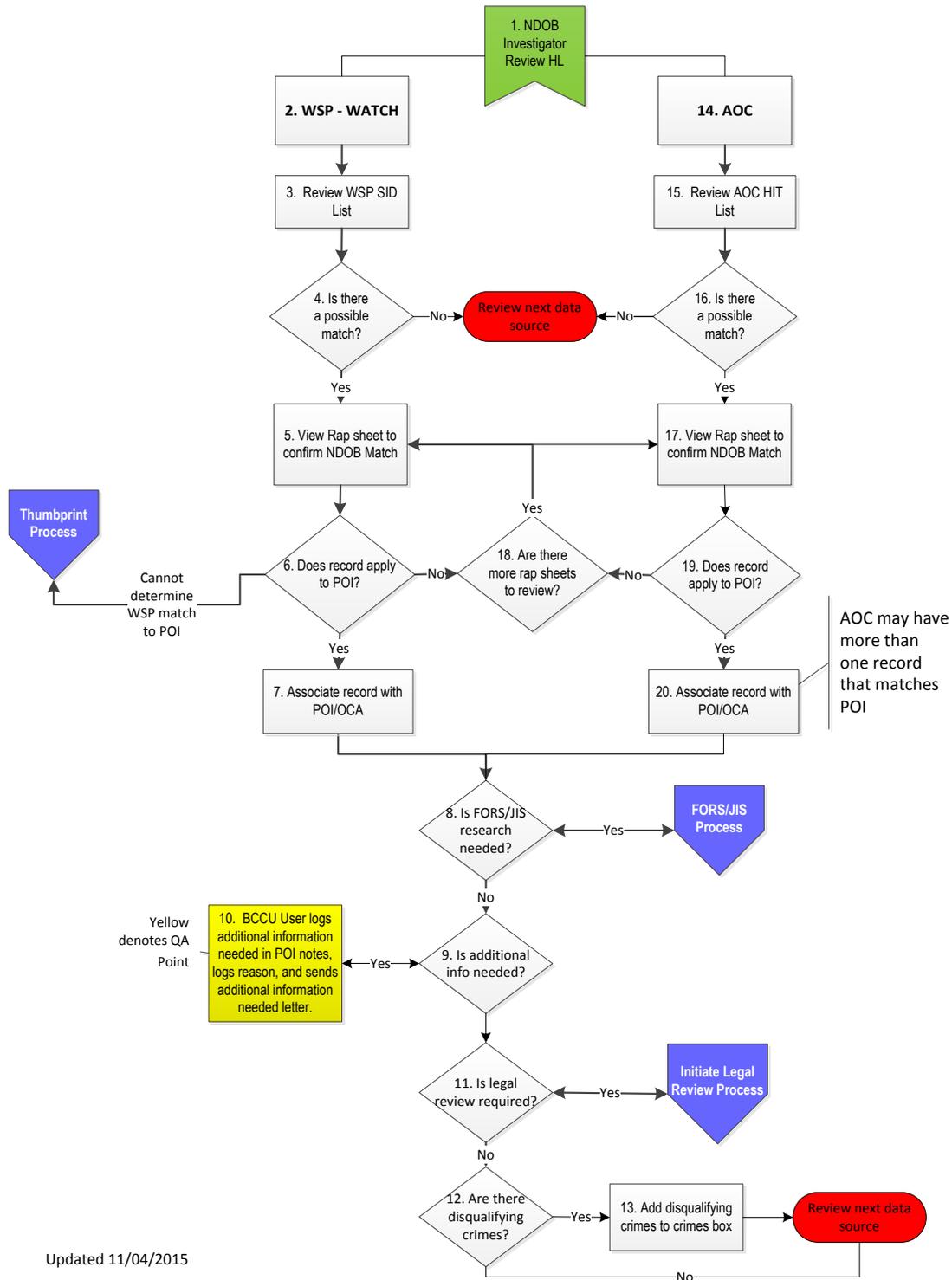
Supporting Documents Table 6.6 – Investigator Review	
The following supporting documents will be provided to the successful vendor at time of requirements verification:	
Name	Location
Source Information Document	Appendix I
Inquiry Type Table	Appendix L
Legacy Data	Appendix M
Legacy Data ER Diagram	Appendix N
Background Check Result Document	Appendix O
Statuses, Triggers, Next Steps, and Workload Queues	Appendix P

Future State – Name/Date of Birth Investigator Review – High Level
 (Current state is significantly the same as future state)

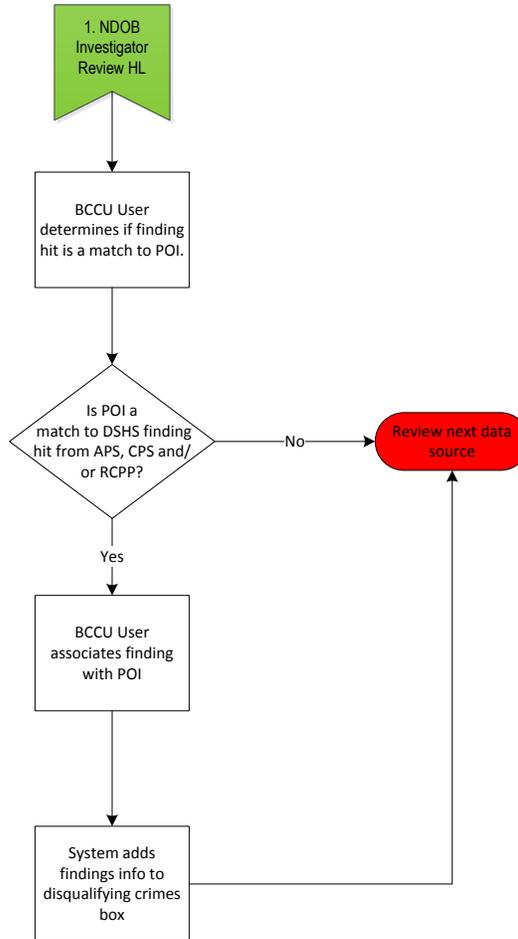


Updated 10/19/2015

Future State – Name/Date of Birth Investigator Review Detail
WSP & AOC Detail Flows
 (Current state is significantly the same as future state)

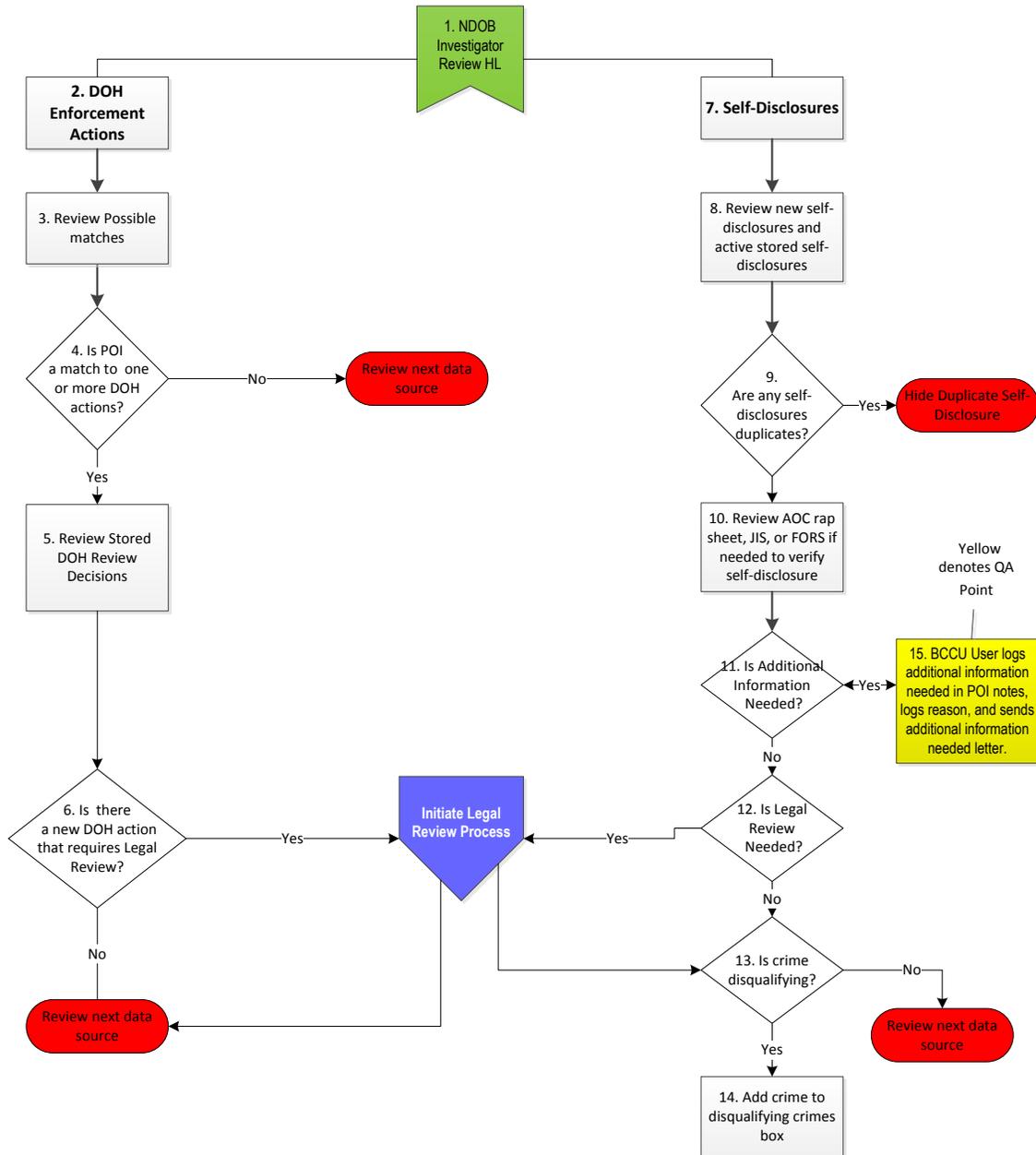


**Future State – Name/Date of Birth Investigator Review Detail
DSHS (RCPP, APS, CPS) Findings Hits Flow**
(Current state is significantly the same as future state)



Updated 11/04/2015

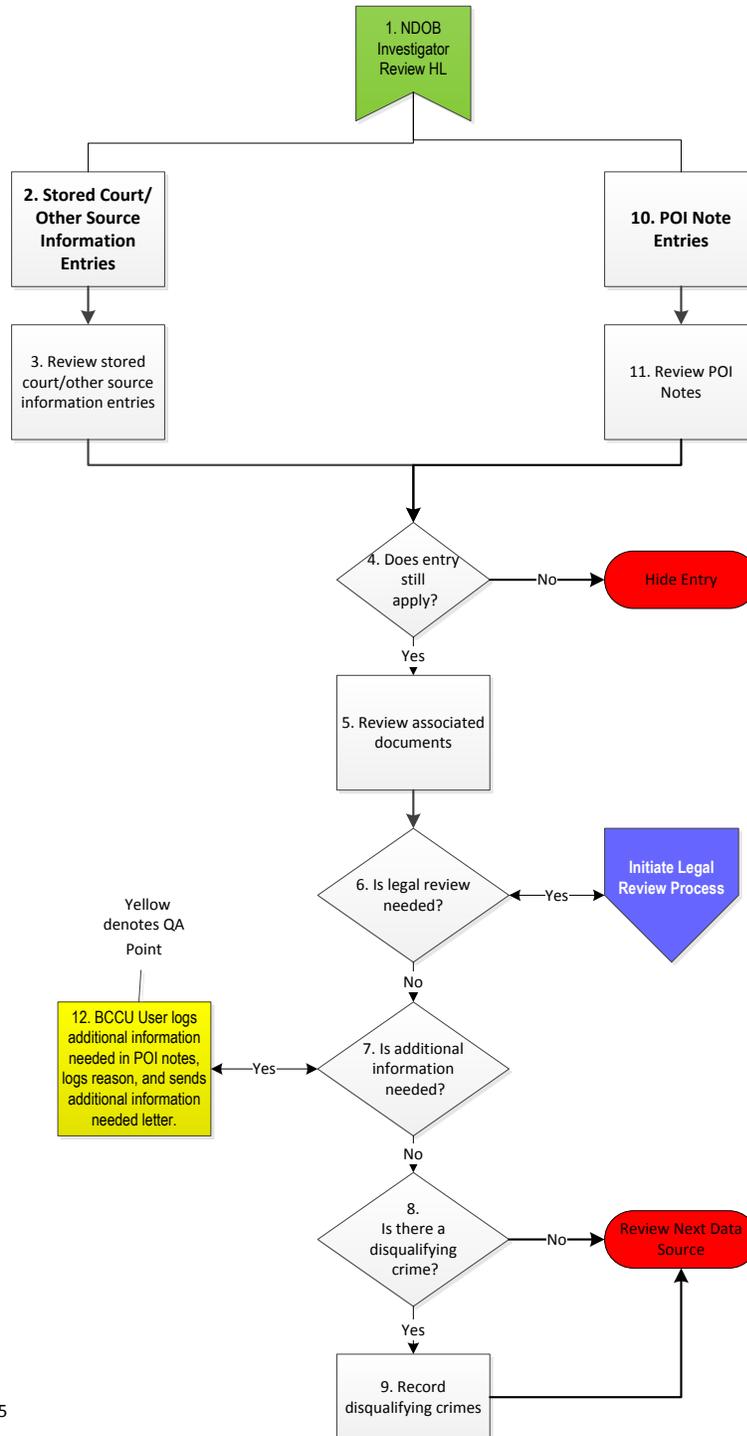
**Future State – Name/Date of Birth Investigator Review Detail
DOH & Self-Disclosure Flows**
(Current state is significantly the same as future state)



Updated 11/04/2015

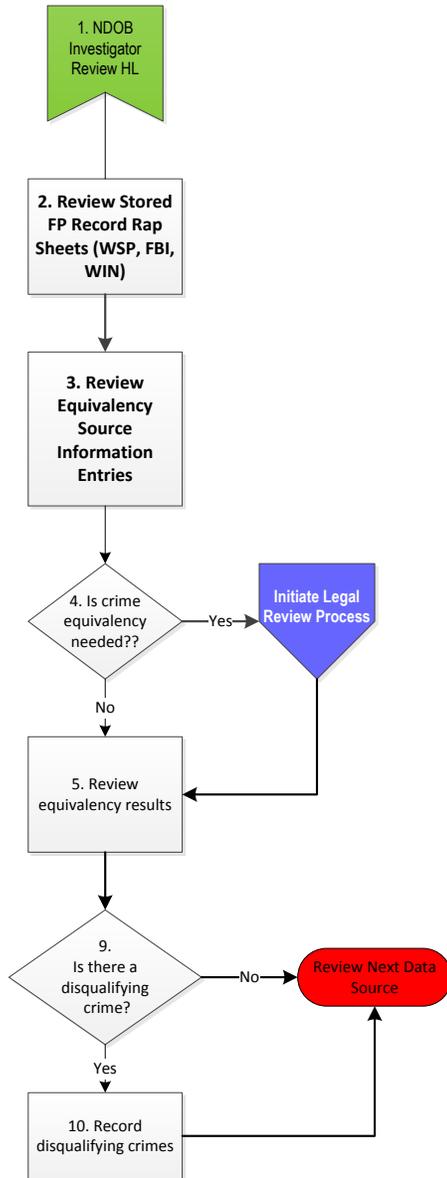
**Future State – Name/Date of Birth Investigator Review Detail
Court\Other Source Information Entries Flow
POI Note Entries Flow**

(Current state is significantly the same as future state)



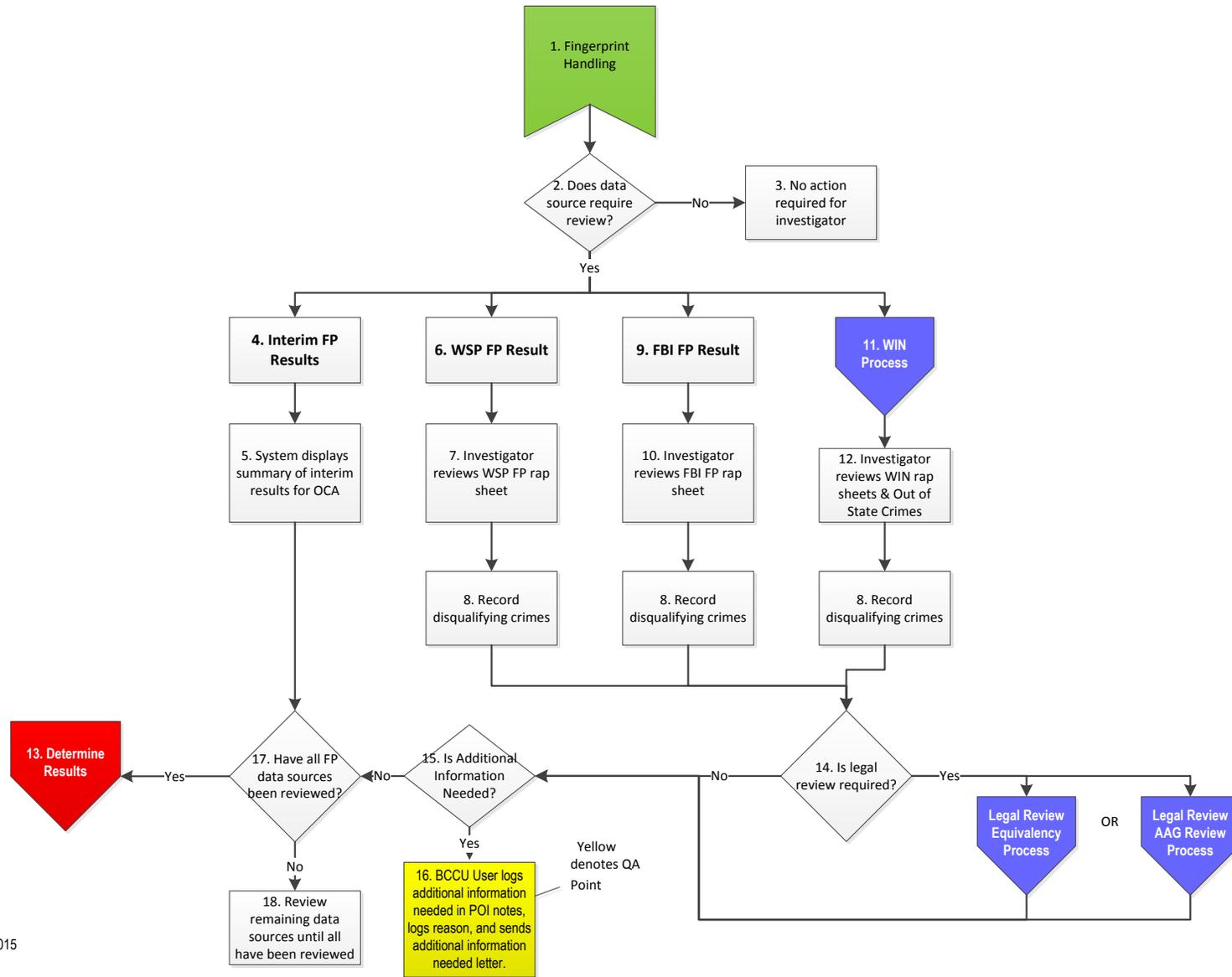
Updated 11/05/2015

Future State – Name/Date of Birth Investigator Review Detail
Stored FP Rap sheets Flow
Stored Equivalency Entries Flow
(Current state is significantly the same as future state)

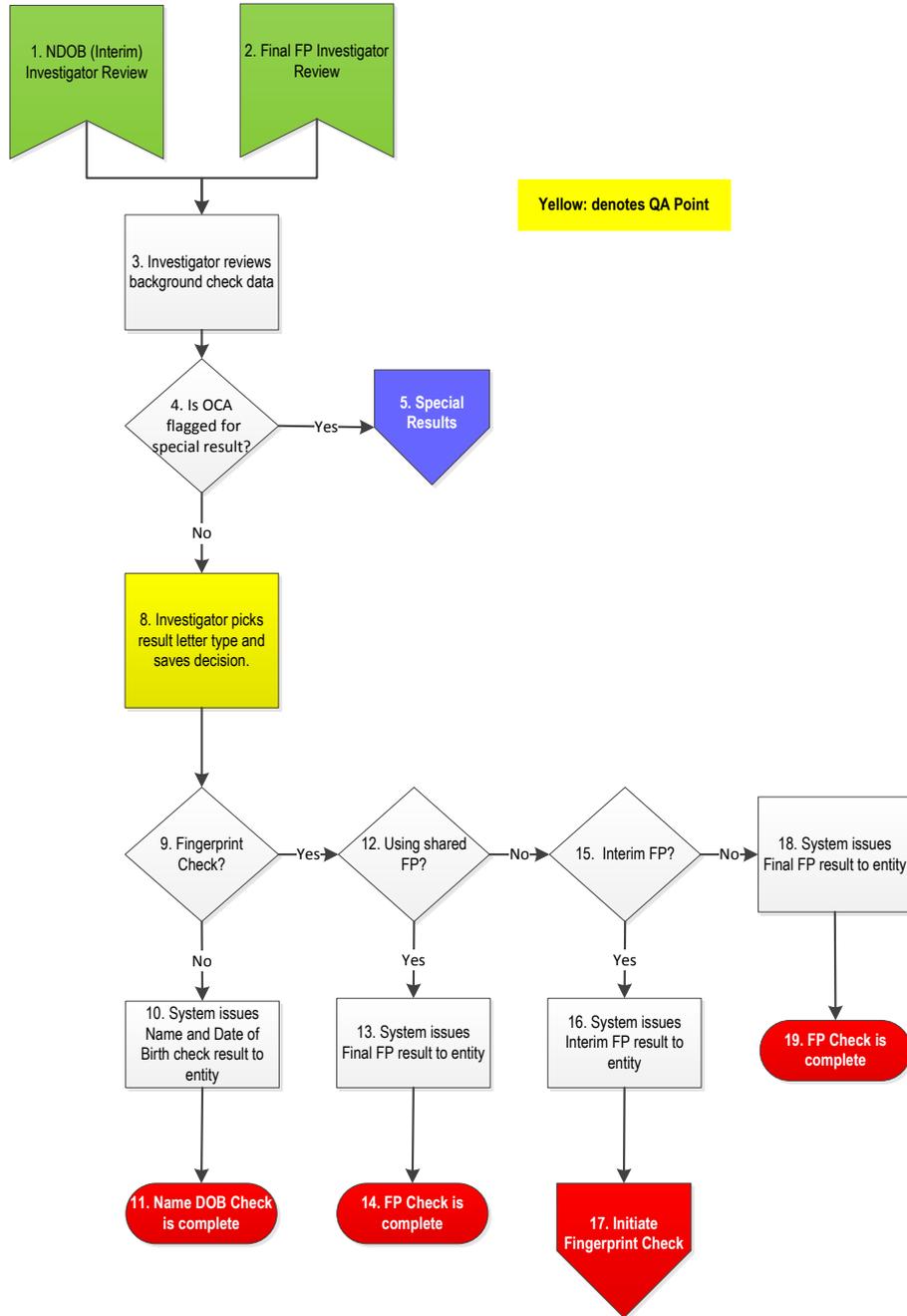


Updated 11/05/2015

Future State – Final Fingerprint Investigator Review
(Current state same as future state)

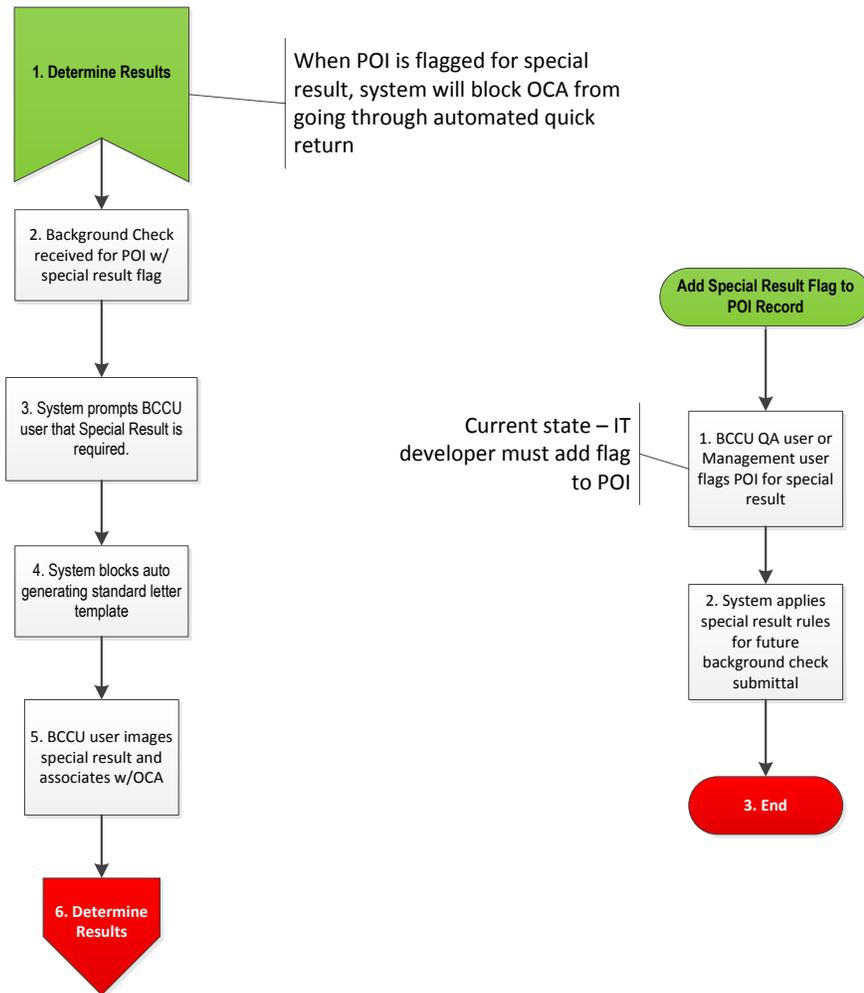


Future State – Determine Results

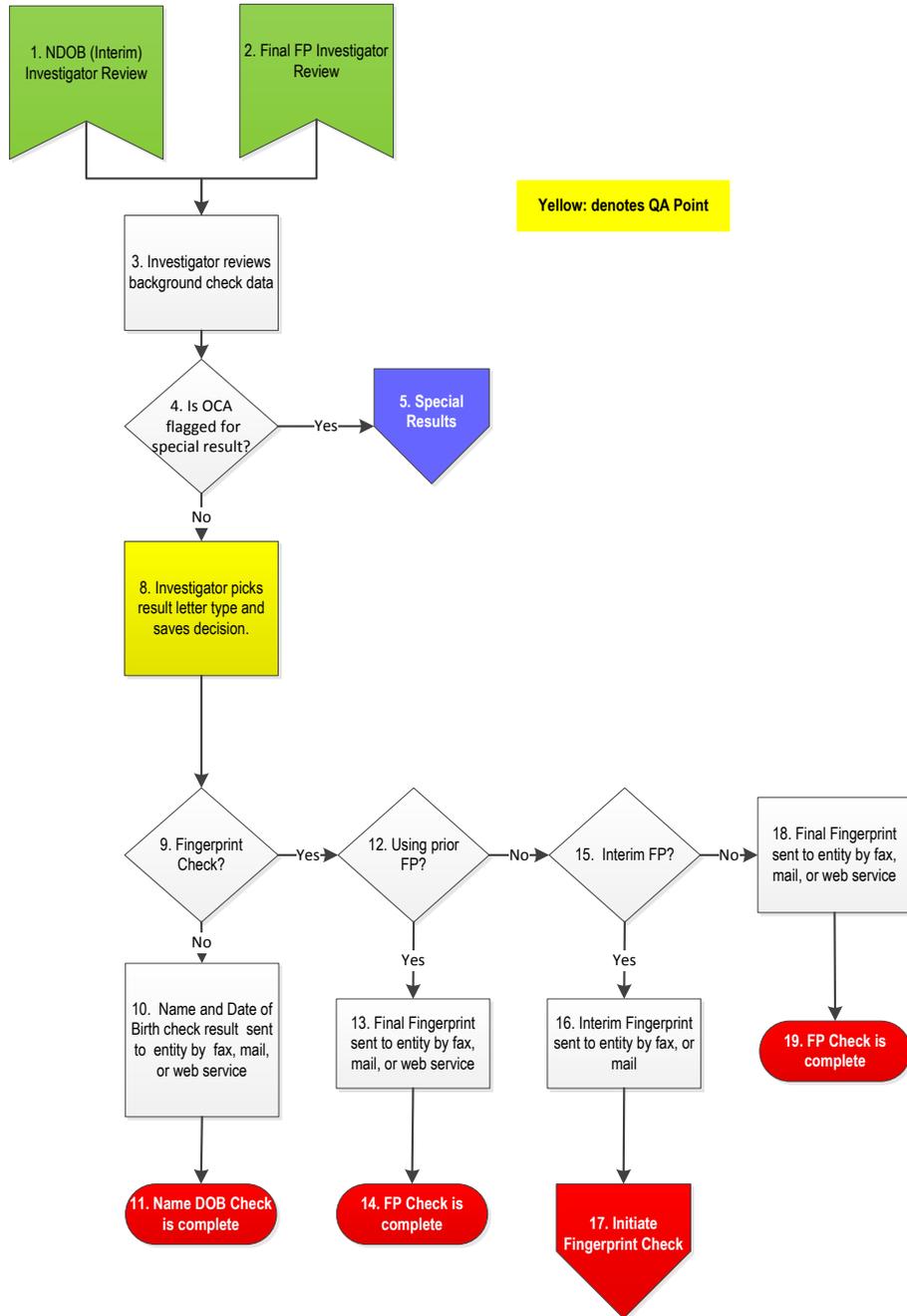


Updated 11/05/2015

Future State – Special Result Process
 (Current state is substantially the same)



Current State – Determine Results



Updated 11/05/2015

6.7 Thumbprint Process

This section describes the requirements, business rules and process for initiating a thumbprint request when the Washington State Patrol WATCH interface returns multiple matching SID records for the person of interest and the BCCU user cannot determine a definite match with the information available.

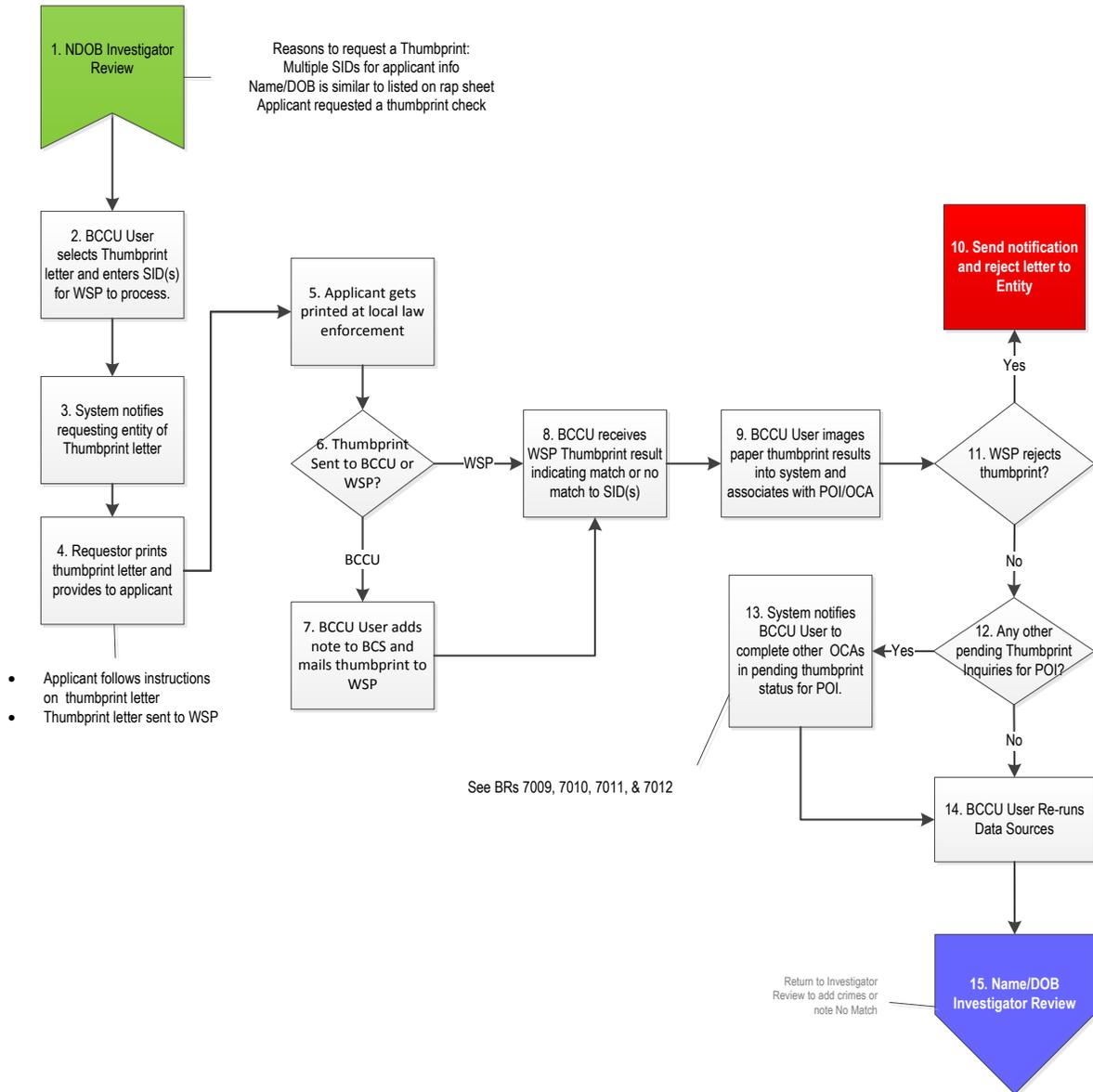
Requirements Table 6.7 – Thumbprint Process		
Requirement Type (F/NF)	Requirement Number	Function/Feature - Requirement
F	7.1	Ability to flag an OCA as requiring a thumbprint.
F	7.2	Track the status of thumbprint requests.
F	7.3	Ability for system to notify the entity user when a thumbprint is required.
F	7.4	Ability to populate thumbprint request packet with required information and distribute thumbprint request packet to entity user.
F	7.5	Have the ability to track when thumbprint result is received from the WSP.
F	7.6	Have the ability to image thumbprint results into the system and associate them with a person of interest/OCA.
F	7.7	Allow BCCU users to complete any outstanding OCAs in thumbprint status for the person of interest using one thumbprint result.

Business Rules Table 6.7 – Thumbprint Process	
BR#	Rule Description
7000	Thumbprints may be requested only for Name/DOB background checks.
7001	The BCCU User may request thumbprints if the WSP returns multiple SIDs for an applicant.
7002	The BCCU User may request thumbprints if the applicant's Name/DOB is similar to another Name/DOB listed on rap sheet.
7003	The applicant may request a thumbprint check if they believe a WSP criminal history record does not belong to them.
7004	The WSP thumbprint result is imaged into the system and associated with the applicable POI/OCA.
7005	Thumbprint document may be sent directly to WSP or to the BCCU.
7006	If BCCU receives the thumbprint document, BCCU User will enter a note into the system and forward the document to WSP.
7007	When a thumbprint is received all Name/DOB data sources are re-run before the BCCU User determines the result. (Name/DOB data sources = WSP, AOC, Findings, Legacy, Source Doc, Prior FP Results.)
7008	When a thumbprint is completed, OCAs pending thumbprints are updated. New OCAs are not created.
7009	A POI may have multiple OCAs in pending thumbprint status.
7010	One WSP thumbprint result may be used to complete multiple pending thumbprint requests for

Business Rules Table 6.7 – Thumbprint Process	
BR#	Rule Description
	the same POI.
7011	When the WSP thumbprint result is received and the POI has multiple OCAs in pending thumbprint status, the system will notify BCS user there are other pending thumbprints for the POI.
7012	When the POI has multiple OCAs in pending thumbprint status, the BCCU User may complete any of the OCAs in pending thumbprint status (System does not require BCCU user to complete all outstanding TP OCAs.)

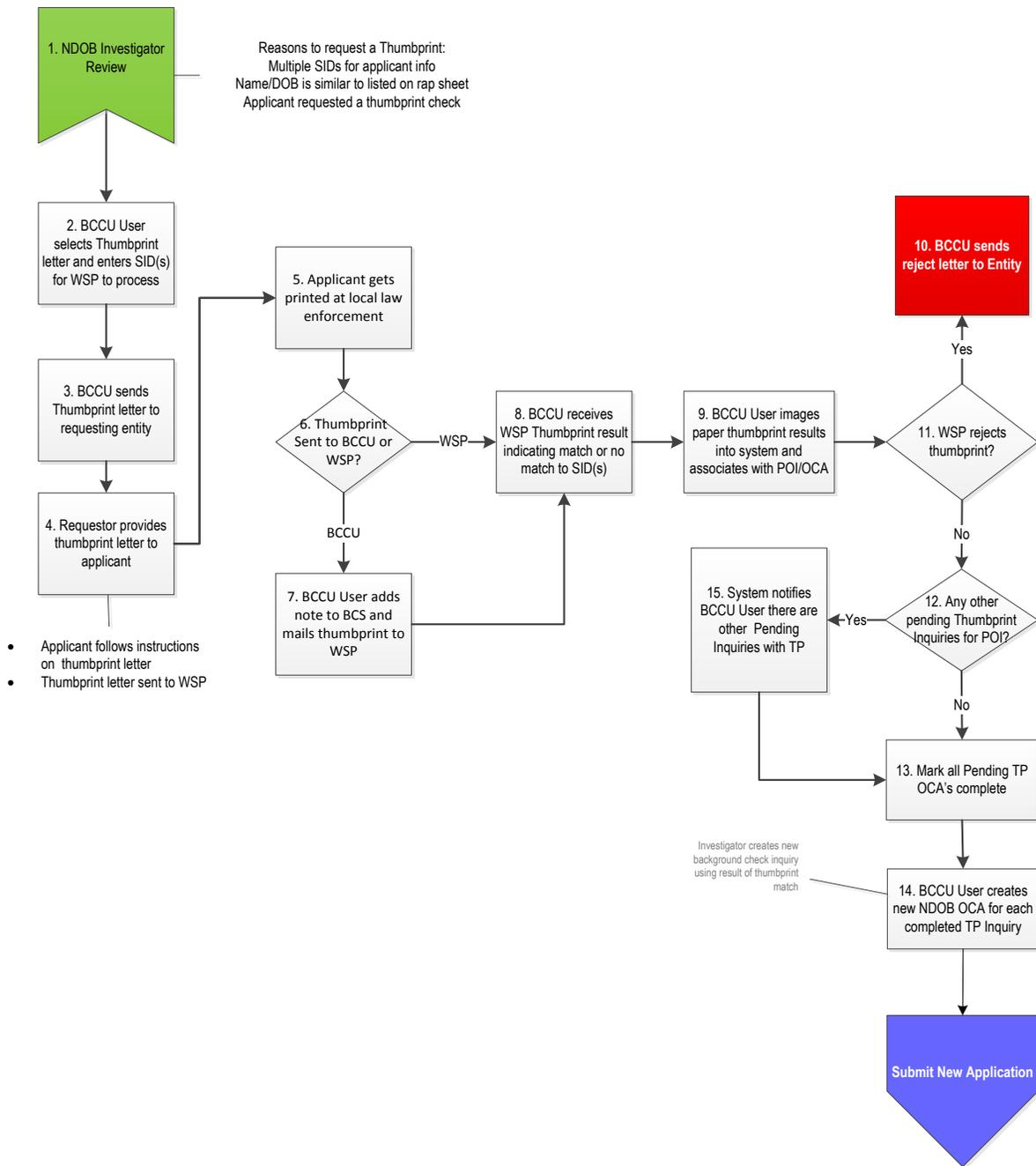
Supporting Documents Table 6.7 – Thumbprint Process	
The following supporting documents will be provided to the successful vendor at time of requirements verification:	
Name	Location
Background Check Result Document (Thumbprint Packet)	Appendix O

Future State – Thumbprint Process



Updated 06/25/2015

Current State – Thumbprint Process



Updated 06/09/2015

6.8 Legal Review Processes

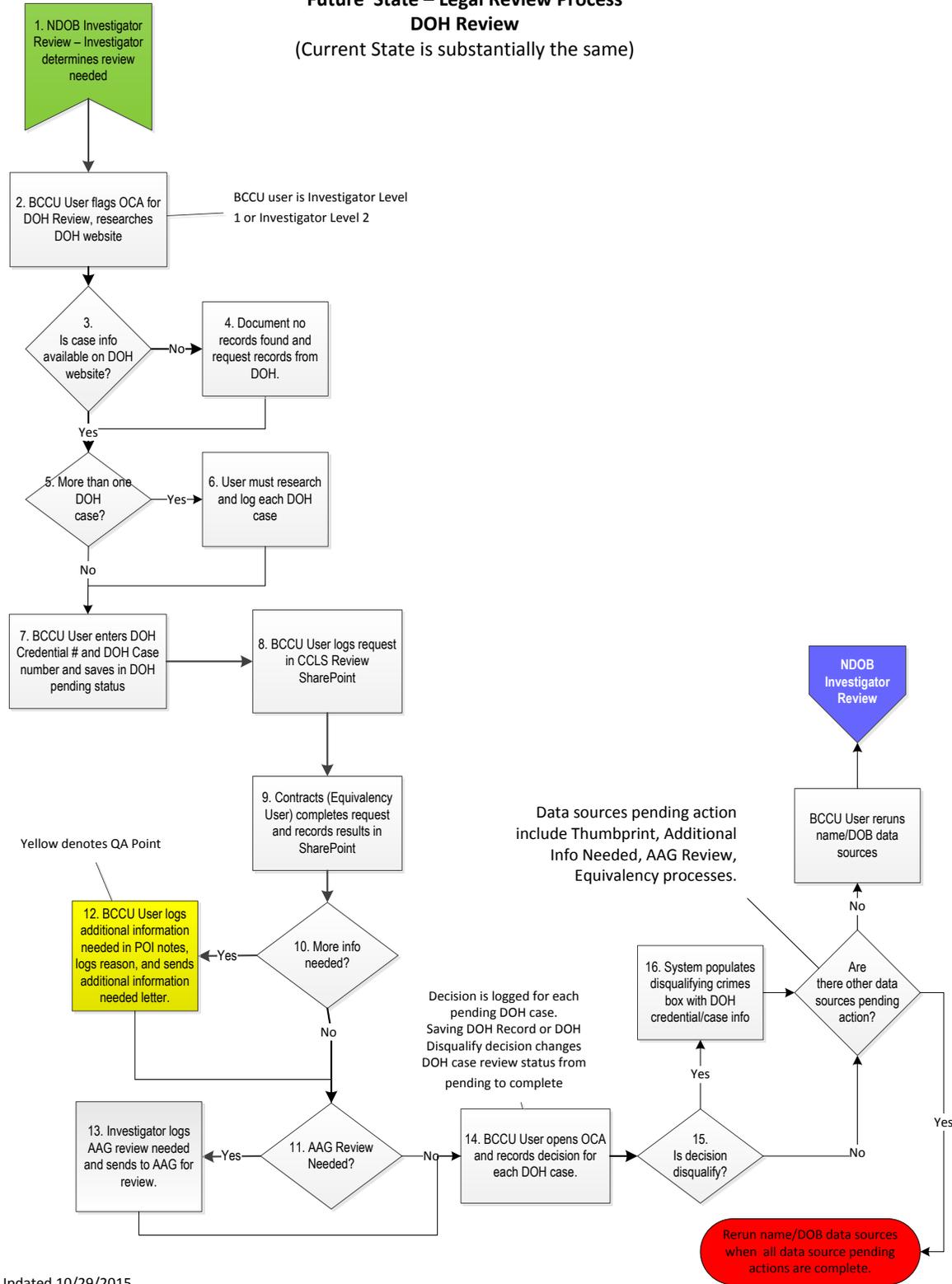
This section describes the requirements, business rules, and processes for BCCU users to initiate, track, and log the results of legal review in the Background Check System. Legal reviews include out-of-state crime equivalency and Department of Health findings reviews by the DSHS in-house legal team or a request to the state attorney general’s office. Legal reviews are associated with a person of interest and the information is used to complete current and future background check requests.

Requirements Table 6.8– Legal Review Processes		
Requirement Type (F/NF)	Requirement Number	Function/Feature - Requirement
F	8.1	Provide a method for initiating an equivalency or DOH findings review request with in-house legal review team or initiating a legal review with the WA assistant attorney general.
F	8.2	Ability to place the background check OCA in a hold status until the legal is complete.
F	8.3	Ability to store legal review documents and log legal review notes and associate them with a person of interest record and make them available for future background check requests.
F	8.4	Ability to track the status of a legal review.
F	8.5	Prevent the background check from being completed until pending reviews are complete.

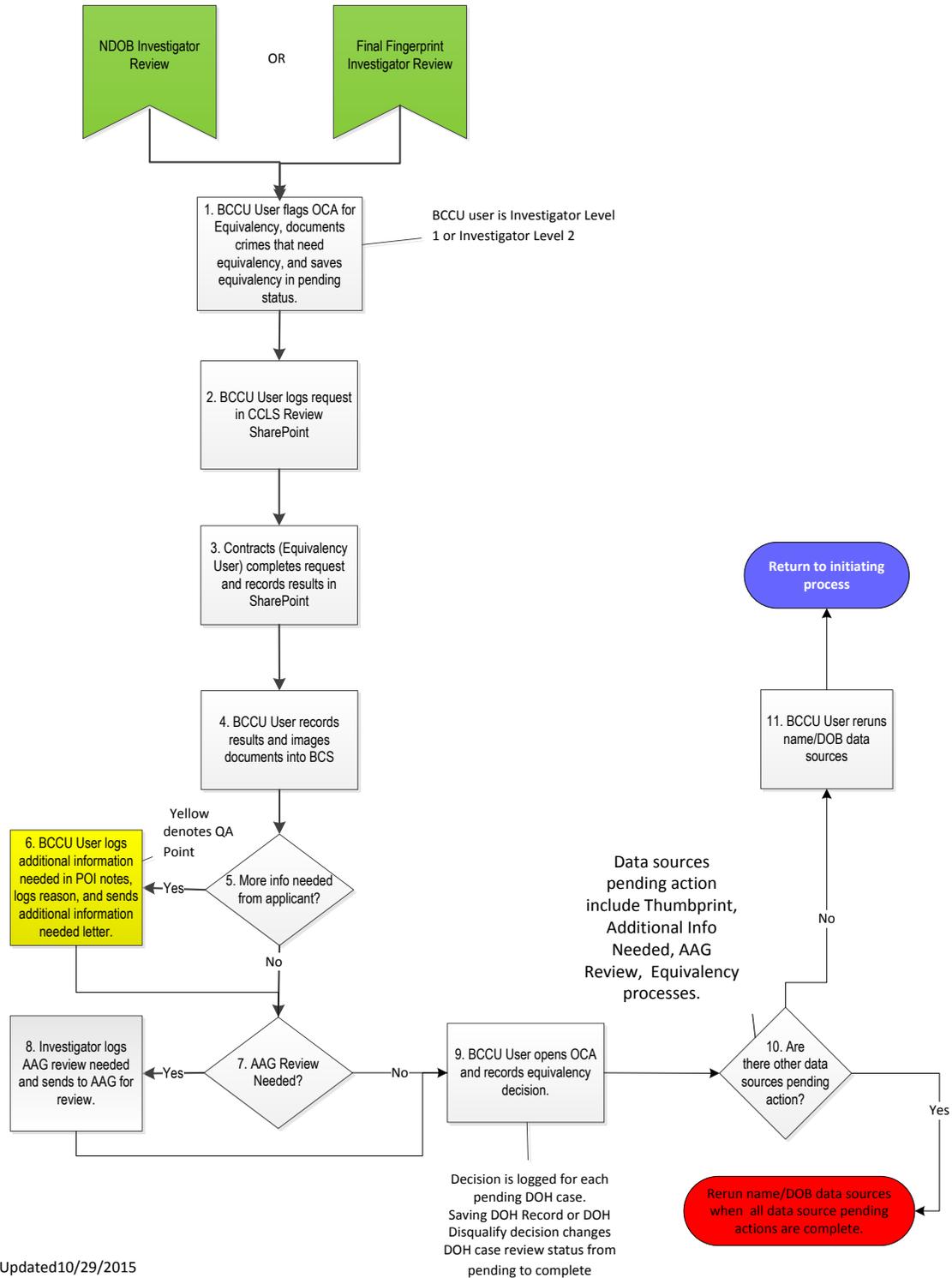
Business Rules Table 6.8– Legal Review Processes	
BR#	Rule Description
Equivalency/DOH Findings Review Processes	
8000	An OCA is sent for equivalency review if an OCA includes crimes that need equivalency review, even if there are other disqualifying crimes that do not require equivalency review.
8001	If the BCCU level 1 users cannot determine if legal review is needed, they will place the inquiry in a hold status and send to the level 2 user for review.
8002	One DOH credential hit may have one or more DOH cases that require determination.
8003	The BCCU user must log the credential number (alpha only) and the case number for each DOH case.
8004	All the crimes requiring equivalency review are noted in the OCA to be reviewed at the same time (the intent is to send an OCA to Contracts for review only once for all crimes and not multiple times).
8005	The Equivalency user may retrieve an OCA with a status of Crime Equivalency Requested or DOH Findings Determination Requested and view all data sources, including Self-Disclosures not marked as “hidden”.
AAG Review Process	
8006	AAG Review is associated at the POI record level.
8007	When the BCCU Level 1 user identifies possible need for legal analysis, the BCCU Level 1 will flag the POI record as "Pending AAG Review" and add a note.
8008	BCCU Level 2 user reviews the need for legal analysis, and if needed, will flag the POI record as "AAG Review Requested" and log the reason for the AAG review.

Business Rules Table 6.8– Legal Review Processes	
8009	BCCU Level 2 user communicates with AAG via standard e-mail and logs the response into the BCS.
8010	When the AAG analysis is received, the BCCU Level 2 User logs the outcome of the analysis and marks the AAG review complete.
8011	The BCCU User images analysis and associates it with POI record.

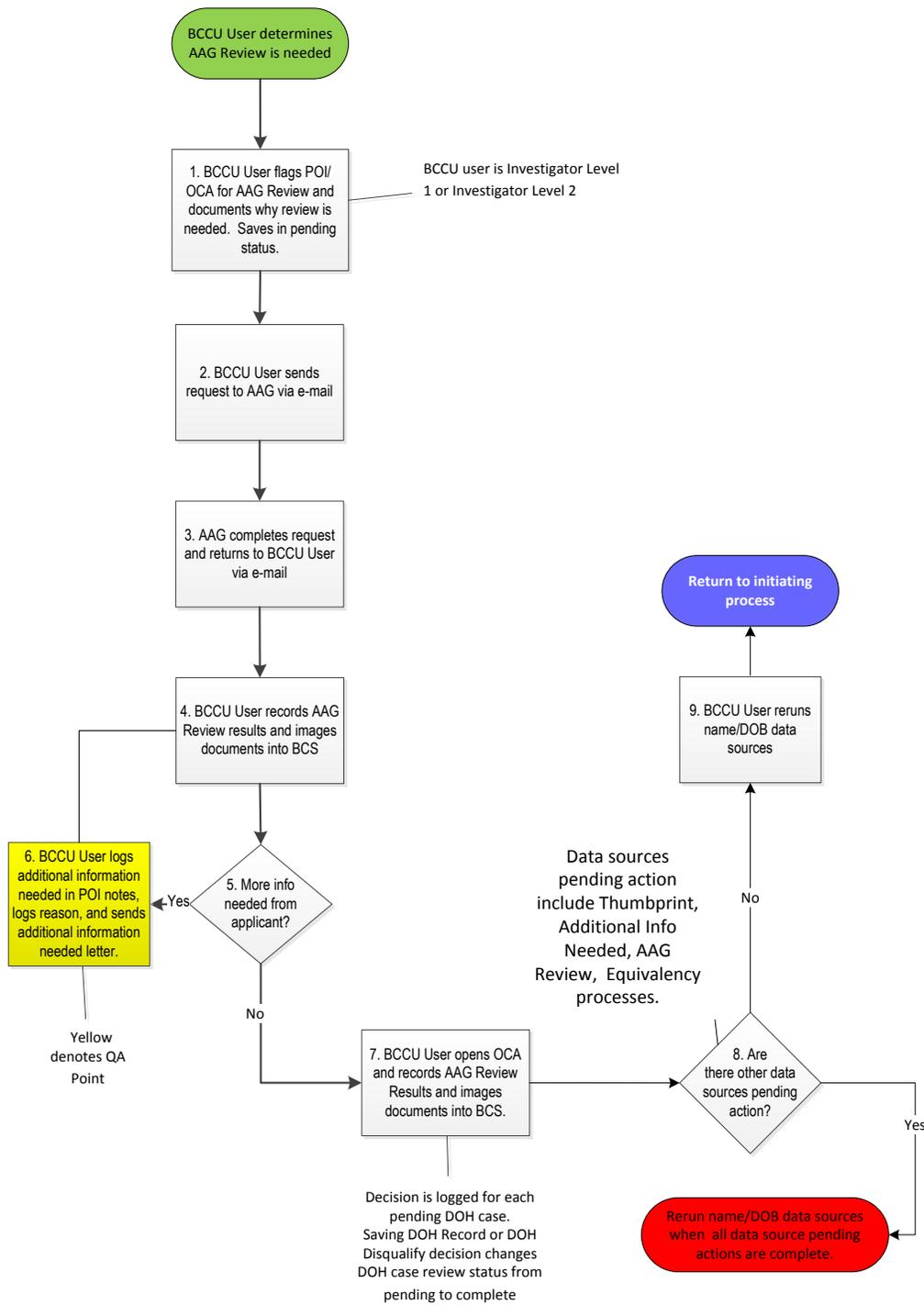
**Future State – Legal Review Process
DOH Review**
(Current State is substantially the same)



**Future State – Legal Review Process
Crime Equivalency Review**
(Current State is substantially the same)



Future State – Legal Review Process
Assistant Attorney General (AAG) Review
 (Current State is substantially the same)



Updated 10/29/2015

6.9 Court and Corrections Research (FORS/JIS)

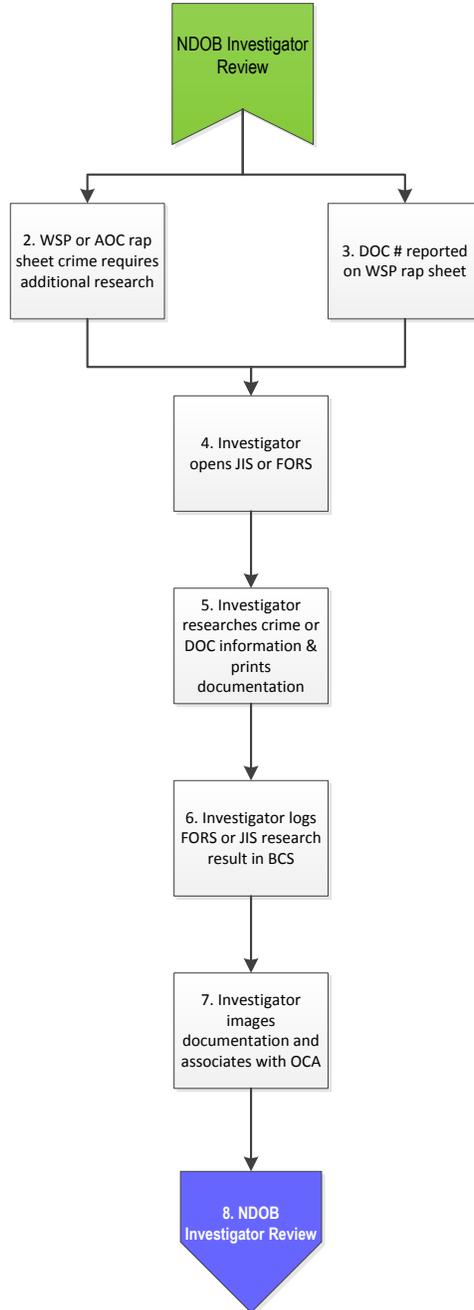
This section describes the requirements, business rules and process for uploading and logging the results of research conducted through the Administrative Office of the Courts Judicial Information System (JIS) or Department of Corrections Felony Offender Reporting System (FORS). Both systems are accessed outside of the Background Check System, information is printed and uploaded into the Background Check System, associated with a person of interest/OCA, and notes are logged for use in completing current and future background checks on the person of interest.

Requirements Table 6.9 – Court and Corrections Research (FORS/JIS)		
Requirement Type (F/NF)	Requirement Number	Function/Feature - Requirement
F	9.1	Ability to associate JIS/FORS research documents with the person of interest and OCA.
F	9.2	Provide a method for BCCU user to review stored JIS/FORS research as a data source for use in completing future background checks on the person of interest.
F	9.3	Ability to log reportable criminal history discovered in JIS/FORS research and include in the background check result.

Business Rules Table 6.9 – Court and Corrections Research (FORS/JIS)	
BR#	Rule Description
9000	When additional research is needed in Department of Corrections Felony Offender Reporting System (FORS) or Administrative Office of the Courts Judicial Information System (JIS), the investigator accesses the desired system outside of the Background Check System.
9001	The investigator creates source information entry for the source and logs crime information. The source information type is: JIS = Washington State Court FORS = Washington State Department of Corrections, Felony Offender Report System
9002	The investigator prints and images documentation, and associates with the Source Information entry.
9003	JIS and FORS entries are source information that is used for future background checks.

Supporting Documents Table 6.9 – Court and Corrections Research (FORS/JIS)	
The following supporting documents will be provided to the successful vendor at time of requirements verification:	
Name	Location
Source Information Document	Appendix I

Future State – Court and Corrections Research (FORS-JIS) Process
(Current State is the same)



Updated 06/03/2015

6.10 Initiate Fingerprint Check

This section describes the requirements, business rules, and work process flows for entities to initiate a fingerprint-based background check, including the validation process used by the fingerprint vendor MorphoTrust (aka MT or IdentoGo).

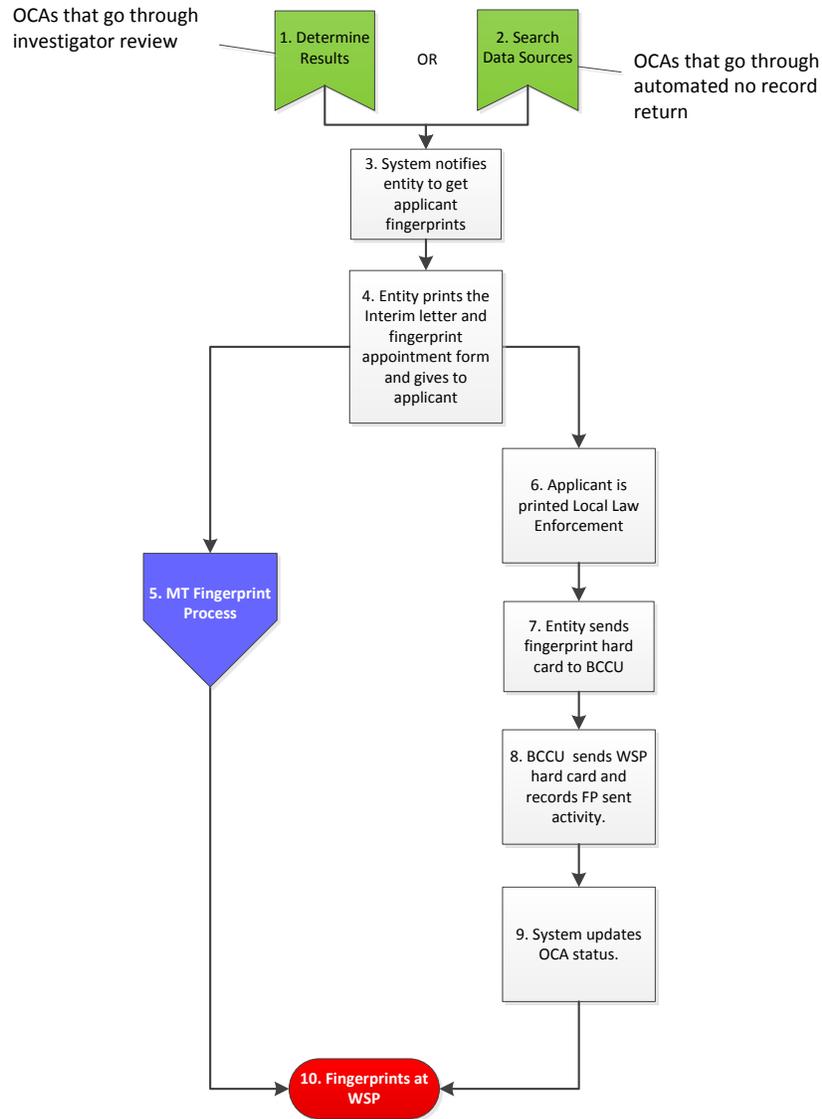
Requirements Table 6.10 – Initiate Fingerprint Check		
Requirement Type (F/NF)	Requirement Number	Function/Feature - Requirement
F	10.1	Integrate a web service with the contracted fingerprint vendor to exchange information with to validate identifiers and to verify that the person-of-interest may be fingerprinted. Information exchange occurs at key steps in the fingerprint process.
F	10.2	Ability to track key steps and statuses in the fingerprint process.

Business Rules Table 6.10 – Initiate Fingerprint Check	
BR#	Rule Description
10000	Fingerprint vendor must verify with BCCU that the applicant is eligible to be fingerprinted before prints are taken.
10001	When BCCU receives hard cards, BCCU User log activity that FP are sent and saves activity - system updates status.
10002	When BCCU FP sent activity is entered manually, system updates status once activity is saved.
10003	If applicant’s prints are rejected, the applicant uses the same process to schedule reprints. BCS will transmit the TCN to MT if WSP has rejected the prints for the OCA.
10004	If applicant was originally printed by local law enforcement and the prints were rejected, the applicant may schedule fingerprint appointment with MT and MT will print the applicant and charge for the prints.
10005	The system captures the source of the fingerprints for reconciling billing sources.
10006	An OCA may have multiple TCNs.
10007	When the BCS Web service is called with the Request ID (OCA), BCS returns the BCCU Account Number, OCA, ORI, Applicant Name and Aliases, DOB, SSN (if available).
10008	Once the fingerprints are sent to WSP and accepted, MT will notify BCS with the date MT receives verification that WSP received the print, TCN, OCA.
10009	When MT web service sends message to BCS indicating that applicant fingerprints are transmitted, BCS logs activity that FP are sent and updates status of OCA.
10010	WSP notifies BCCU about the reject. BCS web service will notify MT that the prints were rejected. (email image tool picks up the rejects and BCS transmits TCN to MT.)
10011	MT Web Service will send the appointment status: Date scheduled, Appointment Date, Date Printed, Location, OCA, Status (No Show, Cancel, Printed).
10012	BCS will display the Date scheduled, Appointment Date, Date Printed, Location, OCA, and Status for the Entity to view.

Business Rules Table 6.10 – Initiate Fingerprint Check	
10013	MT will not allow walk-ins, though applicants may schedule same day appointments.
10014	MT will no longer provide an extranet site.
10015	MT will no longer be able to edit applicant information. If applicant information is incorrect, applicant must contact the entity to update information.
10016	DSHS/BCS will provide applicant information for scheduling, but MT will need to collect the demographic information such as height, eye color, etc. (per the Technical Summary).

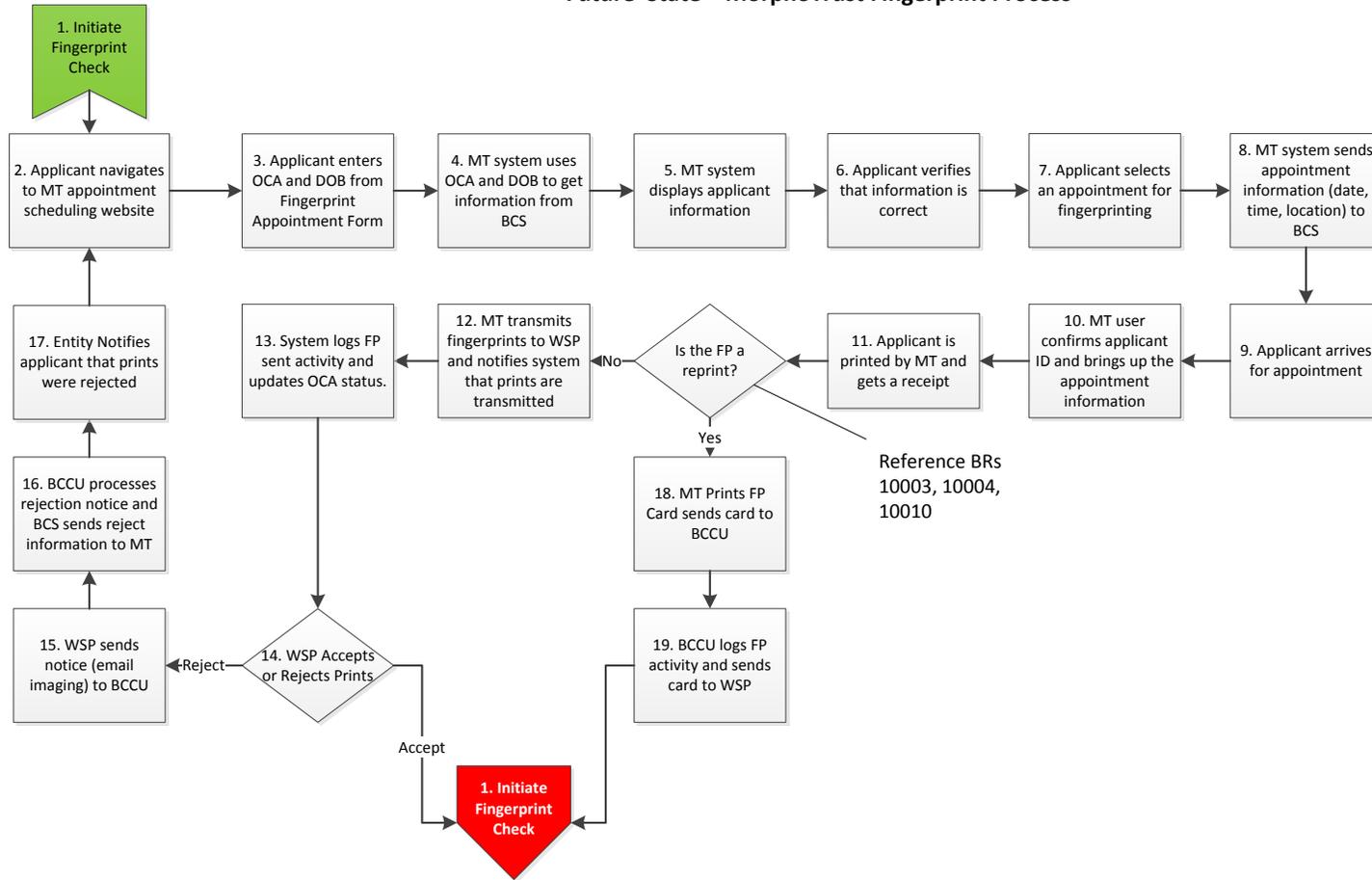
Supporting Documents Table 6.10 – Initiate Fingerprint Check	
The following supporting documents will be provided to the successful vendor at time of requirements verification:	
Name	Location
MorphoTrust Technical Documentation	Appendix Q

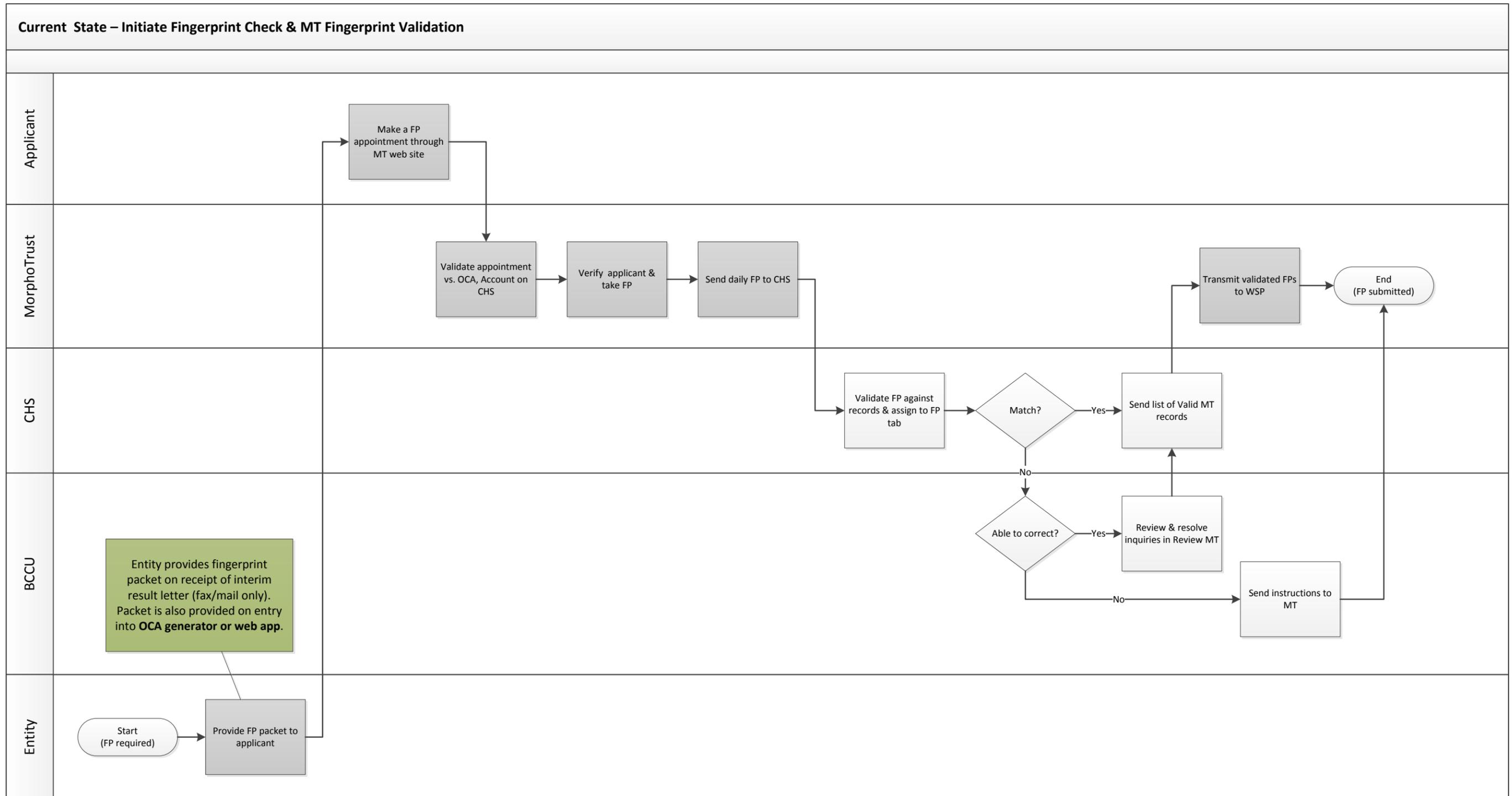
Future State – Initiate Fingerprint Check



Updated 06/03/2015

Future State – MorphoTrust Fingerprint Process





Shaded boxes = not performed by DSHS

6.11 Fingerprint Handling

This section describes the requirements for handling applicant fingerprint results and rejects from the Washington State Patrol and Federal Bureau of Investigation, including an e-mail imaging process that parses and handles e-mailed results, the sub process for handling out-of-state research reported through the Western Identification Network, the automated final fingerprint no-record, and the sub process for requesting a federal name/date of birth result from the Federal Criminal Justice Information System (CJIS) when certain conditions are met for rejected fingerprint checks.

Requirements Table 6.11 – Fingerprint Handling		
Requirement Type (F/NF)	Requirement Number	Function/Feature - Requirement
F	11.1	Receive and store fingerprint results from the WSP & FBI. Fingerprint results are received as a password protected e-mail or received via mail and scanned into the system. Fingerprint results include a WSP name/date of birth rap sheet, fingerprint reject notice, WSP and FBI fingerprint rap sheets, or WSP and FBI no record notifications.
F	11.2	The system must have the capability to automatically issue a final fingerprint no-record result when the following fingerprint automated no-record criteria are met: system receives the final WSP and FBI fingerprint results and the results indicate no record; Washington State Patrol fingerprint rap sheet does not indicate a WIN hit; interim fingerprint result was a no record result.
F	11.3	Provide an automated method for importing password-protected results from e-mail into the background check system.
F	11.4	Provide a method to track when the applicant has a Western Identification Network (WIN) hit on the WSP fingerprint rap sheet. (When a Western Identification Network "hit" is indicated on the fingerprint rap sheet, the state (or states) where the information originates is searched. DSHS Exception: NV and WY cannot be searched by BCCU. Applicant must submit fingerprints directly to the state.
F	11.5	Identify the status of WIN search, including: - when a WIN search is initiated by BCCU for each WIN state indicated on the rap sheet - when each WIN state search is complete BCCU should not be able to complete an OCA when a WIN search is pending.
F	11.6	Record and track the results of each WIN state searched.
F	11.7	Ability to track when fingerprints are rejected by the WSP or FBI including which agency rejected the prints.
F	11.8	Have the capability to notify the requester that the fingerprints have been rejected. Reject notification must include necessary information for the applicant to be reprinted.
F	11.9	CJIS process – Enforce the business rule that BCCU may request a federal name/date of birth background check when the applicant's fingerprints have been rejected by the FBI two times within 100 days.

F	11.10	Have the capability to notify BCCU users when a fingerprint OCA is eligible for CJIS request.
F	11.11	Allow BCCU users to record when a CJIS is requested.
F	11.12	Have the capability to create a CJIS request letter and populate with required information.
F	11.13	Track the status of CJIS requests including whether the result was a record, or no record.
F	11.14	Import scanned CJIS results into the system and associate with an OCA.
F	11.15	Complete the fingerprint result when the CJIS result is received.
F	11.16	The system must provide the ability to close a fingerprint OCA when the following conditions apply: - Applicant has not resubmitted fingerprints after fingerprints were rejected by WSP or the FBI and 372 days have passed from the date the first fingerprints were transmitted to WSP. -Applicant has failed to be fingerprinted and 372 days have passed since the interim letter was completed
F	11.17	The system must have the capability to track the two conditions for closing a fingerprint check listed in 11.16 for reporting purposes.
F	11.18	Fingerprint Tracking The system must have the ability to track turnaround time for key events during the fingerprint check process, including: Overall time to process from submission of request to results being issued; Time from submission to issuing an interim result; Time from fingerprint being scheduled to prints being taken by vendor; Time from prints being taken to prints sent to WSP; Time from prints sent to WSP to WSP/FBI final results received by BCCU; and Time from WSP/FBI final results received by BCCU to final result notification being distributed to requesting user.
F	11.19	The system must track and display the status of key events of the fingerprint process.

Business Rules Table 6.11 – Fingerprint Handling	
BR#	Rule Description
11000	Fingerprints are transmitted to WSP either electronically by fingerprint vendor (MorphoTrust or MT) or as hard cards via mail.
11001	WSP reviews prints and either accepts or rejects prints.
11002	If prints are rejected, WSP sends reject notice to BCCU.
11003	If reject is received via e-mail, the e-mail imaging process parses reject and adds reject activity to the OCA.
11004	If reject is received via mail, the investigator may image reject into system and will add reject activity to the OCA.
11005	The fingerprint reject activity will indicate if the prints were rejected by WSP or FBI.
11006	Fingerprints may be rejected multiple times by either WSP or FBI
11007	When the CJIS conditions are met, the system will initiate CJIS process.
11008	When the fingerprint reject activity is saved to the OCA, the system will generate FP reject letter and send letter and notification to entity.
11009	Fingerprint Reject Letter includes the rejecting agency (WSP or FBI), TCN, OCA and applicant name and account number.

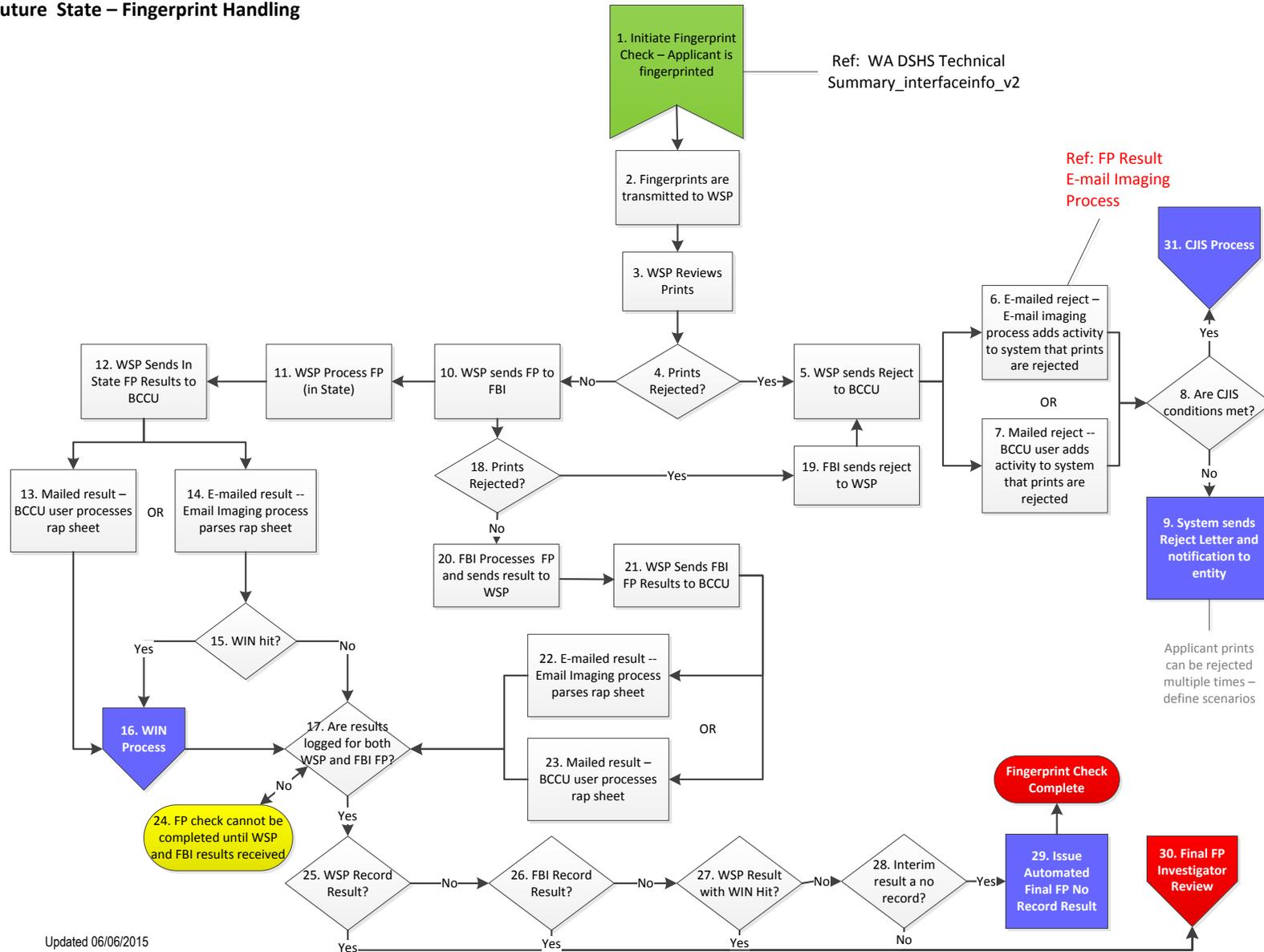
Business Rules Table 6.11 – Fingerprint Handling	
11010	WSP and FBI fingerprint results are sent to BCCU by WSP.
11011	Fingerprint results are received from WSP via e-mail or mail.
11012	If result is received via e-mail, the fingerprint result e-mail imaging process parses result, saves the document to the system and associates it with the OCA. E-mail imaging process adds result activity (WSP Record, WSP No Record, FBI Record, or FBI No Record) to the OCA.
11013	If e-mailed result or reject cannot be processed by e-mail imaging process and results in error, investigator will follow manual process for imaging documents into system and adding FP activities.
11014	If result is received via mail, the investigator will image result document into system and associate it with the OCA. The investigator will add result activity (WSP Record, WSP No Record, FBI Record, or FBI No Record) to the OCA.
11015	The WSP fingerprint result may include a WIN hit.
11016	All WSP fingerprint results that are manually added to the system (not add by e-mail imaging process) must be reviewed for WIN hit.
11017	If the WSP does not have a WIN hit, the WSP and FBI results must be logged in the system before the OCA moves to FP Investigator Review or is completed as Automated Final FP No Record.
11018	If the WSP has a WIN hit, the WSP and FBI results and any WIN state results must be logged in the system before the OCA moves to Final FP Investigator Review or is completed as Automated Final FP No Record.
11019	When all fingerprint results are received and the following conditions are met, the system automatically generates a Final Fingerprint No Record letter and sends it to the entity: <ul style="list-style-type: none"> • No WIN hit on WSP rapsheet • WSP result is no record • FBI result is no record • Interim FP result was no record
11020	If the fingerprint results do not meet the automated final fingerprint no record criteria, the investigator must review the fingerprint results and determine the result letter.
11021	The system will automatically close fingerprints if: <ul style="list-style-type: none"> • Applicant has not resubmitted fingerprints after fingerprints were rejected by WSP or the FBI and 372 days have passed from the date the first fingerprints were transmitted to WSP; or • Applicant has failed to be fingerprinted and 372 days have passed since the interim letter was completed.
11022	The system will track which close condition was met for each OCA that is automatically closed.
11023	Fingerprint tracking activities include: <ul style="list-style-type: none"> • FP Sent • WSP Reject • FBI Reject • FBI Record • FBI No Record • WSP Record • WSP No Record • FBI CJIS • WIN Hit for each WIN state • No Record/Record for each WIN state • FBI Non-Conviction • WSP Non-Conviction

Business Rules Table 6.11 – Fingerprint Handling	
11024	CJIS request is initiated when the # of days between the most recent FBI reject and the previous FBI reject is equal to or less than 100 days for the same OCA.
11025	When CJIS conditions are met, add a CJIS activity that triggers automated CJIS request.
11026	CJIS activity is added into system via automated e-mail imaging process or manually by BCCU.
11027	When automated CJIS request is initiated, system populates CJIS Name Search Request Form fields with from information in the BCS system: ORI associated with Inquiry Type, user name of BCCU Investigator submitting request, TCR number (is populated in field for Transaction Control Number), Name, alias first names, alias last names, date of birth, SSN, OCA, BCCU POI #.
11028	When automated CJIS request is initiated, OCA is set to pending CJIS status.
11029	Populated CJIS Name Search Form is placed in queue for BCCU staff to print.
11030	System notifies entity OCA is pending CJIS.
11031	For DEL web service inquiries, system sends notification of CJIS.
11032	BCCU Investigator prints populated CJIS request and faxes to FBI.
11033	FBI CJIS results are received outside of the system, imaged into BCS and associated with the OCA by BCCU staff.
11034	BCCU investigator records FBI CJIS result for OCA, marks CJIS complete, and completes background check processing.
11035	E-mail imaging process parses WSP FP result for WIN indicator and logs WIN FP state hits.
11036	Both WSP and FBI FP result activities must be logged for OCA before initiating WIN process.
11037	BCCU users will enter WIN FP activities when FP results are received via mail or fax.
11038	When WSP or FBI FP result activity is entered manually (not via e-mail imaging process) the OCA is placed in the WIN queue once both WSP and FBI FP result activities have been logged. The BCCU Level 2 user must review the OCA for possible WIN hits when FP result activity is entered manually.
11039	FP OCAs that are added to the WIN queue for BCCU Level 2 review because of manual FP activity are labeled or marked to differentiate them from OCAs with automated WIN hits.
11040	When the BCCU level 2 user reviews FP OCA and determines WIN hit exists, user logs WIN hit for each WIN state reported.
11041	BCCU user uses decision criteria (outside of system) for determining when to initiate a WIN state search.
11042	Criteria for determining when to initiate a WIN state search varies by state.
11043	If BCCU user determines WIN search is not required, BCCU user completes FP and issues final FP result letter.
11044	OCA may have WIN hit in more than one WIN state.
11045	If an OCA has WIN hits in more than one WIN state, the BCCU user logs each state that is being searched.
11046	When WIN state search is Nevada, the system will insert source text for Nevada into "unknown" result letter.
11047	When WIN state search is Wyoming, the system will insert source text for Wyoming into "unknown" result letter.
11048	When WIN state search result is received, BCCU user images WIN state result into system and associates with OCA.
11049	When WIN state search result is received, BCCU user logs WIN Record or WIN No Record FP result activity.

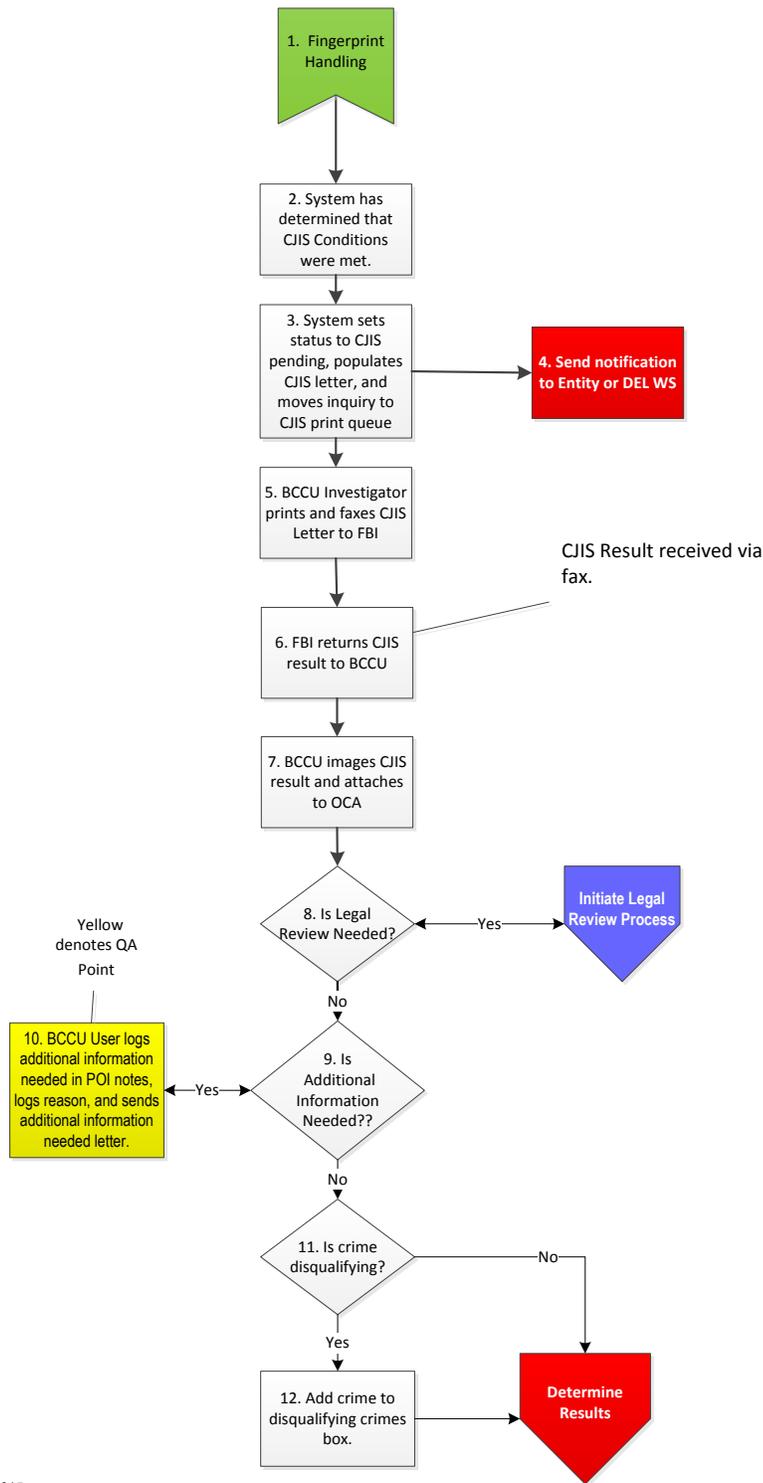
Business Rules Table 6.11 – Fingerprint Handling	
11050	If multiple WIN states are searched, each state result will be received independently at different times.
11051	All WIN state searches must be complete before the background check result can be determined.
11052	If WIN state reports new information that is not included on FBI rap sheet or has disposition for pending charge, information is entered in out of state court source.

Supporting Documents Table 6.11 – Fingerprint Handling	
The following supporting documents will be provided to the successful vendor at time of requirements verification:	
Name	Location
Entity Statuses, Notifications, and Next Steps	Appendix K
Background Check Result Templates and Merge Text	Appendix O
CJIS Name Search Request Form	Appendix R
Data Sources and Automated No Record	Appendix G
Source Information Document	Appendix I

Future State – Fingerprint Handling

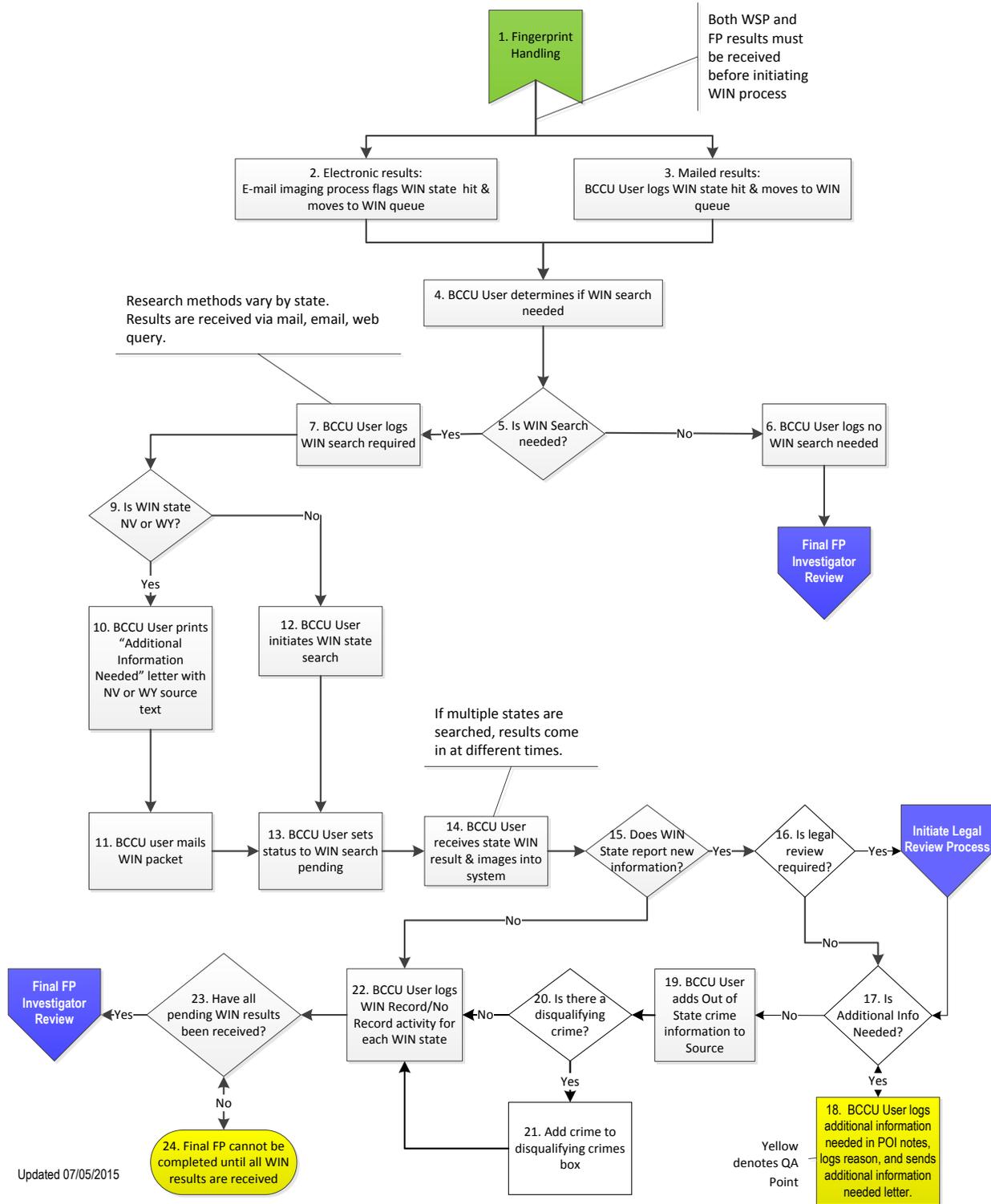


Future State – CJIS Sub Process

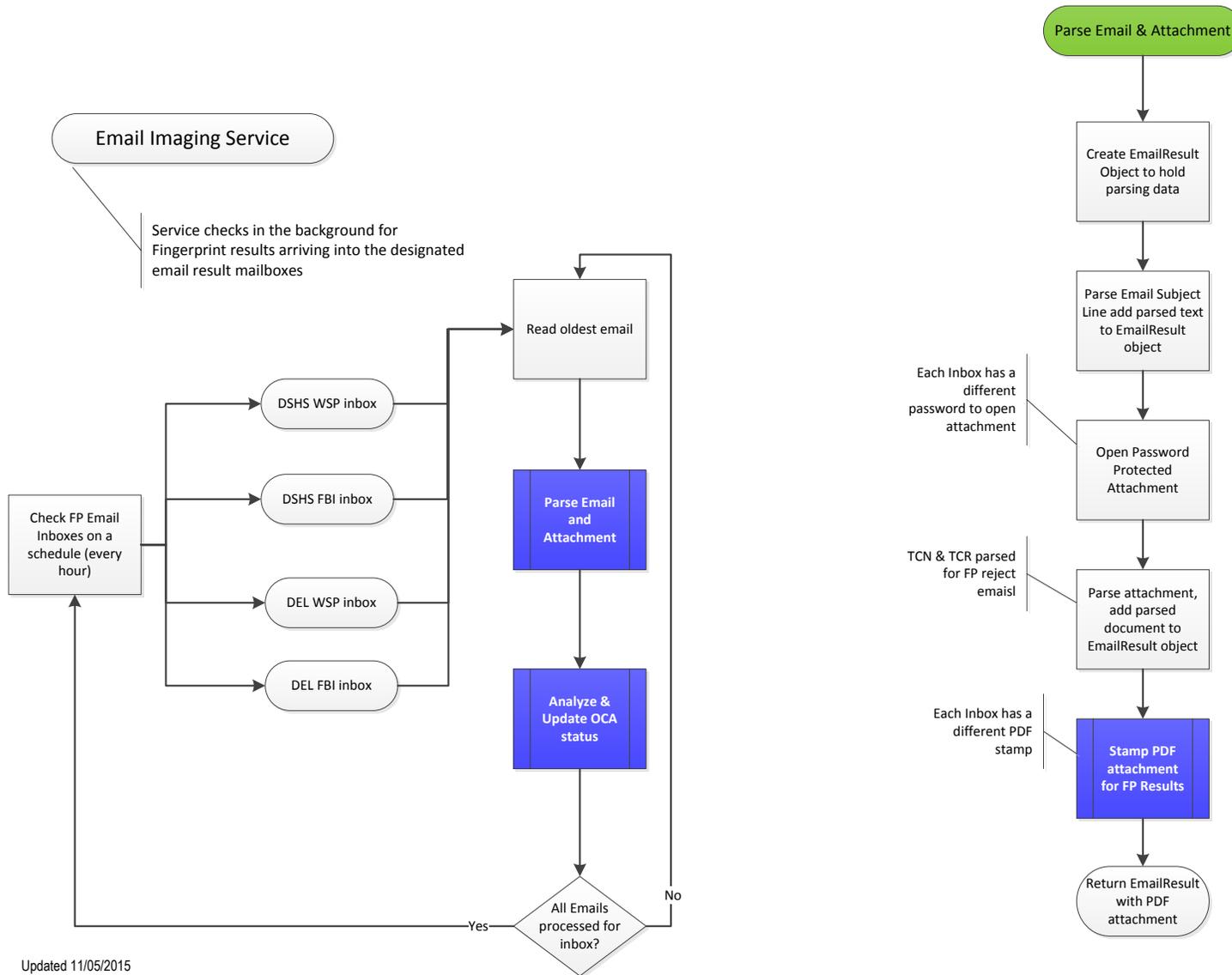


Updated 11/05/2015

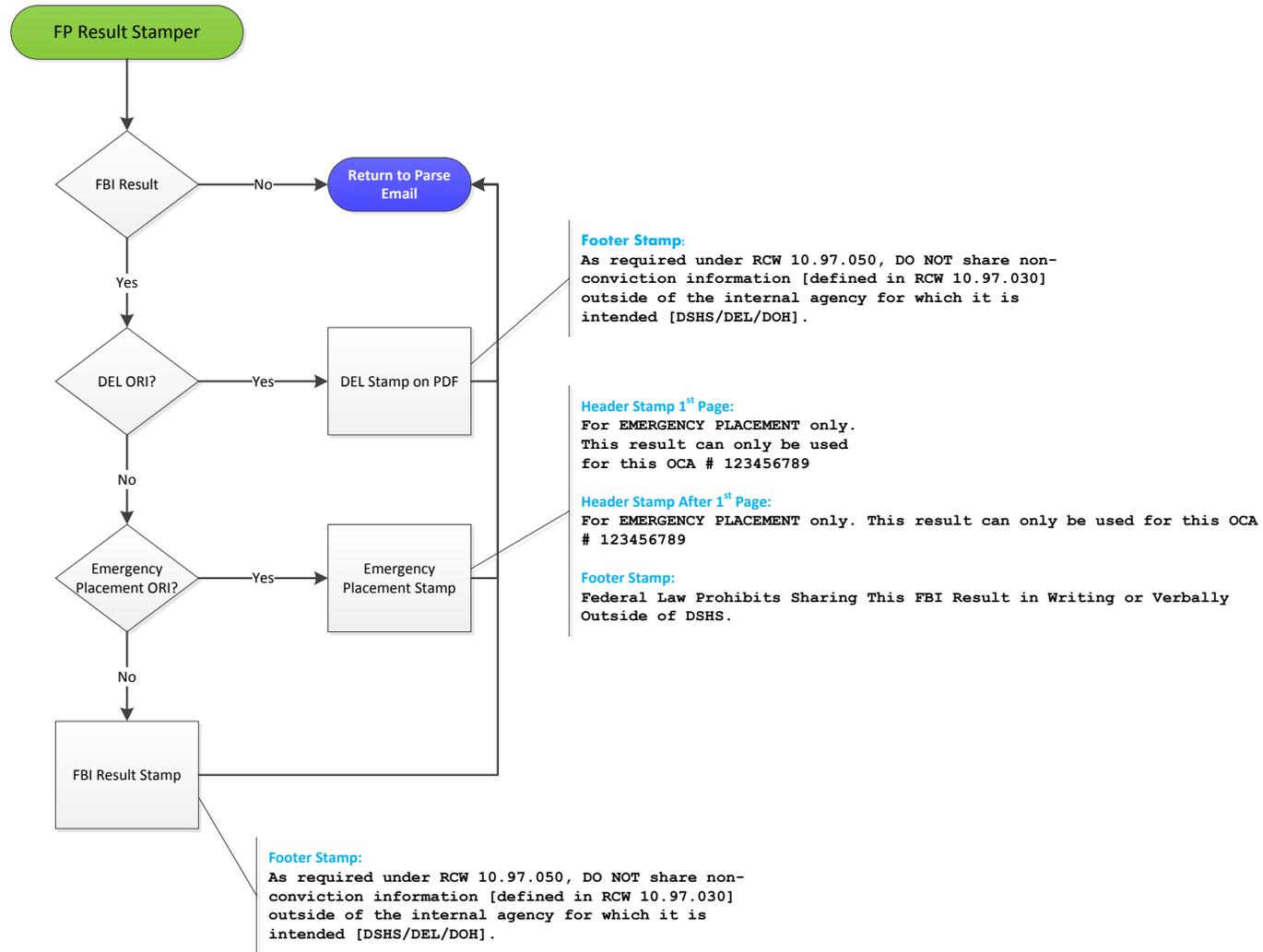
Future State – Western Identification Network (WIN) Sub Process



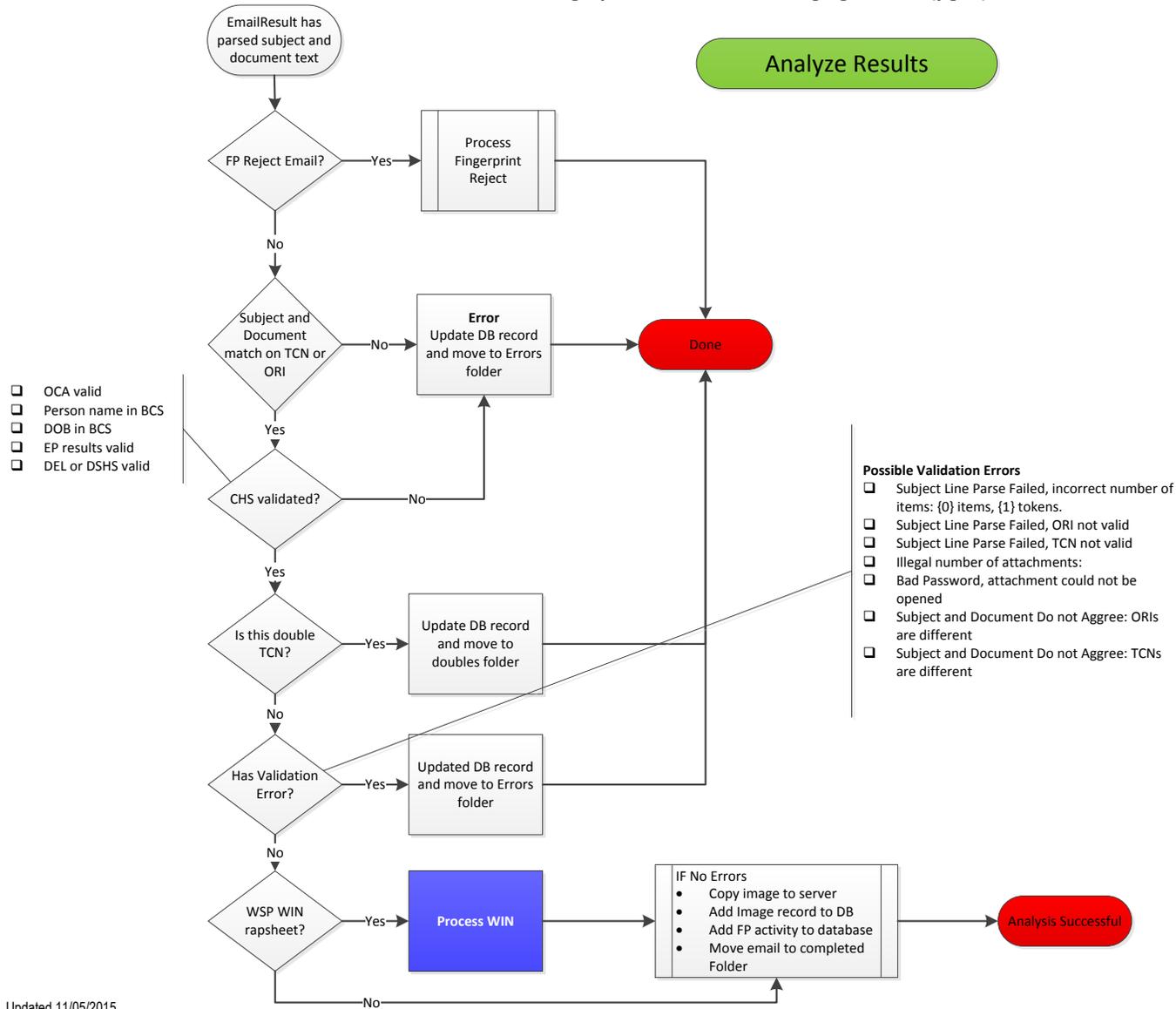
Future State – Fingerprint Result E-mail Imaging Process (pg. 1)



Future State – Fingerprint Result E-mail Imaging Process (pg. 2)

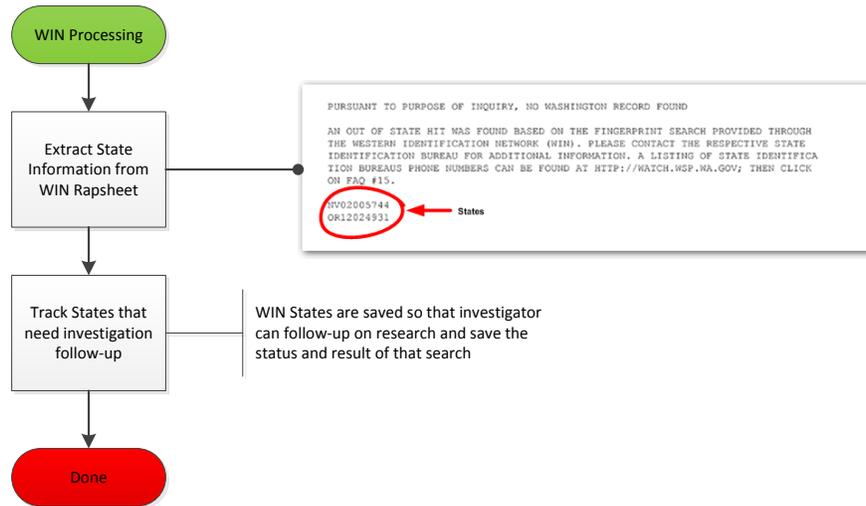


Future State – Fingerprint Result E-mail Imaging Process (pg. 3)



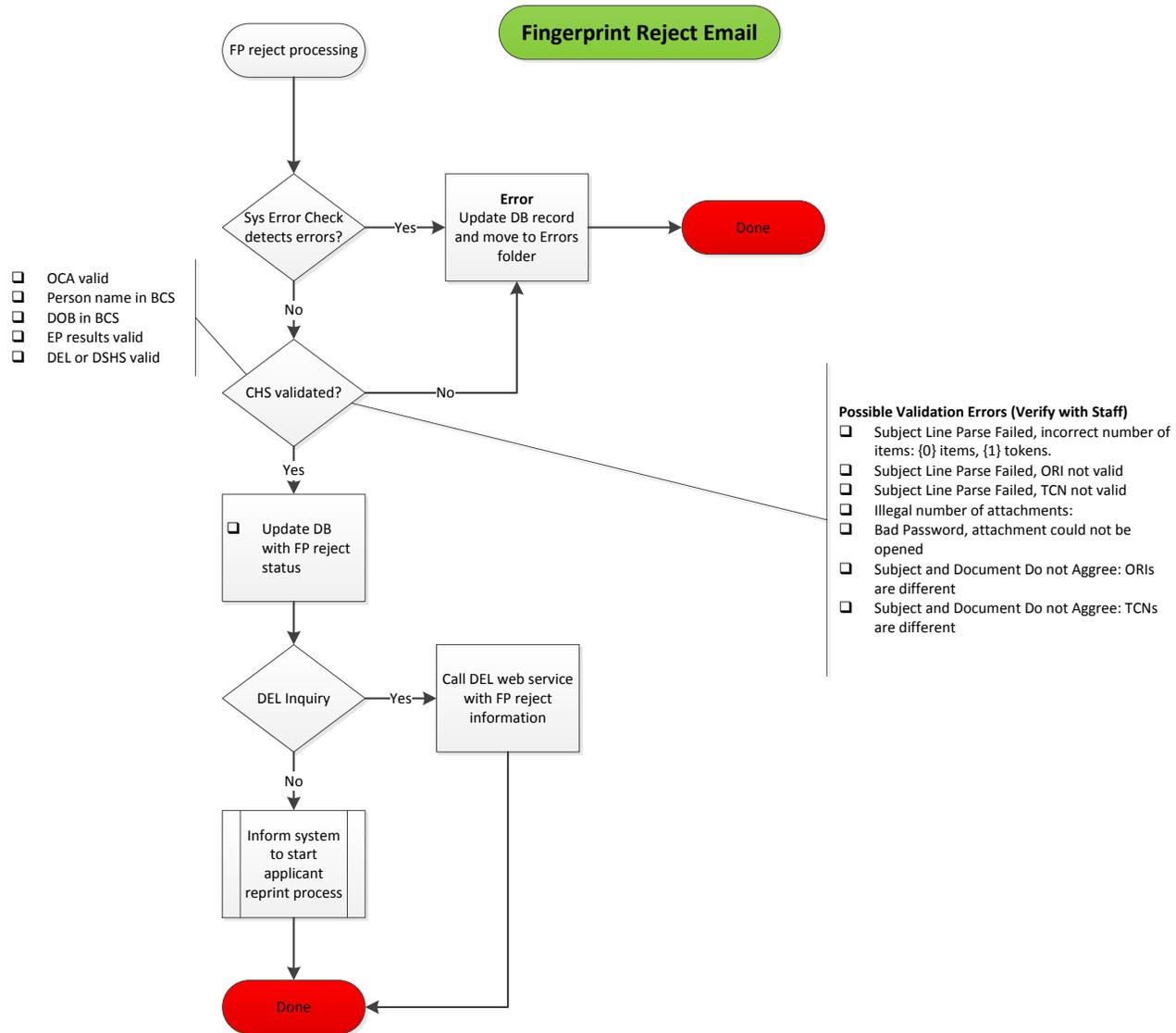
Updated 11/05/2015

Future State – Fingerprint Result E-mail Imaging Process (pg. 4)



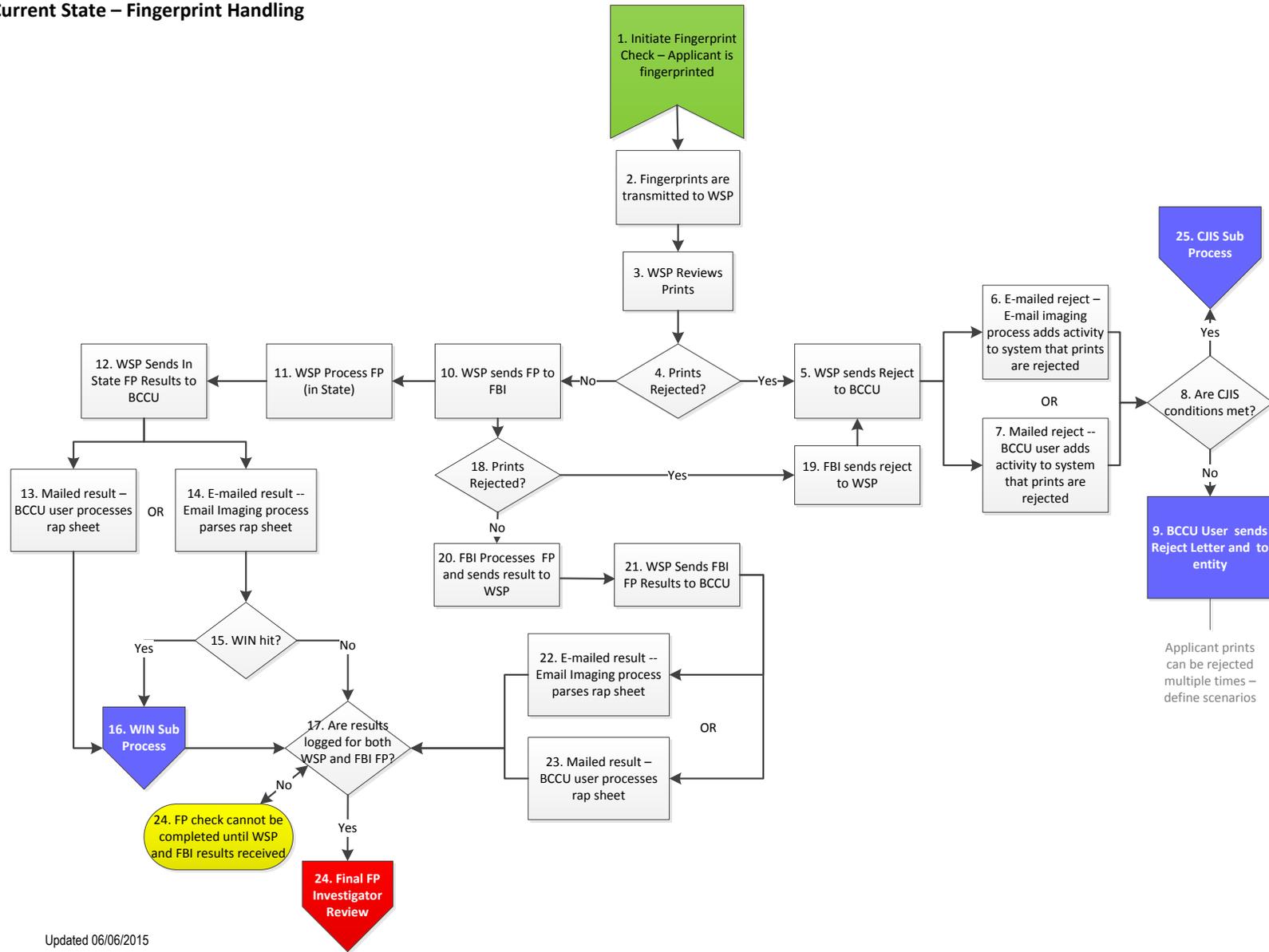
Updated 11/05/2015

Future State – Fingerprint Result E-mail Imaging Process (pg. 5)



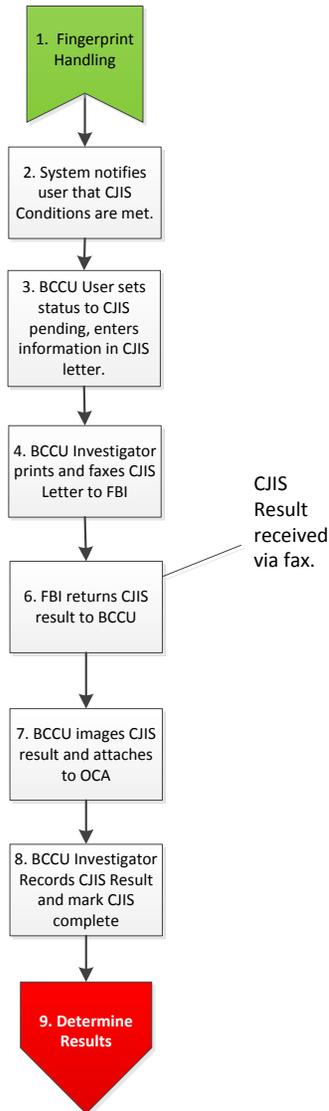
Updated 11/05/2015

Current State – Fingerprint Handling



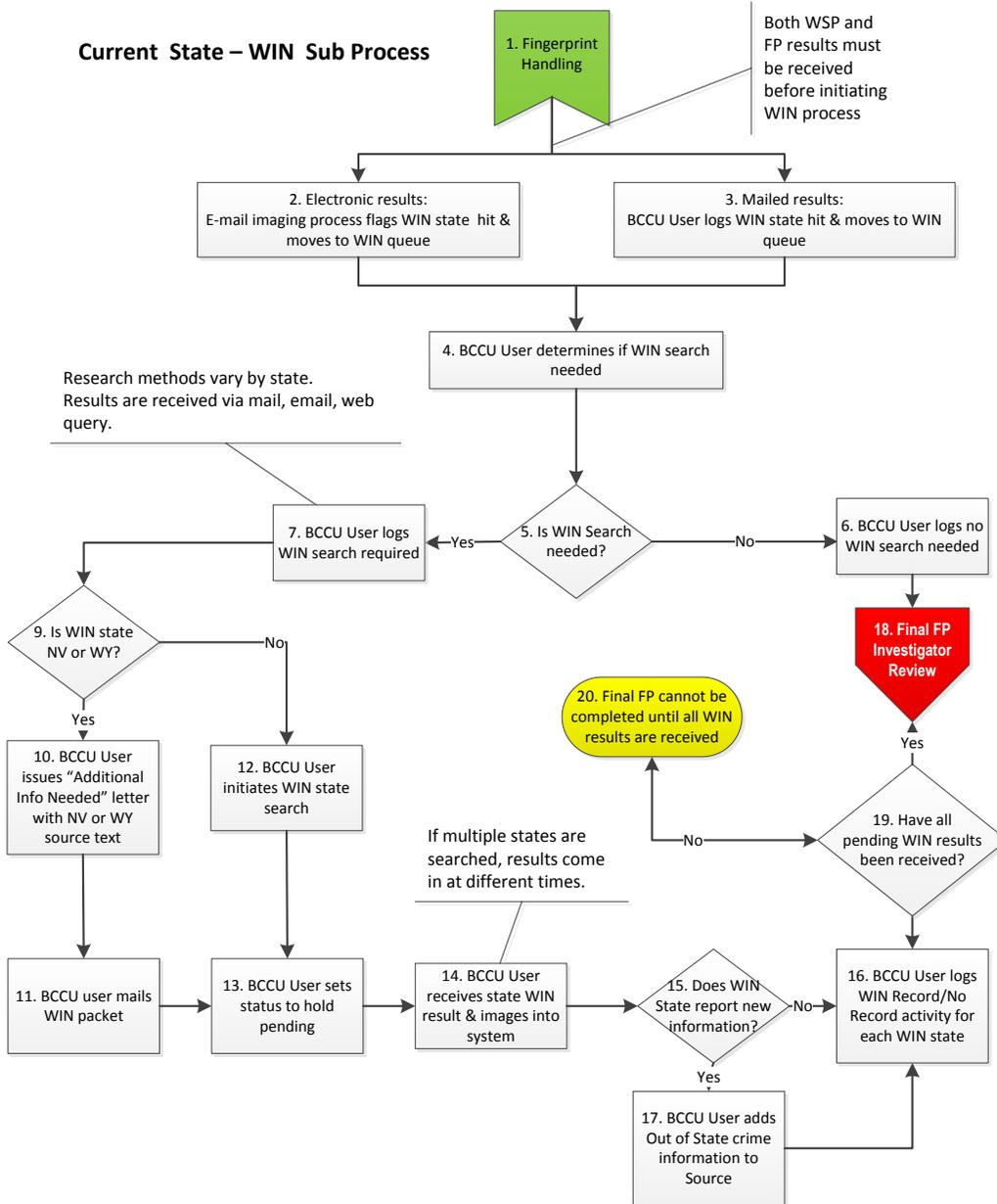
Updated 06/06/2015

Current State – CJIS Sub Process

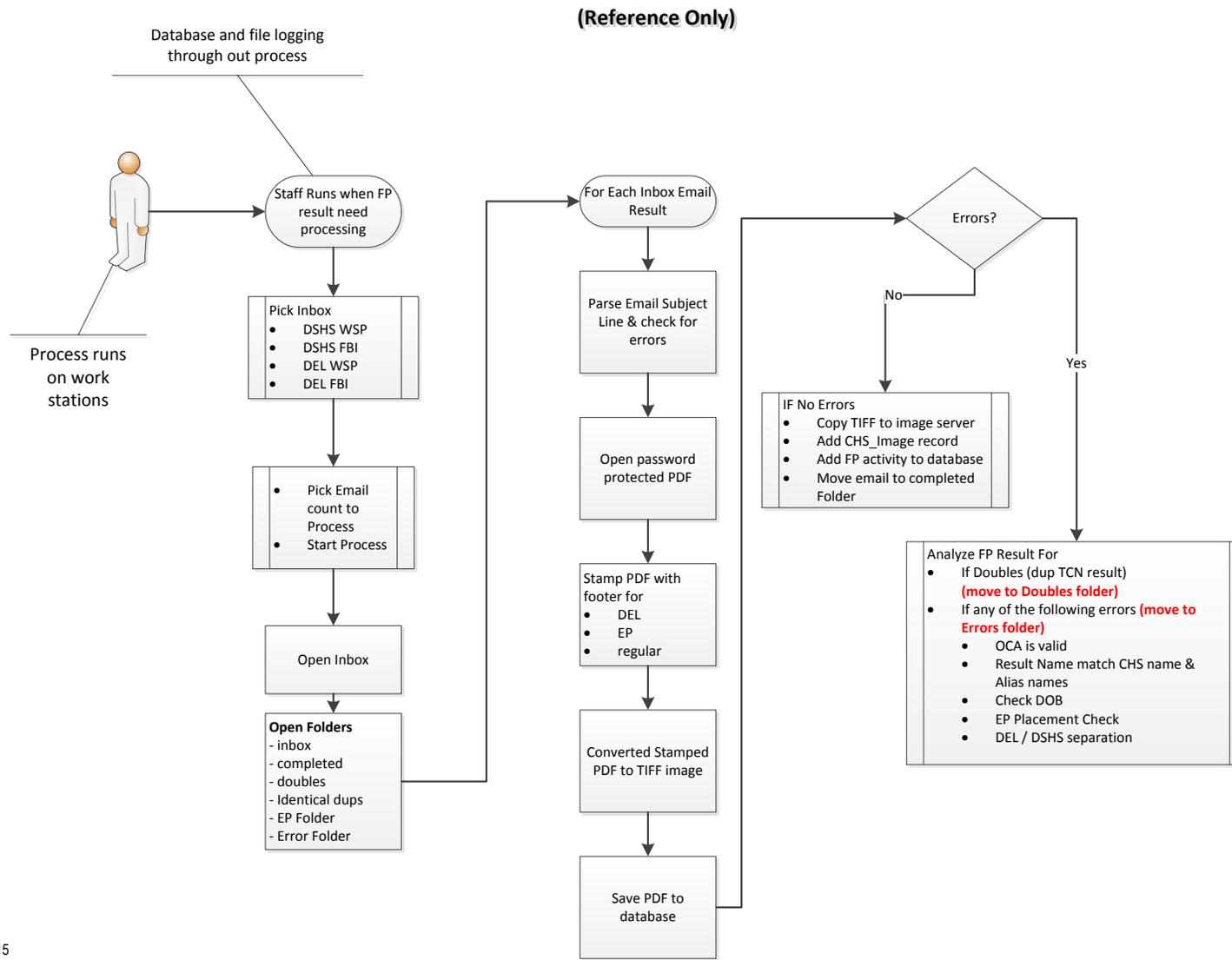


Updated 11/05/2015

Current State – WIN Sub Process



Current State – Fingerprint Result E-mail Imaging Tool



Updated 06/06/2015

6.12 Documents and Imaging

This section describes the requirements, business rules and process for system-generated documents and for providing BCCU users a method for uploading, using, and distributing documents in the Background Check System.

Requirements Table 6.12 – Documents and Imaging		
Requirement Type (F/NF)	Requirement Number	Function/Feature - Requirement
F	12.1	The system must have the ability to create, view and store system-generated documents.
F	12.2	Provide a method for BCCU user to scan, upload, store, and view supporting documents and rap sheets. Example: court documents, affidavits, legal opinions, and rap sheets are types of supporting documents.
F	12.3	Provide the ability to associate system generated documents and scanned documents to a POI or OCA.
F	12.4	For documents originating as paper and imaged into the system, the format must be TIFF or PNG.
F	12.5	Associate documents to specific inquiries, person of interest records, entities, etc.
F	12.6	Date stamp a document when it is created, scanned, or uploaded.
F	12.7	Retrieve and display stored documents and images.
F	12.8	Ability for users to view and print documents
F	12.9	Scan and upload standard document types. (Court documents, affidavits, Compromised Identity Card, AAG opinions, rap sheets, etc.)
F	12.10	Cross-reference documents by POI, OCA, data source (registry, WSP, AOC), and date created.
F	12.11	The system must maintain document templates for system-generated documents. The templates will specify the general layout of the document and the data to include in the document. Document types include letters, forms, and mailing labels or envelopes.
F	12.12	Populate the selected document template with data retrieved from the database.
F	12.13	Use United States Postal Service (USPS) standards for the formatting of addresses on all system-generated documents that will be mailed.
F	12.14	Add user name in the printout footer.
F	12.15	For electronic documents that come to us in electronic format (FP rap sheets, e-mails) or are generated by the system in electronic format (result letters), the electronic document must be retained in electronic format and remain usable, searchable, retrievable and authentic for the length of the designated retention period.
F	12.16	Apply document naming conventions to identify the type of document stored in the system.

Business Rules Table 6.12 – Documents and Imaging	
BR#	Rule Description
12000	Purpose: To take hard copy documents that is received (i.e. affidavit, court docs, correspondence, etc.) and convert them to image/PDF. Update the database by associating Image/PDF with a background check inquiry, person of interest; Give each Image/PDF a processing category/sort that staff can use to pull a category of similar work items.
12001	Hardware: Kodak Document Scanner (already being used by BCCU). Computer Workstation (Windows) to run a imaging tool that controls the scanner and processes the image/PDF created
12002	Document Types to Process: Court Documents; Affidavit; WSP or FBI FP Results that are received as a hard copy; Potentially WIN Result; any other hard copy document that needs to be kept as part of the background check record.
12003	System Usages: Reports on Image types stored; display associated images for an OCA or POI; record retention purging. Images are used by BCCU investigator for processing background check and certain images are transmitted to entity as part of the background check result.
12004	Documents are scanned using existing DSHS equipment.
12005	Scanned images are assigned a Document Type.
12006	Scanned images are assigned to a POI or an OCA.

Supporting Documents Table 6.12 – Documents and Imaging	
The following supporting documents will be provided to the successful vendor at time of requirements verification:	
Name	Location
Background Check Result Templates and Merge Text	Appendix O

Current State – Document Imaging
 (Future state will be determined with development team)

Note: this is for reference only. Need to identify how imaging will be done in BCS.

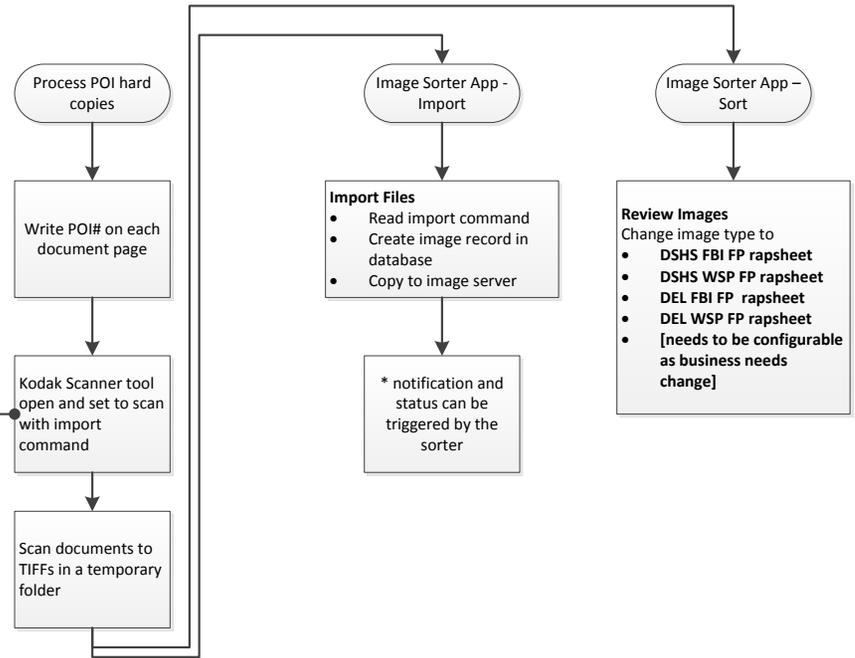
Tool runs on work stations connected to Kodak Image Scanner



Only portion of this tool that is needed for BCS is:

- Import scanned images
- Sort scanned images

- Import Command Name**
- **aps-** : Adult Protective Services.
 - **rush-** : Daily rush code, Community Protection, New Hire, Initial Contract, Initial License, State Employee.
 - **reg-** : All disclosure questions marked NO.
 - **mgr-** : Documents for Manager or Supervisor review.
 - **self-** : One or more of the disclosure questions marked YES.
 - **rej-** : Form has incomplete or blank information.
 - **fp_req-** : "Fingerprint Required" indicated on form.
 - **court-** : Court Documents or Affidavits
 - **poi(poi#)-** : Used to image directly to an existing POI in CHS.
 - **fp_reject-** : Incomplete forms with fingerprint card.
 - **fp_incmail-** : Authorization form with fingerprint card.
 - **fp_resub-** : Authorization form with a resubmitted fingerprint card.
 - **pub_disc-** : Applicant request for background check information.
 - **fp_cjis-** : Faxed or mailed results from the FBI.
 - **int_rls-** : Internal Release Requests
 - **PS_dup-** : Sort to place duplicate forms CHS will not allow you to enter
 - **PS_del-** : Items for deletion
 - **Proc-** : Items for Processing Supervisor Review
 - **tech_sup-** : Items for Technical Supervisor (Errors)
 - **TS_del-** : Items for deletion (Technical Supv)



Updated 06/25/2015

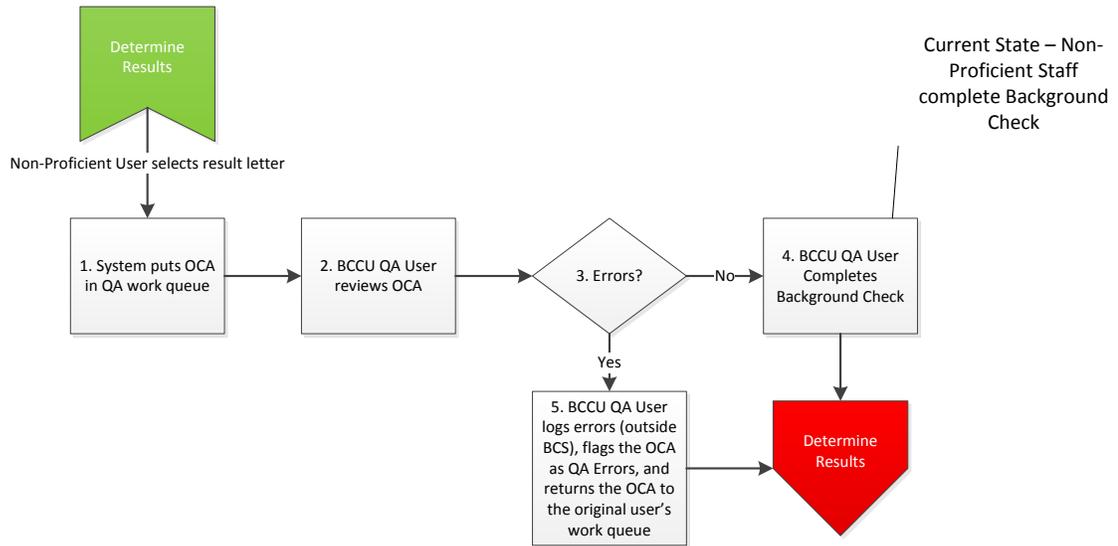
6.13 Quality Assurance

This section describes the requirements, business rules and process for allowing BCCU quality assurance staff to perform quality assurance reviews on work performed by non-proficient investigators prior to distributing results.

Requirements Table 6.13 – Quality Assurance		
Requirement Type (F/NF)	Requirement Number	Function/Feature - Requirement
F	13.1	Provide a method for certain BCCU Quality Assurance (QA) user role to perform quality assurance review on the work performed by non-proficient staff after the result is chosen and prior to distributing background check result to entity.
F	13.2	Provide a report for QA users to monitor the POI matching work of non-proficient staff.
F	13.3	Provide the ability to place BCCU Investigator Level 1 and BCCU Investigator Level 2 users in a non-proficient status or proficient status.

Business Rules Table 6.13 – Quality Assurance	
BR#	Rule Description
13000	QA errors are logged outside of the BCS.
13001	When a BCCU Level 1 or Level 2 Investigator is in non-proficient status, the background check results that they choose must not be distributed to the entity until the BCCU QA user has reviewed and approved them for release.
13002	If the BCCU QA user finds an error during QA review, the BCCU QA User flags the OCA as having QA Errors and reassigns the OCA to the BCCU Investigator who processed the background check for correction.
13003	When an OCA has been returned to the BCCU Investigator due to error, the OCA appears in the user's queue with a flag indicating that it's been returned from QA.
13004	To conduct the QA review, the BCCU QA User will view all information that was available to the BCCU Investigator to evaluate the accuracy of the selections.
13005	To be in proficient status, BCCU Level 1 and Level 2 Investigators must meet the current BCCU accuracy and volume performance standards.
13006	The system places an OCA in the QA work queue when the following conditions are met: 1) Investigator is in non-proficient status; and 2) the Investigator has chosen a result and indicated the OCA is complete.

Future State – Quality Assurance
(Current state is similar)



Updated 06/08/2015

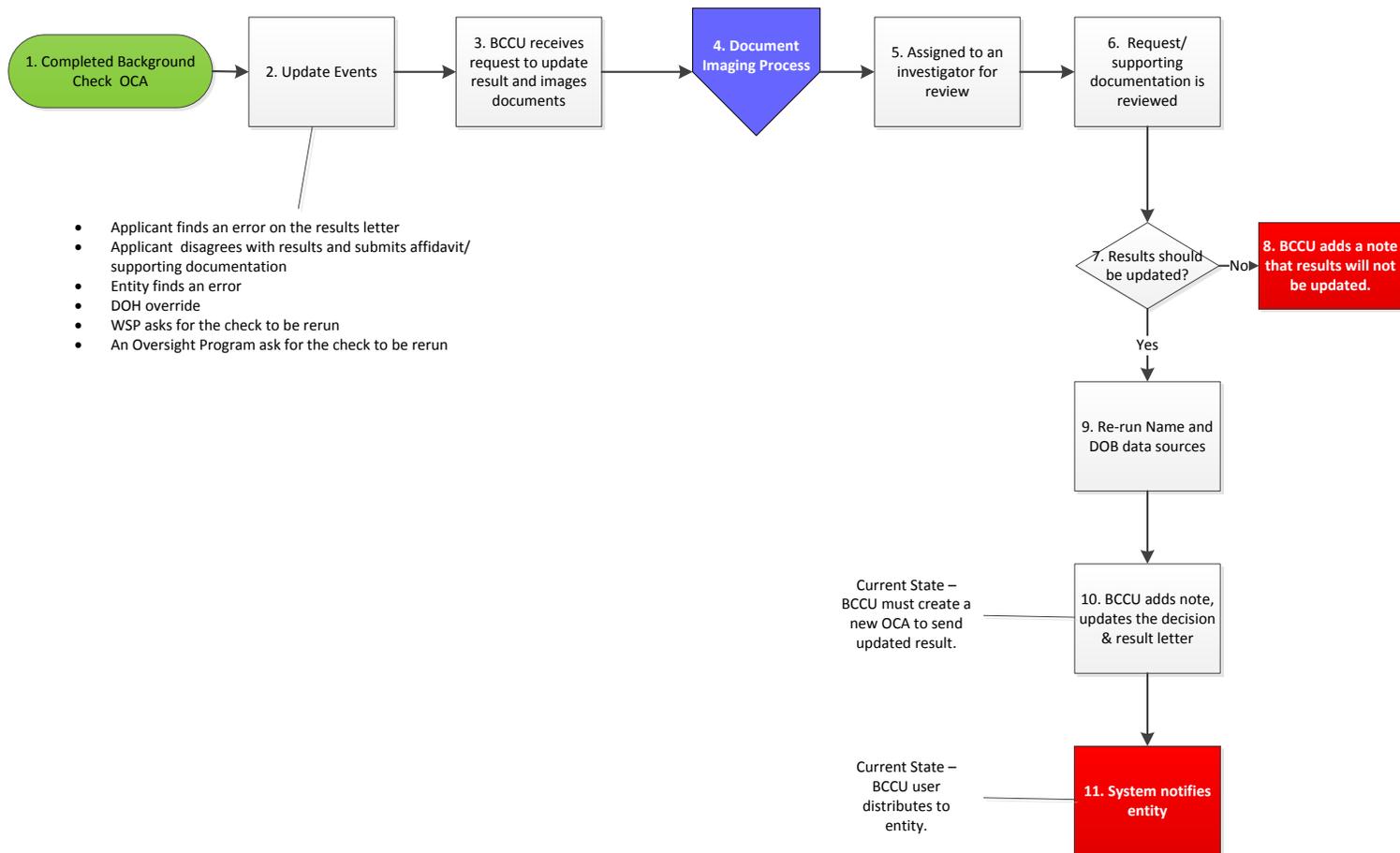
6.14 Background Check Update

This section describes the requirements, business rules and process for updating a background check result after additional information is received by BCCU.

Requirements Table 6.14 – Background Check Update		
Requirement Type (F/NF)	Requirement Number	Function/Feature - Requirement
F	14.1	Provide a method for BCCU to update a result when new information is received.
F	14.2	Provide the ability to retain the history of the original background check result as well as the updated result information.
F	14.3	Provide the ability to track the activities associated with the original and updated background check.
F	14.4	Notify the entity when an updated background check is sent.

Business Rules Table 6.14 – Background Check Update	
BR#	Rule Description
14000	A Background Check Result may be updated if one or more of the following events occur: Applicant finds an error on the results letter; applicant disagrees with results and submits affidavit; entity finds an error, WSP asks for the check to be rerun; or an Oversight Program asks for the check to be rerun.
14001	An applicant may have multiple applications with different result letters that need to be updated.
14002	The BCCU User may use supporting documentation to update one OCA or multiple OCAs.
14003	When a background check is updated, the BCCU User may receive additional documentation from the applicant in support of their request to update their record.
14004	When a background check is updated, the system must display a history of the original result and the updated result.
14005	BCCU receives supporting documentation by mail, fax or email and scans the information into the system and associates with the OCA or the POI depending on the type of information received.
14006	The BCCU User will re-run all Name/DOB data sources prior to updating the background check result.
14007	The BCCU User will enter notes documenting the request to update applicant result and the outcome of the request.
14008	When background check is updated, the result type in application summary will show "updated" after the result letter type and display the update date.
14009	Different inquiry types have different disqualifying crimes. An applicant may have several applications with different result letters.

Future State – Background Check Update Process
(Current state is similar)



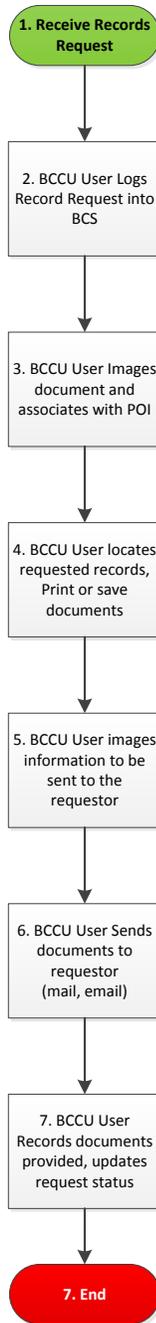
6.15 Records Request

This section describes the requirements, business rules, and process for tracking and documenting requests for background check records in the Background Check System.

Requirements Table 6.15 – Records Request		
Requirement Type (F/NF)	Requirement Number	Function/Feature - Requirement
F	15.1	The system must provide a method for BCCU user to record and track internal and external requests for background check records.

Business Rules Table 6.15 – Records Request	
BR#	Rule Description
15000	The system tracks a Records Request Log including the following information: Request date, requester (Last Name, First Name), POI, oversight program, request source, image of documents sent to requester.
15001	Records requests are associated with a POI.
15002	BCCU Request Statuses are: Open, Closed.

Future State – Background Check Records Request
(Current state is the same)



Updated 06/08/2015

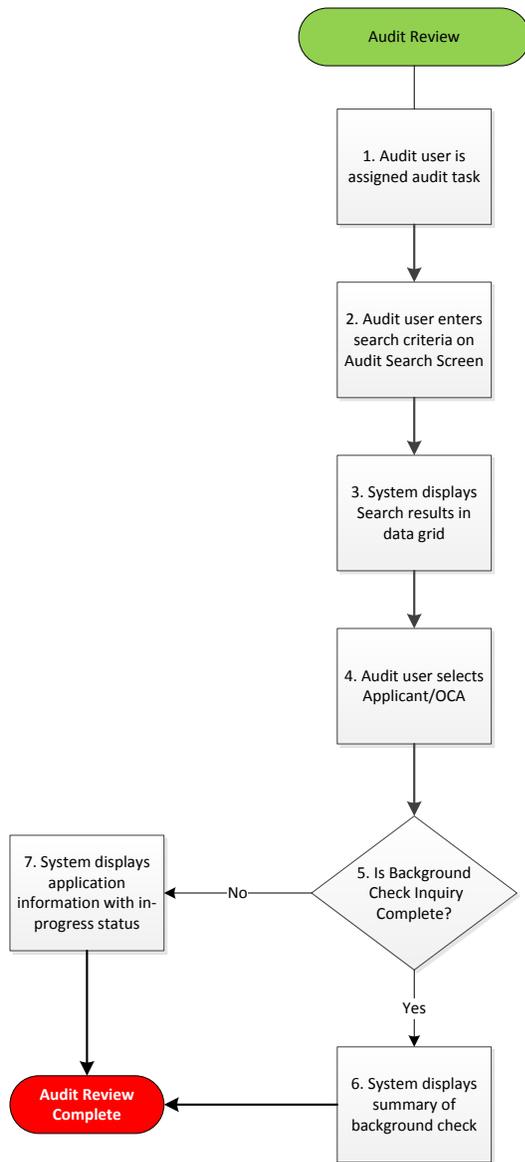
6.16 Audit Review

This section describes the requirements, business rules, and process for allowing internal audit users and DSHS oversight users to search and view background check inquiries.

Requirements Table 6.16 Audit and Oversight Review		
Requirement Type (F/NF)	Requirement Number	Function/Feature - Requirement
F	16.1	The system must have the capability for DSHS programs and internal audit users to oversee background check activities and hiring/contracting decisions.
F	16.2	Provide a method for audit users to search for background check records and return a list of matching records.
F	16.3	Provide the ability for audit user to download search results into an Excel spreadsheet.
F	16.4	Provide the ability for audit user to access an audit review screen to display a summary of a specific background check inquiry (OCA) that can be opened from the search result.
F	16.5	Audit function must search and return legacy records.

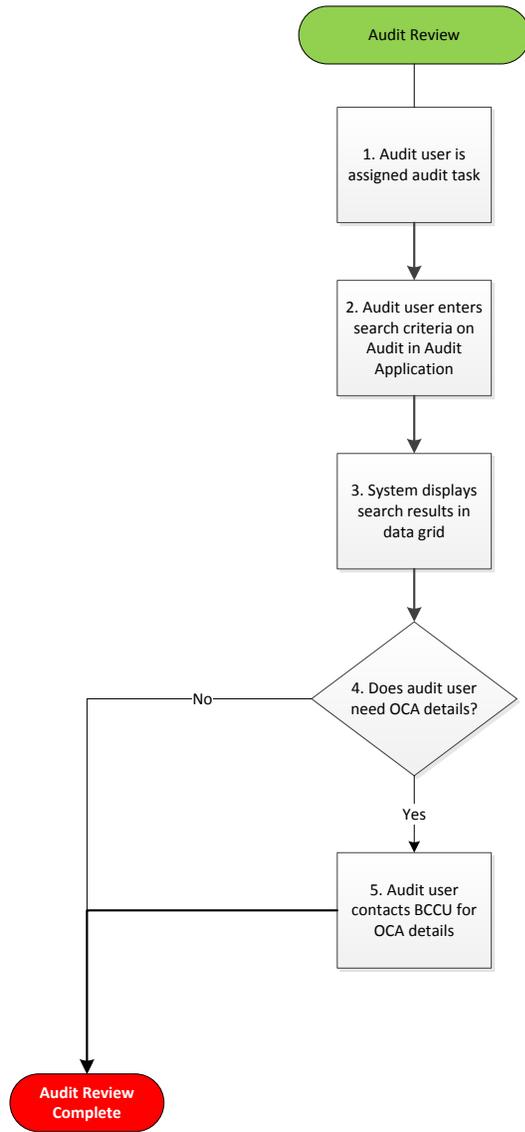
Business Rules Table 6.16 Audit and Oversight Review	
BR#	Rule Description
16000	Audit users do not submit background checks.
16001	Audit search options include First Name, Last Name, BCCU Account #, Entity Name, City, Status, Inquiry Type, Social Security Number, Date Created (date range), and OCA#.
16002	Audit users who are assigned to a specific DSHS administration, may only view background checks submitted within their administration hierarchy.
16003	Audit users who are assigned department-wide access may view background checks submitted by any DSHS administration.
16004	Audit search includes completed and in-progress OCAs.
16005	Search results will display the information listed in BR 16001 and result letter types, completion date, and engagement decision/engagement date.
16006	The OCA summary on the audit review screen will <u>not</u> include OIG results, links to result letters, self-disclosures, or other source information.

Future State - Audit Review Workflow



Updated 06/01/2015

Current State - Audit Review Workflow



Updated 06/01/2015

6.17 Department of Health Review Inquiry

This section describes the requirements, business rules and process for meeting the legal requirement for the Department of Social and Health Services to share the results of long-term care fingerprint checks with the Department of Health.

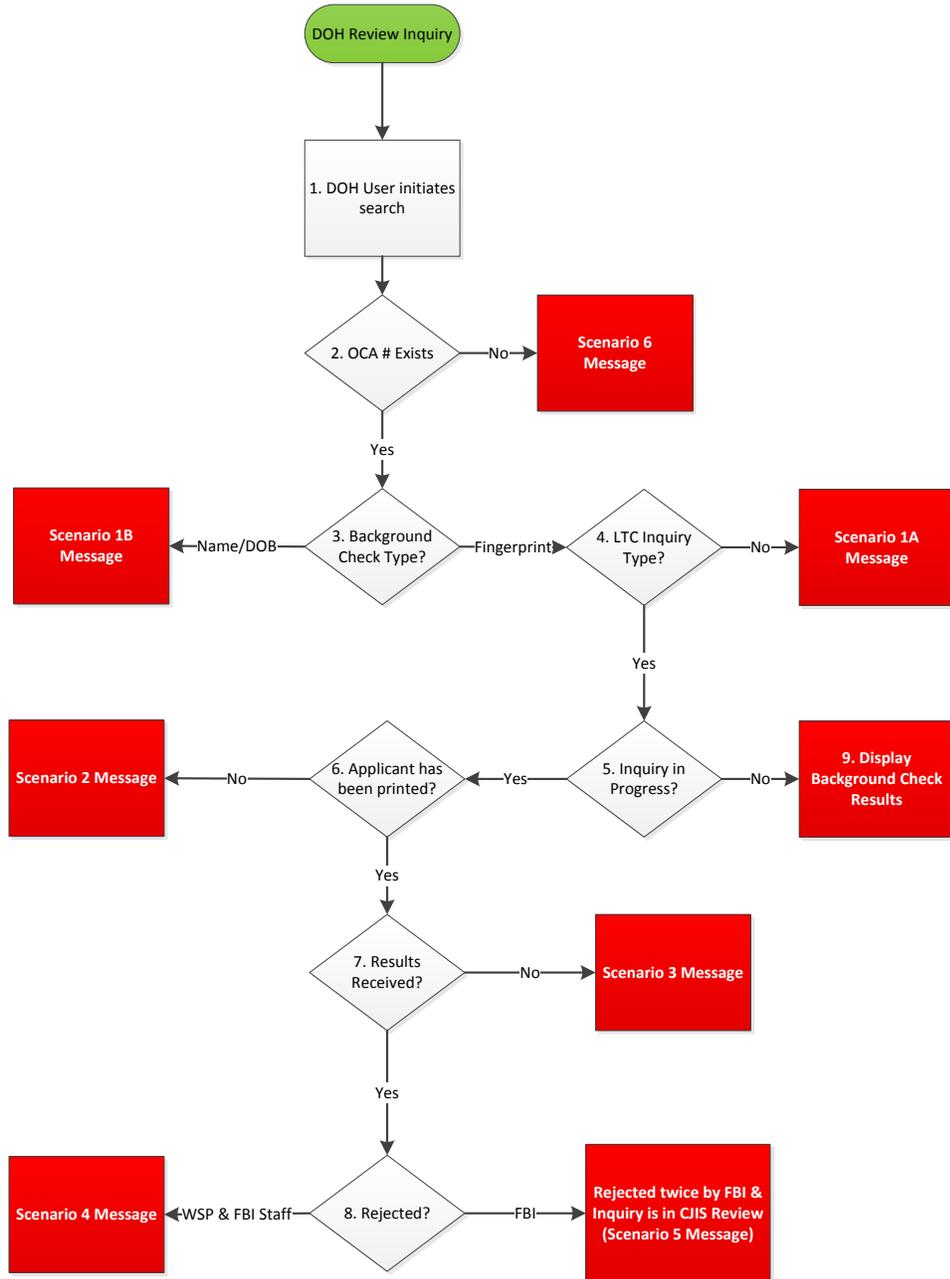
Requirements Table 6.17 – Department of Health Review Inquiry		
Requirement Type (F/NF)	Requirement Number	Function/Feature - Requirement
F	17.1	Provide a method for Department of Health (DOH) users to search for long-term care OCA#s and view the results of valid long-term care fingerprint results. See user role descriptions in Section 6.18.
F	17.2	Return appropriate search message to user for each search scenario. (See business rules and flow)

Business Rules Table 6.17 – Department of Health Review Inquiry	
BR#	Rule Description
17000	Search requires a valid OCA # from a long-term care inquiry type to return background check details.
17001	DOH review must be able to return legacy data.
17002	Scenario 6: When user enters an OCA that does not exist in the system, show this message – "OCA does not exist. Enter a valid long-term care fingerprint OCA." Do not display background details.
17003	Scenario 1a: When user enters OCA where background check type is fingerprint and inquiry type is not a long-term care inquiry type, show this message - "OCA entered is not a long-term care fingerprint check." Do not display background details.
17004	Scenario 1b: When user enters OCA with any Inquiry type and background check type is Name/DOB. Show this message - "OCA entered is not a long-term care fingerprint check." Do not display background details.
17005	Scenario 2: When user enters OCA where inquiry type is long-term care and background check type is fingerprint check and inquiry is in process and applicant has not been printed, show this message- "Fingerprint check is not complete. Applicant has not been printed." Do not display background details.
17006	Scenario 3: When user enters OCA where inquiry type is long-term care and background check type is fingerprint type and inquiry is in process, and applicant has been printed, show this message -"Long-term care fingerprint check is in progress." Do not display background details.
17007	Scenario 4: When user enters OCA where inquiry type is long-term care and background check type is fingerprint type and inquiry is in process and applicant prints were rejected by WSP or FBI, show this message - "Applicant prints rejected. Applicant must be reprinted." Do not display background details.
17008	Scenario 5: When user enters OCA where inquiry type is long-term care and background check

Business Rules Table 6.17 – Department of Health Review Inquiry	
	type is fingerprint and inquiry is in process and applicant prints were rejected twice by FBI and inquiry is in CJIS review, show this message "Inquiry is pending FBI CJIS review" Do not display background details.
17009	Valid search returns Applicant details (Applicant name, date of birth, SSN); Fingerprint Check Details (OCA#, Result Date, Received Date, Result Type); Related documents (AOC Rap Sheet, WSP Rap Sheet, WSP FP Rap Sheet, FBI FP Rap Sheet, Source Documents.)
17010	If the background check result was based on a shared fingerprint, the system displays a note in the Fingerprint Details section: "Based on fingerprints shared from OCA# [OCA#] on [DateofOCA]".

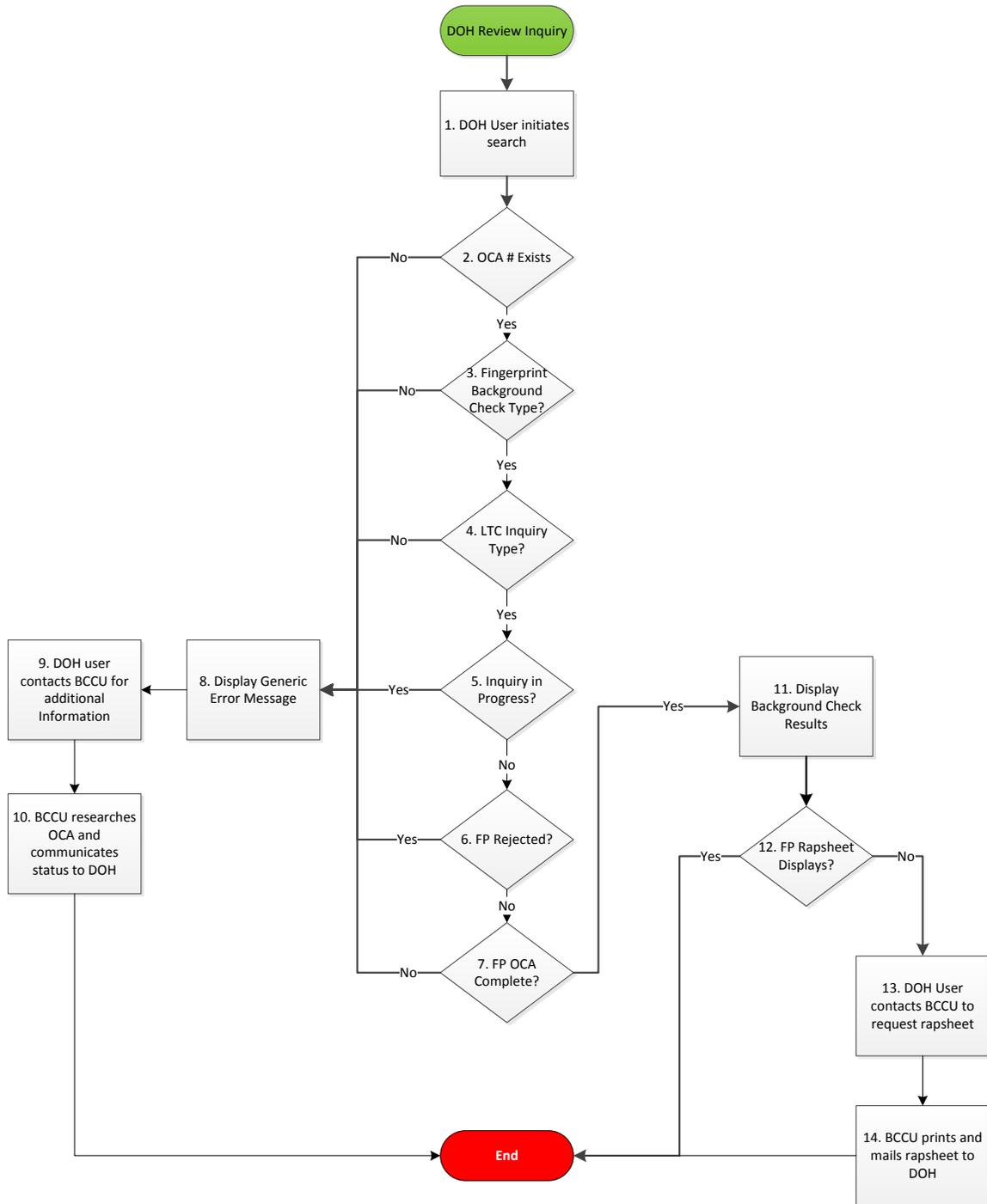
Supporting Documents Table 6.17 – Department of Health Review Inquiry	
The following supporting documents will be provided to the successful vendor at time of requirements verification:	
Name	Location
Current DOH Web Application – Screen Examples	Appendix V

Future State - DOH Review Inquiry



Updated 06/01/2015

Current State - DOH Review Inquiry



Updated 06/01/2015

6.18 Entity Accounts, Users and User Roles

This section describes the requirements for managing records for users and entities. Entities are added to the system in two ways; 1) Nightly upload of data from external databases, 2) manually by system users. Entities added to the system through the nightly upload cannot be edited within the system.

Primary entities are the entities with the authority to submit background checks to the Background Check Central Unit. The primary entity is the BCCU account holder. A secondary entity is a contractor, licensee, or other entity who will be the final recipient of the background check result.

System users are added manually by other users with access to functionality based on user roles. User roles are based on a hierarchy of system functionality and grouped by User Type. User Types are Entity, Program, BCCU, and Partner (DOH).

User Role Descriptions		
User Type	User Role	Description
Program	Program Oversight - Administrator	Authorize Entities to access BCS and manage users for entities with inquiry types associated with the user's Administration/Division.
Program	Program Oversight	Oversee entity background check activities.
Program	Audit User	Search for and view limited results of a background check.
Entity	BCS User	Entity user who submits and receives results of background checks.
Entity	BCS Admin	Entity user who manages users for an entity.
Partner	DOH User	DOH staff who view results of completed background checks for designated inquiry types.
BCCU	Investigator Level 1	BCCU user who processes background checks.
BCCU	Investigator Level 2	BCCU user who processes background checks and researches results.
BCCU	Quality Assurance	BCCU User who trains and monitors BCCU Investigators; manages workload and performs other management activities.
BCCU	Management	BCCU User who manages users, workload assignments, and system tools.
BCCU	Accountant	BCCU User who reconciles billing sources.
BCCU	Equivalency	BCCU User who views background checks.

Requirements Table 6.18 – Entity Accounts, Users, and User Roles		
Requirement Type (F/NF)	Requirement Number	Function/Feature - Requirement
F	18.1	The system must have the ability to add/change/close BCCU accounts.
F	18.2	Ability to maintain contact information for an account as a primary entity profile.
F	18.3	Ability for entity account users to track and maintain secondary entity contacts.
F	18.4	Ability to associate DSHS organizational information to each account (e.g., administration and division).
F	18.5	Ability to associate an inquiry type to each account (Inquiry types include: nursing home, state employee, provider, provider-internal, licensed childcare).
F	18.6	Capability to process a nightly upload from external databases to automatically add/close/update entity accounts. Automatic upload of data comes from ADS and DOH.
F	18.7	Ability for users to add and update certain contact information to the primary entity such as contact name and e-mail.
F	18.8	Prevent automatically uploaded data, such as from DOH or ADSA, from being changed by a user.
F	18.9	Option for entities to designate an email address to receive notifications.
F	18.10	Ability to add/change/disable Users.
F	18.11	Provide access to system functionality based on assigned user roles.

Business Rules Table 6.18 – Entity Accounts, Users, and User Roles	
BR#	Rule Description
Entity Auto Upload	
18000	Entities may be added manually or through the auto upload.
18001	The system interfaces with two programs to upload entities automatically: ADS and DOH.
18002	The ADS nightly upload sends all records each night. When BCS receives the ADS upload file, the system updates the entity records with information received from ADS; no records are deleted or dropped. If a previously received record is not present in the latest upload, the system will set the record to "Disabled".
18003	The data received from the nightly uploads is stored in the same tables, though data is not shared between the two programs. DOH uploads data for ADS Private Home Care Agencies, but ADS upload process does not update data for these entities.
18004	The upload files include a field for License Number. This field is imported into the system, but may be null.
18005	The license number field is used only to search for entities that are added to the system through the nightly upload.
18006	For accounts without a license number, the legacy data includes a "-x" in the License Number field rather than allowing the field to be null. BCS may allow a null value in License Number.
18007	The system notifies the Oversight User when an entity has been added through the Nightly Upload.
Add Entity	

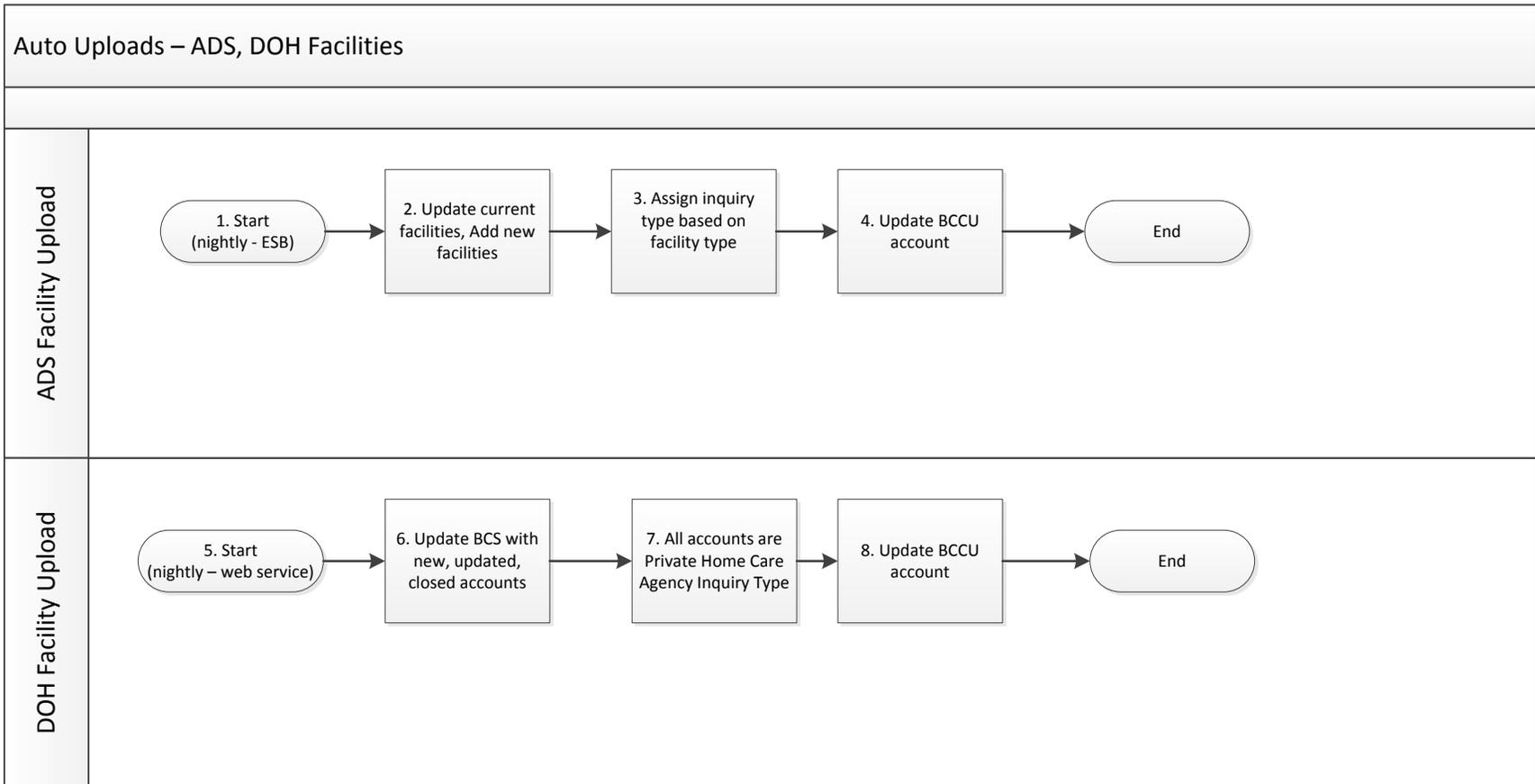
Business Rules Table 6.18 – Entity Accounts, Users, and User Roles	
18008	System Users may add a new entity to the system. See User Role Description section.
18009	Users are blocked from adding an Entity for any inquiry type that is automatically added into the system as part of the ADS or DOH nightly updates.
18010	The system follows the rules described in "Account Number Nightly Updates" when assigning BCCU Account Numbers.
18011	If the entity was added to the system manually (not through the Nightly Upload Process), the entity contact information may be edited. Entity Contact Information includes phone/fax, address, owner...
18012	If the entity was added to the system through the Nightly Upload Process, the entity contact information may not be edited.
18013	BCS Admin users may add a Secondary Entity to the Entity Account Profile.
18014	Entities are not required to have secondary entities.
18015	Secondary Entities are assigned a unique ID that is linked with the primary entity's account number.
Entity Activation	
18016	Oversight Users may generate Join Letters for a single entity or for multiple entities at a time.
18017	The Join Letters are generated only once and stored in the system. (See Requirement 9.1. This requirement is intended to abide with the state laws about how to store and display Rap Sheets.)
18018	When a new entity is added, (either manually or through the auto upload) the system generates the Entity Registration Key.
18019	The Entity Registration Key is printed on the Join Letter.
18020	When a user registers the entity and the registering user is an existing user: <ul style="list-style-type: none"> a. the system will set entity status to Active, and b. the system will associate the user with the entity, and c. the system will display the Thank You page with a link to View Account Settings, and d. the system will send an activation confirmation (notification) to the user who registered the entity.
18021	When a user registers the entity and the registering user is a new user: <ul style="list-style-type: none"> a. the system will set entity status to Active, and b. the system will associate the user with the entity, and c. the system will set user status to Active, and d. the system will display the Thank You page with a link to Access the Background Check System (login), and e. the system will send an activation confirmation (notification) to the user who registered the entity.
18022	When system sets entity (and user) status to active, the system will send an activation confirmation to the user who registered the entity.
18023	The system sends an email notification to the Oversight User when an entity has registered.
18024	The system sends an email notification to the BCS Administrator User when the entity has been activated.
User Login and Registration	
18025	If hosted by the State, the external user will authenticate via Secure Access Washington/SEAP.
18026	If hosted by the State, the internal user will authenticate via Active Directory.
18027	The User Agreement is updated through a system tool (i.e. the BCCU staff can update the

Business Rules Table 6.18 – Entity Accounts, Users, and User Roles	
	agreement without a change request to the development team).
18028	The user is required to agree to the User Agreement when they register.
18029	If the User Agreement has been updated since the user last logged in, the user is required to agree to the User Agreement before accessing the system.
18030	Entity Registration may be completed by a new user through the User Registration Process, or by an existing user through the User Settings.
18031	When a user registers an entity, the system validates the Entity Registration Key and allows the user to enter the BCS Administrator information.
18032	Entity Registration may be completed by a new user through the User Registration Process, or by an existing user through the User Settings.
User Management	
18033	A user must be registered in BCS before they can be assigned a user role or added to an entity.
18034	A user cannot be assigned to an entity which is not active.
18035	Authorized user must enter a valid Username and Account Type to associate a user with the entity.
18036	If the user being added cannot be found, display message, "[User] does not exist, please enter a valid User ID and Account Type or direct the user to create a new account and Register in BCS."
18037	If the user being added already has access to the entity, display a message "[User] already has access to [Entity]."
18038	If the new user is found, the Authorized User must select a User Role for the new user.
18039	If the user has been added, display a confirmation message. "[User] has been assigned to [Entity]."
18040	An Authorized User may only search users who are associated with an entity that the Authorized User manages. (Examples: Oversight Users may only search for users assigned to entities with inquiry types managed by the Oversight User. Entity Administrators may only search for users who are assigned to entities that the Entity Administrator is assigned as administrator.)
18041	Only users associated with an entity appear in the results list when the Authorized User is an Entity or Oversight User. Registered users who are not associated with an entity do not appear in the list for Entity or Oversight users.
18042	BCCU Users may search all users registered in BCS.
18043	User Statuses are Pending, Active, Disabled
18044	User Status can't be pending once they have been activated.
18045	The Manage Users functionality will only be displayed for users who have a security role that allows User Management.
18046	If user profile has been updated, display message "User Profile for [User] has been updated"
18047	If a user status is set to disabled, then disable all field grids and hide access to account.
18048	The selected user profile will display all entities the user currently has access to and the Access Level for each entity.
18049	The selected user profile provides an option for changing the Access Level for assigned entities or removing an assigned entity.
18050	A user cannot edit their own access level or user role; the user can only edit their profile settings
18051	The entity must have at least one BCS administrator. You must add a BCS Admin before

Business Rules Table 6.18 – Entity Accounts, Users, and User Roles	
	removing one.
18052	The system displays a tool-tip next to access level stating that, “There must be at least one BCS administrator. You must add a BCS administrator before removing one.”
18053	The primary BCS administrator is the person that registered the entity originally.
18054	The system sets the next oldest BCS administrator as Primary Administrator after the previous primary is disabled.
User Roles	
18055	A user may have more than one user role. User roles are independent of login access (SAW or AD).
18056	If a user has more than one user role assigned, the system will either: a) provide access to all functionality included in all user roles assigned to the user, or b) allow the user to select which role to sign in as (e.g. which dashboard to display).
18057	If a user has more than one user role assigned and the system requires the user to select which role to use, the system allows the user to change roles (e.g. switch dashboards) without having to log out of the system.
18058	Some user roles are assigned access to inquiry types, rather than entities (i.e. DOH Lookup may only see inquiry types for long term care)
18059	User Roles are managed through a system tool. BCCU Management may update or create new user roles to assign to users without technical assistance.
18060	BCCU Investigators will have a quality assurance status if they are not proficient (Proficient=the investigator can work independently without Quality Assurance. This is assigned manually. Proficiency is an attribute of the BCCU Investigator user role).

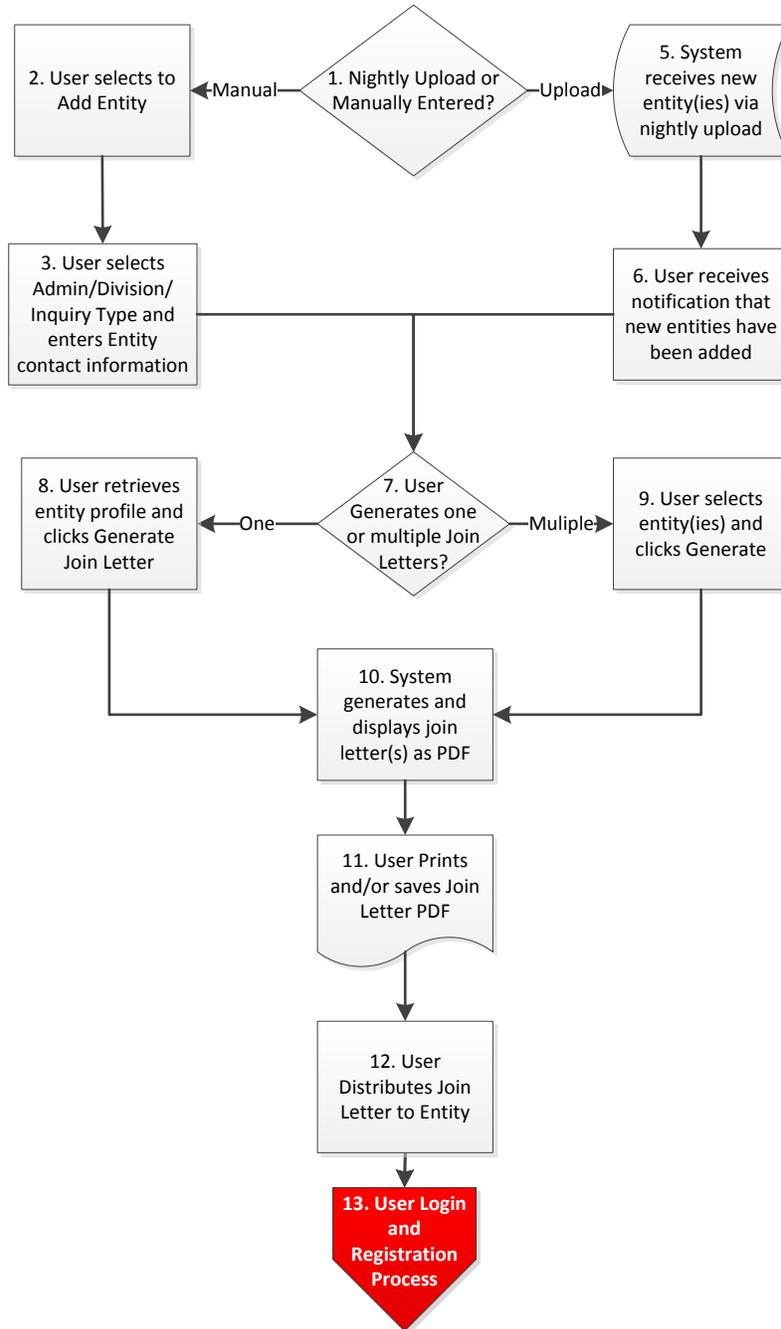
Supporting Documents Table 6.18 – Entity Accounts, Users, and User Roles	
The following supporting documents will be provided to the successful vendor at time of requirements verification:	
Name	Location
Account Number and Nightly Update Rules	Appendix S
User Role Functionality Table	Appendix W

Future State – Auto Upload



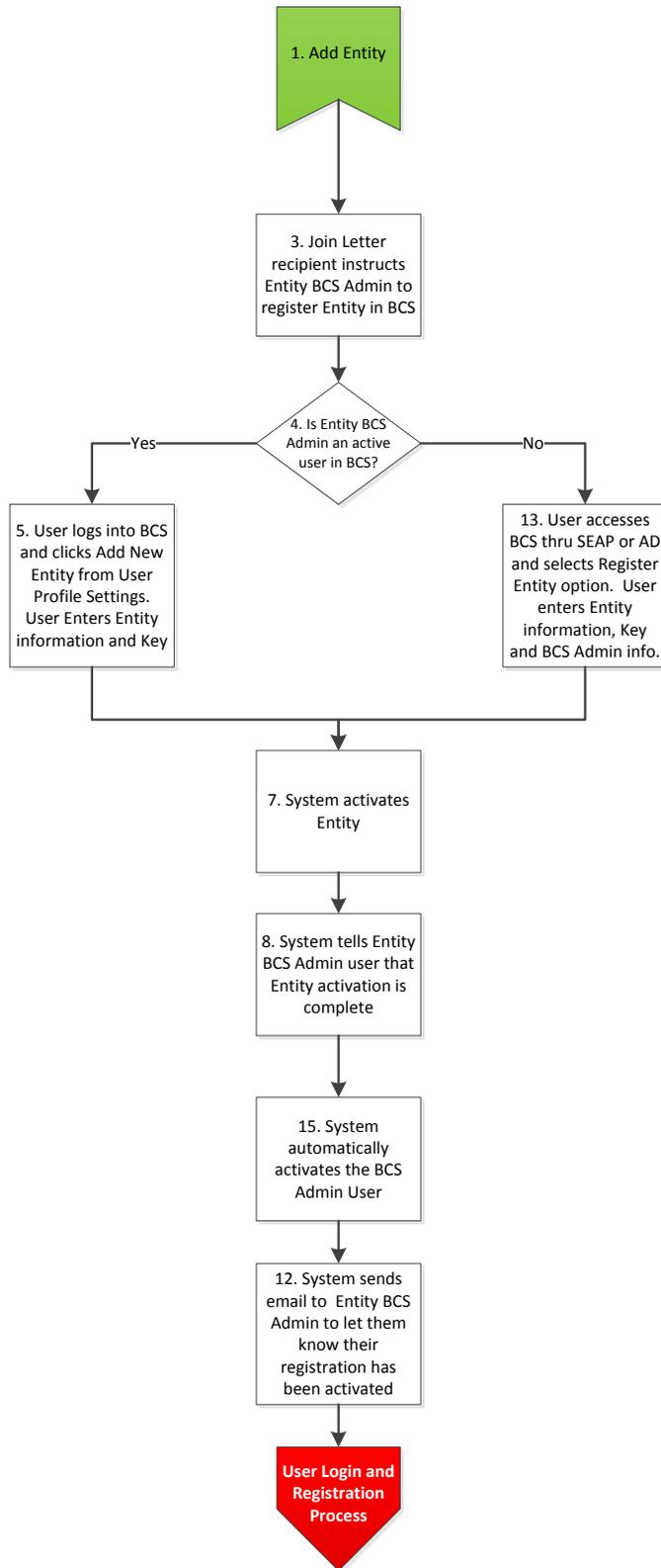
Updated 06/10/2015

Future State – Add Entity



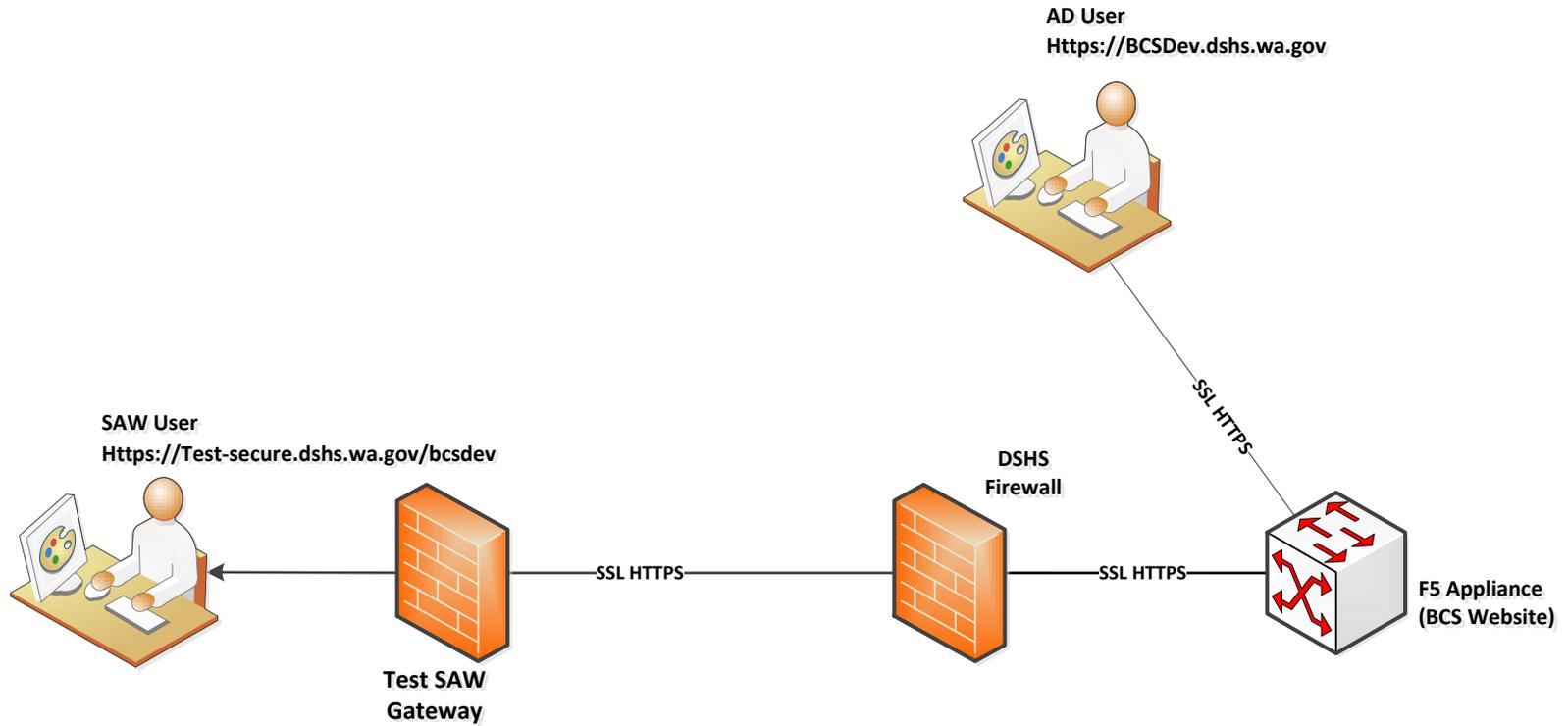
Updated 06/10/2015

Future State – Activate Entity



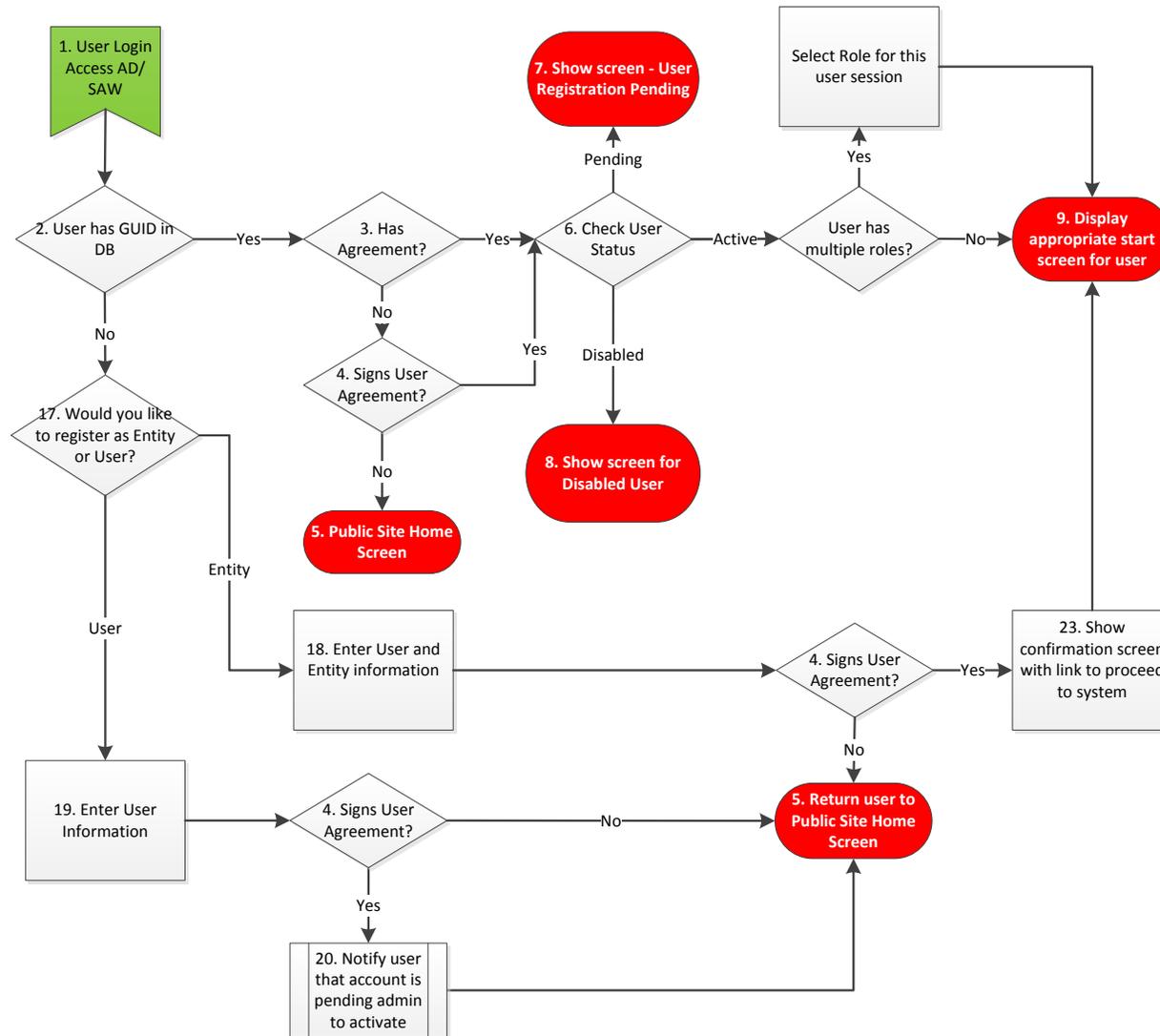
Updated 06/10/2015

Future State – User Login Access



Updated 06/10/2015

Future State – User Login and Registration Process



Updated 06/10/2015

6.19 Workload Management

This section describes the requirements for managing BCCU user workload. A Work Item (typically a background check or associated task) is assigned to a work queue based on the assigned status. The workload management functions will allow BCCU managers or leads to efficiently manage and monitor workload and make workload assignments and reassignments to respond to the changing needs of the production unit.

Requirements Table 6.19 – Workload Management		
Requirement Type (F/NF)	Requirement Number	Function/Feature - Requirement
F	19.1	The system must provide supervisors the ability to manage staff workload, such as by designating which staff will receive certain tasks or types of background checks, reassigning tasks, or temporarily blocking the system from automatically assigning tasks.
F	19.2	The system must have the capability to automatically assign background checks to a staff work list based on the type of background check, division, inquiry type, and where it is in the processing flow.
F	19.3	Provide a work list for each level of staff involved in processing background checks.
F	19.4	Move a background check to the next step in the processing workflow when a key task is complete.
F	19.5	Track key tasks and timelines and flag rush requests by putting them at the top of the user work queue.
F	19.6	Provide a method for each staff member to view the tasks in their work list.
F	19.7	Remove the inquiry from the processing work list once a final result is issued.
F	19.8	Maintain a history of staff assigned to each key task in the processing workflow.

Business Rules Table 6.19 – Workload Management	
BR#	Rule Description
19000	Work Queues are maintained in a system tool.
19001	Staff may be assigned to one or more work queues at a time.
19002	A work item may be assigned to a Work Queue automatically based on the status of the work item or manually by a user with the appropriate user role.
19003	A single Work Item is distributed from each Work Queue to assigned staff on an as available basis. (i.e. work may sit in a work queue and be assigned to a user's queue as the user becomes available, not distributed to a user's queue to await user availability).
19004	Staff/users do not have large queues except for work assignments in process/on hold/awaiting some particular action.
19005	A work item may be reassigned from one staff/user to another or returned to a queue.
19006	Work in each investigator's dashboard will be listed by priority and by the "date received" (i.e. oldest time stamp first)

Business Rules Table 6.19 – Workload Management	
19007	Priority of a work item is determined by the priority of the inquiry type and the applicant type. Inquiry Rush Types – priority processing By Inquiry Type RCS -- Initial License All State Employee HCS – Adult Protective Services Emergency Placement By Applicant Type New Hire Initial Contract Initial License
19008	Staff/users work assignments may be change at any time during a work day.
19009	A work type may be added to the system that doesn't include system activities (i.e. phone or email assignments).
19010	A user may search for work item (e.g. application/OCA) and perform an action on that work item regardless of which work queue the item is assigned.
19011	A QA or Manager role may reassign all work, or an individual work item from a staff/user's queue to another user or return all items work queues.

Supporting Documents Table 6.19– Workload Management	
<p style="color: red;">The following supporting documents will be provided to the successful vendor at time of requirements verification:</p>	
Name	Location
Statuses, Triggers, Next Steps, and Workload Queues	Appendix P

6.20 Customer Support

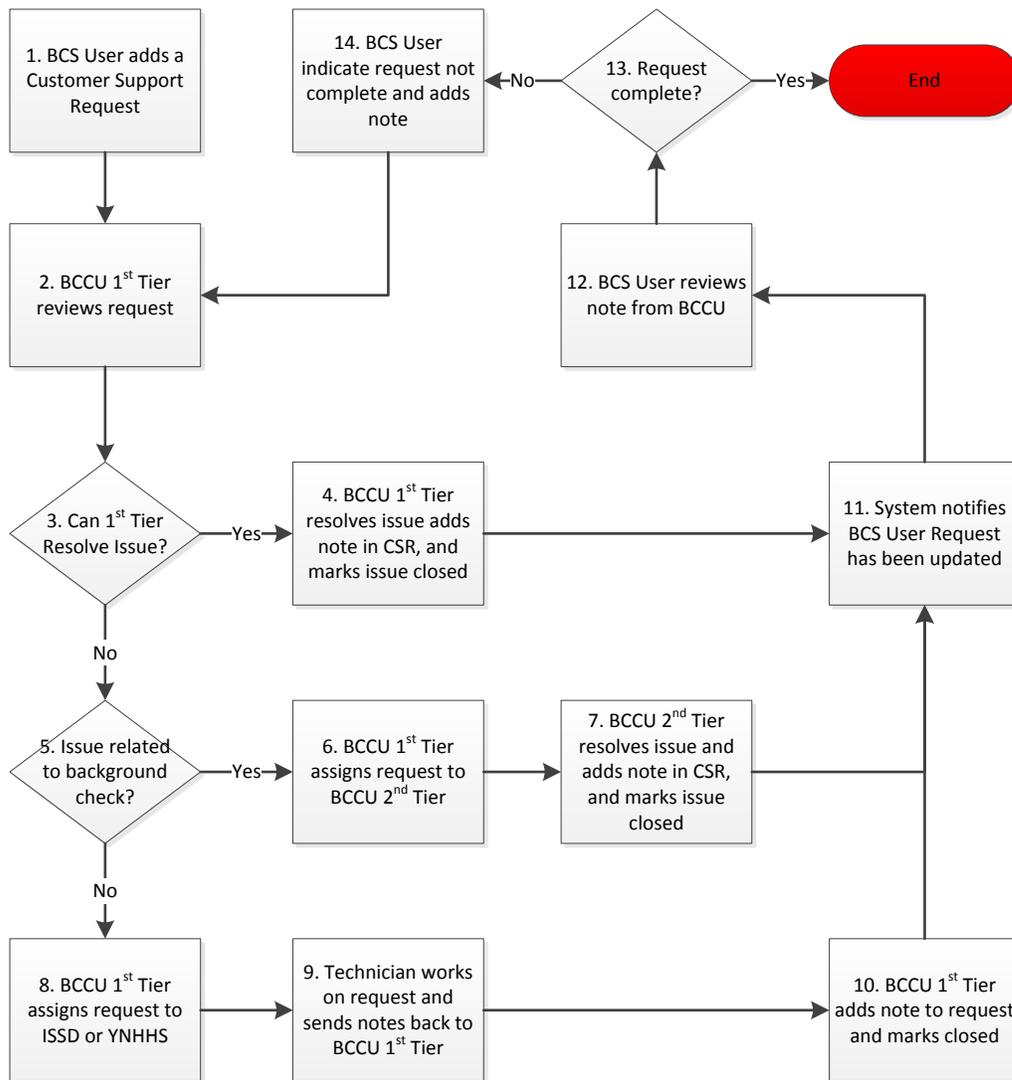
This section describes the requirements, business rules and process for submitting and responding to customer support requests.

Requirements Table 6.20 – Customer Support		
Requirement Type (F/NF)	Requirement Number	Function/Feature - Requirement
F	20.1	Enable users to initiate support requests within the system.
F	20.2	Allow users to categorize the type of support request from a predefined drop down list or add a custom support category.
F	20.3	Provide a method to manage support requests, with the ability to assign support requests to BCCU users and notify assigned users when support requests arrive in the work queue.
F	20.4	Have the ability to respond to a support request via e-mail or system notification.
F	20.5	Have the ability to reassign a support request to another user for resolution.
F	20.6	Associate support requests with a person of interest, OCA, or entity depending on the type of request.
F	20.7	Retain a history of support requests.
F	20.8	Provide a method for BCCU staff to log a support request received outside of the system (via phone or e-mail.)
F	20.9	Flag unresolved support requests after given # of days and notify assigned users that the request is pending.
F	20.10	Provide a method for users to log notes, resolution action, and close a support request.
F	20.11	Have the ability to track and report the volume and status of support requests by category and user and the turnaround time from receipt of request to resolution.
F	20.12	Have the ability to search for support request by multiple criteria.

Business Rules Table 6.20 – Customer Support	
BR#	Rule Description
20000	The system will pre-populate the Customer Support Form with User Information (name, email and phone fields) from the user's Profile Settings.
20001	User may select to assign the Customer Support Request to any entity the user has access to or to "All Entities".
20002	Customer Support Requests may be associated with a person of interest, OCA, or entity.
20003	When a user submits a Customer Support Request, the system sends a system notification and/or email to the user (The notification contains all the fields on the Customer Support Page except the email and phone.)
20004	Any system user may submit a Customer Support Request.
20005	BCCU Users may add a Customer Support Request and associate with a user, applicant, or entity based on a phone call or email to BCCUInquiry.
20006	Users must select the category of the request from the following list:

Business Rules Table 6.20 – Customer Support	
	<ul style="list-style-type: none"> • Technical assistance with the Background Check System • Fingerprint Vendor Question • Background Check requirements, status, rules • Check the status of a request • Dispute or correct a background result • Other
20007	<p>BCCU users review Customer Support Requests and assign to the appropriate queue. Queues include:</p> <ul style="list-style-type: none"> • Customer Support • Technical Team • Vendor/Customer Relations • ISSD Technical Support • YNHHS Technical Support
20008	BCCU users may add notes and assign the Customer Support Request (CSR) back to the user for more information without having to open a new CSR.
20009	When a Customer Support Request is assigned back to the user, the system notifies the user by email or and/or BCS notification. The notification includes the details and notes from the request.
20010	If a BCCU User closes a Customer Support Request, the user who submitted the request may select to have the request re-opened and add new notes.
20011	The user who submitted the Customer Support Request may only see notes that are marked by the BCCU user as visible to the requestor (this can be done through separate fields or indicators).
20012	The system records the user and date/time each time the Customer Support Request is updated.
20013	The BCCU User who reviews all Customer Support Requests may assign the request to any BCCU user or queue (there is no hierarchy).
20014	Only BCCU may assign a Customer Support Request back to the requestor. (ISSD may not assign to the requestor).
20015	BCCU Users are assigned to individual Customer Support work queues.
20016	The system notifies all members of the queue by system notification and/or email when a new request is assigned to the queue.
20017	Any user may query support requests that they submitted regardless of status.
20018	BCCU Users may query any support request that was entered by any user regardless of status.
20019	Support requests may be queried by any field that's associated with a Customer Support Request (e.g. category, status, OCA, POI, Entity, keyword in notes, etc.)
20020	The system provides reports that show the volume and status of support requests by category, user, length of time between when the request was submitted to 'today' or the date the request was closed.
20021	The system provides an at-a-glance view of BCCU users who are online and how many CSRs are in each queue.
20022	The system will display an indication on the POI, OCA, and Entity record if the record has an associated Customer Support Record.
20023	The system sends Customer Support notifications through email and system notifications.
20024	The User may opt to enable or disable email and system notification for CSR notifications.

Future State – Customer Support



Updated 06/10/2015

6.21 Reconcile Accounts

This section describes the requirements, business rules and process for reconciling billing accounts charged to BCCU. Billing accounts include the WSP WATCH, WSP Fingerprint, MorphoTrust and accounts for individual WIN states.

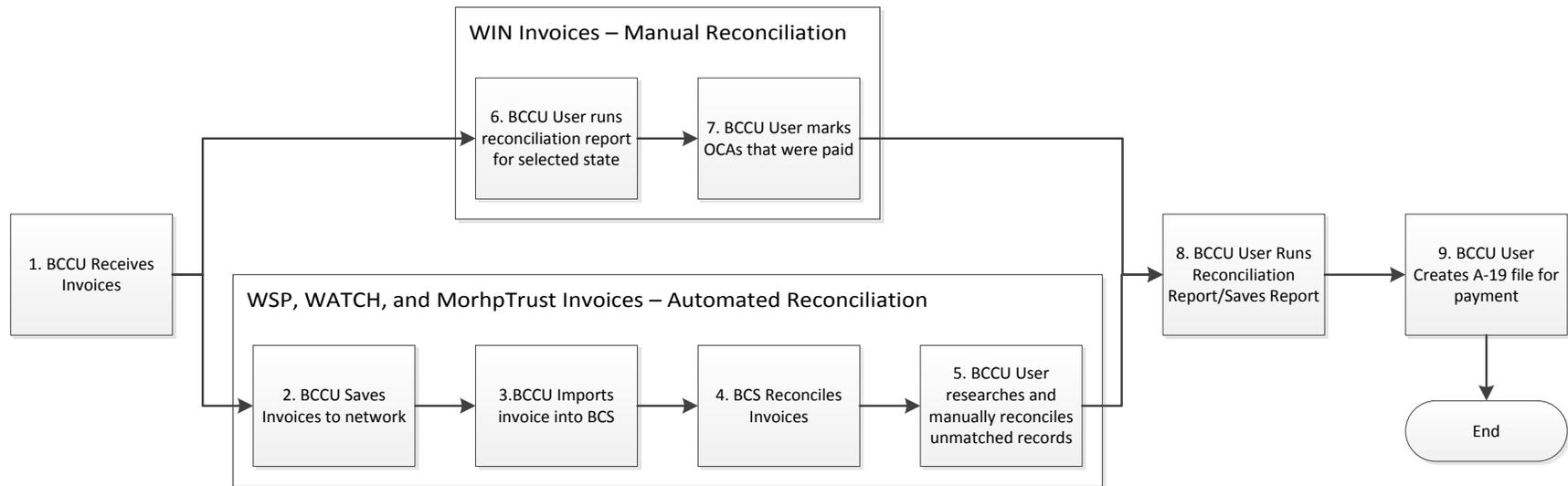
Requirements Table 6.21 – Reconcile Accounts		
Requirement Type (F/NF)	Requirement Number	Function/Feature - Requirement
F	21.1	The system must provide the ability to run an automated billing reconciliation process that compares data contained in the background system against data contained in invoices from various billing sources.
F	21.2	The system must have the capability of reconciling a WSP WATCH invoice with data contained in the background check system.
F	21.3	The system must have the capability of reconciling WSP fingerprint billing with data contained in the background check system.
F	21.4	The system must have the capability of reconciling a fingerprint vendor invoice with data contained in the background check system.
F	21.5	The system must have the capability of tracking and reconciling WIN billings with data contained in the background check system.
F	21.6	The system must have the capability of tracking multiple fingerprint billing sources for each fingerprint OCA and recording when the source is paid.
F	21.7	The system must keep a record of each billing reconciliation.
F	21.8	The system must provide the ability for BCCU users to manually reconcile OCA records for items that cannot be automatically reconciled.

Business Rules Table 6.21 – Reconcile Accounts	
BR#	Rule Description
21000	The system reconciles invoices for: WSP WATCH WSP Fingerprint Checks WIN Billings - Oregon, Utah, Montana MorphoTrust (Fingerprints)
21001	Invoices are received for different billing periods. Currently most invoices are received monthly. Oregon WIN invoices are received quarterly.
21002	Invoices are received in different formats. -Oregon is received on paper via USPS. -Montana is retrieved as PDF file by the BCCU user from the Montana website. -Utah is PDF file received by email. -WSP EP and Reg Fingerprints in spreadsheets by email. -WSP WATCH in CSV by email.

Business Rules Table 6.21 – Reconcile Accounts	
	-MorphoTrust in spreadsheet by email.
21003	WSP invoices for EP fingerprint and Reg Fingerprint are received in the same email.
21004	WATCH data comes in separate email from the invoices and EP/Reg data.
21005	MorphoTrust data spreadsheet is password protected. The password changes each month.
21006	Most billing includes the details of each search (applicant identification) with the exception of Utah.
21007	The Utah invoice includes a count of the number of searches completed by day.
21008	File layouts for each invoice that is automatically processed are included in the Invoice Layouts and Reconciliation Process document. Samples of each file layout are included as spreadsheets in the Invoice Samples folder.
21009	Rules for automatically matching invoice records to BCS are included in the Invoice Layouts and Reconciliation Process document.
21010	BCCU users may submit an OCA to WATCH more than once. WATCH dataset includes one record for each time the OCA was submitted and charges for each submission.
21011	MorphoTrust may only charge once per OCA unless the subsequent charge is more than 12 months after the first.
21012	WSP may only charge once per OCA unless the subsequent charge is more than 12 months after the first.
21013	The system tracks multiple billing sources for each OCA.
21014	For each OCA, the system tracks the billing source and if the billing source is paid.
21015	The system reconciles billing records if the activity occurred within the billing period.
21016	BCCU users may complete a match manually and indicate if a charge should be paid or not.
21017	When the BCCU user manually reconciles a billing source, the system tracks the username and date/time (for both approving and declining payment).
21018	Only three WIN states charge for their services. The system will track activities for a WIN data source that is not a billing source.
21019	The system provides an interface for BCCU user to reconcile all WIN searches to indicate that the billing source has been paid.
21020	The system provides a way for a user to search for past billing reconciliation by billing month, TCN, OCA, Reference ID, and POI First and Last Name.
21021	The system provides a Reconciliation Report by billing period for each billing source that includes counts by Program/inquiry type.
21022	BCCU staff will use information in the Reconciliation Report to manually populate the A-19 form.

Supporting Documents Table 6.21 – Reconcile Accounts	
The following supporting documents will be provided to the successful vendor at time of requirements verification:	
Name	Location
Invoice Layouts and Reconciliation Process	Appendix T

Future State – Reconcile Accounts



Updated 06/10/2015

6.22 Reporting Requirements

This section describes the reporting requirements for the Background Check System.

Requirements Table 6.22 Reporting Requirements		
Requirement Type (F/NF)	Requirement Number	Function/Feature - Requirement
F	22.1	The system must provide pre-built ("canned") reports that allow users to select appropriate parameters to broaden or narrow the report (date range, administration, division, inquiry type, background check type, BCCU account, applicant type, etc.)
F	22.2	The system must be capable of including mathematical (e.g., sum, difference, percentage) and statistical (e.g., average, median, standard deviation) information as part of a report.
F	22.3	The system must be capable of including charts and graphs as part of a report.
F	22.4	The system must allow tabular reports to be exported to Microsoft Office Excel.
F	22.5	The system must allow reports to be saved as PDF files.
F	22.6	The system must allow DSHS to add or modify ad hoc reports.
F	22.7	Ability to provide a variety of operational reports like: <ul style="list-style-type: none"> • background check volumes • background check results and engagement decisions • number and percentage of background checks require special handling • processing times
F	22.8	View/print the work list of applications assigned to a BCCU user.
F	22.9	View all background checks in a particular status/step in the process.
F	22.10	The system must have the capability to display an online summary of in-progress background checks. The background checks may be displayed sorted by elapsed processing days in ascending or descending order.
F	22.11	The system must be capable of reporting individual entity account summaries and overall system activity.
F	22.12	The system must be capable of producing productivity reports of investigators.
F	22.13	The system must be capable of producing productivity reports of entities.
F	22.14	The system must report the number and percentage of total background checks by staff members for a specified period of time.
F	22.15	The system must be capable of calculating turnaround time for background checks based on specified milestones.

Supporting Documents Table 6.22 Reporting Requirements	
The following supporting documents will be provided to the successful vendor at time of requirements verification:	
Name	Location
BCS Reporting Needs	Appendix U

6.23 Non-Functional Requirements

Requirements Table 6.23 Non-Functional Requirements		
Requirement Type (F/NF)	Requirement Number	Function/Feature - Requirement
NF	23.1	The system must provide workflow efficiencies that enable the BCCU user to process a Name/DOB check in less than 1.5 minutes on average.
NF	23.2	The system must provide sort-by-column functionality for all data grids.
NF	23.3	The system must provide the capability to log out from anywhere within the system.
NF	23.4	The system must provide drop down boxes, hierarchical "pick lists", calendars, or similar controls for data selection.
NF	23.5	The system will have spell-check capability for all free text fields.
NF	23.6	The system will provide navigational links to related screens.
NF	23.7	The system will provide a unique visual indication (e.g., grayed out) of read-only fields.
NF	23.8	The system will provide a visual indication of required fields.
NF	23.9	The system will provide a visual indication of when the system is processing.
NF	23.10	The system will provide a consistent appearance and formatting (look and feel) throughout the application in compliance with State IT and DSHS common look and feel standards.
NF	23.11	The system must be accessed through a web browser.
NF	23.12	The web site must be capable of providing the following information to users. An overview of the background check process Frequently Asked Questions relating to the background check process Privacy policy User manual Tutorial
NF	23.13	The web site must provide a secure login capability for authorized users to gain access to the Background Check System.
NF	23.14	The system must require specified users to read and agree to the Background Check System user agreement upon initial logon and each time the agreement is revised.
NF	23.15	The system must provide page views with links, menus, and functionality appropriate to each different account type.
NF	23.16	The system must provide a searchable help function to provide users help in using the system for both BCCU and external users.
NF	23.17	Browsers technical requirement 32.6 (RFQQ 2.6) covers which browsers; applicant will also be able to register in iOS and Android mobile devices but not necessarily be able to do other business.
NF	23.18	The system must provide the ability to assign user functions according to the account inquiry type.
NF	23.19	The system must provide search capability for applicants, entities, background checks, and other data components.
NF	23.20	The system must automatically populate fields that can be retrieved based on user search results.

NF	23.21	The system must be able to search by multiple criteria at once.
NF	23.22	Text searches must not be case-sensitive.
NF	23.23	Search fields must allow search on full or partial entries.
NF	23.24	The system must be capable of sending email using the State's SMTP email capabilities.
NF	23.25	The system must have the ability to provide event-driven automated notifications by email.
NF	23.26	The system must provide pre-defined ("canned") notes for standard and frequently entered comments.
NF	23.27	The system will have the ability to perform data validation and prevent the entry of invalid data by users.
NF	23.28	The system must validate that all required fields are entered prior to the submission of the electronic application.
NF	23.29	The system must post data in real time.
NF	23.30	The system will have a unique title for each screen.
NF	23.31	The system will contain robust error handling and will provide clear and meaningful error notifications - not system codes - to users.
NF	23.32	The system will have the ability to export data to standard file formats, including PDF and MS Excel.
NF	23.33	The system will include an audit trail that records and maintains transactions for certain tables identified by DSHS.
NF	23.34	The system will have an audit trail that records the user ID and IP addresses.
NF	23.35	The system must maintain a record of any change to a Criminal History Check application as specified by the defined audit tables.
NF	23.36	The system must be capable of recording at least 300,000 background checks per year.
NF	23.37	The system must have the capacity to manage initial record counts of _____ (current number will be provided to successful vendor at requirements review).
NF	23.38	The system must have a software architecture that, given sufficient hardware and modern DBMS (such as SQL Server 2012), supports large initial volumes of data records and document/image files, as well as a 10 percent annual growth rate, without degradation of performance. See Req. 23.37
NF	23.39	If the current database is not used, the background check system must have a subset of data converted from the legacy system, including persons of interest (applicants), applicant self-disclosures, rap sheets, and documents associated with applicants and inquiries.
NF	23.40	Legacy data must be searchable and available for use in processing future background check requests, including the ability to transmit legacy documents as part of a new background check result.

Supporting Documents Table 6.23 Non-Functional Requirements	
The following supporting documents will be provided to the successful vendor at time of requirements verification:	
Name	Location
Legacy Data Document	Appendix M

6.24 Technical Requirements

Requirements Table 6.24 Technical Requirements		
Requirement Type (F/NF)	Requirement Number	Function/Feature - Requirement
T	24.1	The system must have an adaptable structure for future enhancements and modifications to the system.
T	24.2	Open systems standards for interfaces (e.g., OASIS standards for web services), to support links with systems of external partners (e.g., other state agencies)
T	24.3	System web pages must meet current United States Access Board Section 508 standards and W3C Web Content Accessibility Guidelines to ensure accessibility for users with disabilities.
T	24.4	Ensure minimal data redundancy.
T	24.5	Each data element should have a single system of record.
T	24.6	The system will be a web application developed using Microsoft .Net technologies 4.5 or higher and hosted in Microsoft IIS 7.0 or higher.
T	24.7	The system will have an IIS Server that will be protected by a firewall.
T	24.8	The system will use Microsoft Windows Server 2012 SP2 or higher and SQL Server 2012 SP2 or higher if hosted by the State. If vendor-hosted, requirements will be determined at requirements verification.
T	24.9	The system will be constructed to take into account the need for appropriate disaster recovery, replication and maintenance processes.
T	24.10	The system must be compatible with modern browsers, such as Internet Explorer, Safari, Firefox, and Chrome. DSHS IT Standard for internal users is Microsoft Internet Explorer 8, but external users will be expected to use any modern browser.
T	24.11	The system must be capable of operating in a virtual server environment.
T	24.12	Users will access the system using a desktop configuration of Windows 7 or Windows XP.
T	24.13	The system database platform must be Microsoft SQL Server 2012 Standard or Enterprise Edition.
T	24.14	The system will have database replication for off-line reporting.
T	24.15	The system must provide concurrent access to data tables.
T	24.16	The database design must be documented in a Visio data model provided to BCCU. Sufficient documentation must be provided to support ad hoc reporting.
T	24.17	The system must comply with DSHS's IT Technical Standards for Network, Operating Systems, Workstation Software, and Service Oriented Architecture.
T	24.18	Ability to reliably send and receive data to/from remote systems.
T	24.19	Ability to send and receive data in multiple file formats (Excel, XML, text, other).
T	24.20	Ability to interact with DSHS's Enterprise Service Bus (ESB), which is built on IBM's WebSphere services, and includes standard interfaces for messaging, data drop (FTP) and XML. The system should support any of these three ESB-supported technologies for the specific system interfaces listed below.
T	24.21	Compatibility with OASIS standards for web services. (https://www.oasis-open.org/)
T	24.22	Ability to import and store scanned documents.

T	24.23	Compatibility with the network architecture and environment currently in place at DSHS
T	24.24	Ability to navigate various firewall and other security layers within DSHS's network architecture
T	24.25	The system must be password protected and in compliance with federal security standards, state security and privacy regulations, and State IT Standards.
T	24.26	The system must adhere to the State's Security Standards as outlined in the State's Information Security Policy. Support all relevant provisions in the DSHS IT Security Manuals.
T	24.27	If hosted by the State, external users will comply with the user name and password standards defined by Secure Access Washington.
T	24.28	If hosted by the State, internal users will use the DSHS active directory user name and password.
T	24.29	The system will provide security based upon roles, groups, and polices within multi-level organizational hierarchies.
T	24.30	The system must provide for role-based security, so that users' access to functions and data can be limited by their roles and levels of authority.
T	24.31	The system must support a high level of data confidentiality, including protecting personal and confidential information (SSN)
T	24.32	Allow each user to perform multiple functions within the system by signing on once, minimizing the need to revalidate credentials when moving to other functions.
T	24.33	If the system is hosted by the State, the must authenticate internal users using Microsoft Active Directory and external users by using Secure Access Washington (SAW). SAW is a standard required for new web applications hosted by the State and requires an interface implementation.
T	24.34	The system must handle at least 500 concurrent connections without performance degradation.
T	24.35	The system must provide a response time of 3 seconds or less for 99% of transactions.
T	24.36	The system must be available 24 hours a day, 7 days a week. Brief maintenance periods may be scheduled outside standard working hours of 8 am - 5 pm Pacific Time, Monday - Friday.
T	24.37	The system will incorporate the ability to control the access rights of users.
T	24.38	Vendor technical support (call in and online help desk service) with first level response must be available at minimum from 8 am to 5 pm Pacific Time for all business days.
T	24.39	For application or technical issues under the control of the vendor that make the system unavailable to staff, vendor maintenance support will include a guaranteed 4 hour response time.
T	24.40	All documentation must be modifiable by DSHS.

6.25 Security Requirements

This section describes the security requirements for the Background Check System.

Requirements Table 6.25 Security Requirements		
Requirement Type (F/NF)	Requirement Number	Function/Feature - Requirement
General Security Requirements		
S	25.1	The system must comply with the requirements outlined in the current FBI CJIS Security Policy.
S	25.2	The application must undergo a DSHS Information Security Design Review and a WA CTS Information Security Design Review before production implementation.
S	25.3	The successful vendor must be approved as described in the FBI Security and Management Control Outsourcing Standard for Non-channelers prior to having access to access to federal criminal history records. Once approved, the successful vendor and must ensure ongoing compliance with the requirements of the above referenced outsourcing standard.
Encryption Requirements		
S	25.4	All criminal history data must be encrypted in accordance with the DSHS Cryptography Standard. Standard will be provided during requirements verification.
S	25.5	A minimum of Transport Layer Security (TLS) 1.2 must be implemented for data in transit.
S	25.6	SSL certificates must not be self-signed.
User Accounts		
S	25.7	All user IDs must be unique. Shared accounts are not allowed.
S	25.8	User identity must be verified before performing an account reset.
Password Requirements		
S	25.9	Passwords must be a minimum length of eight (8) characters and contain at least three of the following character classes: uppercase letters, lowercase letters, numerals, special characters.
S	25.10	Passwords cannot contain dictionary words or names.
S	25.11	Passwords cannot include the User ID as part of the password.
S	25.12	Passwords must expire within a minimum of 90 days.
S	25.13	Passwords cannot be identical to the previous ten (10) passwords.
S	25.14	Passwords cannot be transmitted in the clear.
S	25.15	Passwords cannot be displayed when entered.
S	25.16	First-time passwords must be set to unique values and must be changed immediately at login.
Account Lockout and Session Lock		
S	25.17	Accounts must lock after five (5) unsuccessful logon attempts.
S	25.18	Session lock must occur after thirty (30) minutes of inactivity.

S	25.19	<p>The following system events must be logged:</p> <ul style="list-style-type: none"> ○ Successful and unsuccessful system log-on attempts. ○ Successful and unsuccessful attempts to use: <ul style="list-style-type: none"> ▪ Access permission on a user account, file, directory or other system resource; ▪ Create permission on a user account, file, directory or other system resource; ▪ Write permission on a user account, file, directory or other system resource; ▪ Delete permission on a user account, file, directory or other system resource; ▪ Change permission on a user account, file, directory or other system resource. ○ Successful and unsuccessful attempts to change account passwords. ○ Successful and unsuccessful actions by privileged accounts. ○ Successful and unsuccessful attempts for users to: <ul style="list-style-type: none"> ▪ Access the audit log file; ▪ Modify the audit log file; ▪ Destroy the audit log file.
S	25.20	<p>The following event characteristics must also be logged:</p> <ul style="list-style-type: none"> ○ Date and time of the event. ○ The component of the information system (e.g., software component, hardware component) where the event occurred. ○ Type of event. ○ User/subject identity. ○ Outcome (success or failure) of the event.
S	25.21	<p>Audit logs must be protected against tampering and unauthorized access.</p>
S	25.22	<p>Audit logs must be retained for a minimum of one (1) year.</p>
Application Development		
S	25.23	<ul style="list-style-type: none"> ● Development, test, and production environments must be separated. ● Separation of duties between development, test, and production environments must exist. ● Production data used for development testing must not compromise privacy or confidentiality. ● Test data and accounts must be removed from the production environment. ● Code must be tested and scanned for vulnerabilities before production release. Examples: Un-validated input; weak or broken access control such as malicious use of UserIDs; broken authentication/session management such as use of credentials and cookies; cross-site scripting (XSS) attacks; buffer overflows; injection flaws such as SQL injection; improper error handling that creates other conditions, divulges system architecture or configuration information; insecure storage; denial of service; insecure configuration management. ● A formal change management and change control system must be in place.

6.26 Specific Interface Requirements

This section describes the interface requirements for the Background Check System.

Requirements Table 6.26 Specific Interface Requirements		
Requirement Type (F/NF)	Requirement Number	Function/Feature - Requirement
I	26.1	<u>Fingerprint Result E-mail Imaging Process</u> Provide a web service interface that provides equivalent functionality to the current system to process fingerprint results from WSP and FBI e-mail inbox. See Section 6.11 – Fingerprint Handling.
I	26.2	<u>BCCU Inquiry Web Services – ESA</u> Provide a web service interface with the ESA Bar Code system to send background check requests and transmit background check results for Name/DOB background checks that provides equivalent functionality to the current Criminal History System.
I	26.3	<u>BCCU Inquiry Web Services – DEL</u> Provide a web service interface with the Department of Early Learning licensing system to send background check requests and transmit background check results for Name/DOB and fingerprint-based background checks that provides equivalent functionality to the current Criminal History System.
I	26.4	<u>MorhoTrust real-time validation Web Service</u> Create a live web service to validate applicant information with contracted fingerprint vendor.
I	26.5	<u>Department of Health Facility Load Web Service</u> Provide a web service to receive location information from the Department of Health and create/update private home care entity accounts in the background check system database. The service is called every night by DOH with the location data. At the end of the update, a status is returned to DOH. Uses asmx technology. Must provide equivalent functionality to the current Criminal History System.
I	26.6	<u>ADS Facility Load – Linked SQL Server</u> Provide a linked SQL server job to retrieve entity account updates from ADS. The job runs nightly. Must provide equivalent functionality to the current Criminal History System.
I	26.7	<u>DOH Inquiry Status Check – Web Service</u> Provide a web service with DOH that provides equivalent functionality to the current Criminal History System. DOH provides a nightly feed of the Inquiry Ids they are currently tracking in their system awaiting licensing approval. The web service responds with the current status of the inquiry or an error message if the Inquiry Id is for a non-Private Home Care organization or is not found in the CHS system.
I	26.8	<u>WSP WATCH – Web Service</u> Integrate the web service provided by the Washington State Patrol for running Name-DOB checks.
I	26.9	<u>AOC Linked SQL Server</u> Integrate the linked SQL server job used in the current Criminal History System to search Administrative Office of the Courts data mart criminal history records.

I	26.10	<u>FAMLink – CA Findings Data</u> Integrate the nightly interface through the Enterprise Service Bus (ESB) that delivers data from Children’s administration Child Protective Services (CPS) database.
I	26.11	<u>FAMLink – ADS Findings Data</u> Integrate the nightly interface through the Enterprise Service Bus (ESB) that delivers data from Aging and Disability Services Adult Protective Services (APS) and Residential Client Protection Program (RCPP) findings databases.
I	26.12	<u>DOH Licensing Actions</u> Integrate the TumbleWeed Secure transport – secured FTP Weekly process that retrieves files and updates search tables containing data for DOH findings.
I	26.13	<u>Office of Inspector General Registry</u> Create a new web service interface with the federal Office of Inspector General to search applicants and identify matching records.

Supporting Documents Table 6.26 Specific Interface Requirements	
The following supporting documents will be provided to the successful vendor at time of requirements verification:	
Name	Location
Data Sources and Automated No Records	Appendix G
MorphoTrust Technical Summary	Appendix Q
Account Number and Nightly Update Rules	Appendix S
DOH Web Service Specification	Appendix X
DEL Web Service Specification	Appendix Y
ESA Web Service Specification	Appendix Z