Appendix 3: Subscribing Entity Reference Guide to NGI's Rap Back Service
Version 2.1 – June 1, 2014

Note to Submitters: *The information in this document is provided for you to use in any manner most appropriate to your implementation. The information could be used as a separate document, integrated into your own documentation, or in any other manner. Where the document asks questions regarding the Submitter's plans or where it states that the Submitter must describe certain Submitter choices to the Subscriber, it is recommended you remove that language and instead provide those functions, choices, or descriptions directly.*

This document is provided as a reference for those non-criminal justice entities who are considering participation in NGI's Rap Back Service. To address the entire population of potential Subscribers, these requirements are listed only as related to NGI and the NGI Rap Back Service. Of course, Submitters with their own Rap Back Programs will implement these requirements as appropriate within the context of their existing activities and, as above, should use this information in any means appropriate for communicating with their Subscribers.

This document is an attempt to summarize key points for the Subscribers.

As stated throughout the Non-Criminal Justice Rap Back Service Policy and Implementation Guide, the robustness of the in-state or federal agency or Authorized CHRI Contractor communications methodology is critical to the success of Rap Back. The Submitter must employ the most efficient communications process possible and must work with the Subscribers to use if effectively.

Following are the steps necessary for a non-criminal justice entity to participate in NGI's Rap Back Service. These steps must be taken in coordination with the Submitter through whom the subscriptions will be sent to NGI.

1. Subscriber must identify the authority they have to participate in Rap Back.

Subscriber must have an appropriate ORI assigned by the CJIS Division. Their statutory or other appropriate authority must be provided to the Submitter, and must include:

a. Authority to submit non-criminal justice fingerprints for search and responses to the Submitter and NGI.
b. Authority for NGI to retain those fingerprints and process future searches against them, including latent fingerprint searches.

Subscribers can only subscribe to persons who have official relationships to the Subscriber under the identified authority.

2. In States or Federal Agencies where Rap Back Systems already exist, the Subscriber must understand how NGI's Rap Back Service will change the information provided to the Subscriber from the Submitter.

Submitters who already operate Rap Back services for their Subscribers must describe to the Subscribers what effect participation in NGI's Rap Back will have upon the future notifications of Rap Back activity and other messages that will be communicated between Submitter and Subscriber.

The Submitting Entity may want to describe the Subscription Management Plan that they have chosen for managing the subscriptions submitted through them. There is no direct requirement on the Subscriber regarding the plan, but it may be helpful for them to understand how the Submitter is handling the subscriptions, which could affect how the new information will be presented to the Subscribers.

The Submitter should describe whether the NGI transactions and functions will look different from the in-state or federal agency transactions, or if they will just be integrated into the Submitter's transactions and messages. For example, if the Submitter is going to simply forward the NGI transactions as they come from NGI, they will have a different look than the in-state or federal agency transactions. This is a training issue for the Submitter to include in its discussion and documents with the Subscribers.

Also key to this point is simply making sure that the Subscribers understand the scope of the NGI Rap Back Service and that they will now be getting notified of out-of-state events that are reported to the FBI.

3. The Subscriber must agree with Submitter on the appropriate Privacy Risk Mitigation Strategy for their subscriptions.

The Subscriber must implement formalized processes, procedures, and controls in alignment with the Rap Back policies to protect the information and the Rap Back Service.

Accordingly, the Subscriber in consultation with the Submitter must choose the appropriate Privacy Strategy to apply to their subscriptions. It is recommended the discussions of the Privacy Risk Mitigation Strategies include:

- The Rap Back Privacy Risk Mitigation Tools and the approved Rap Back Privacy Risk Mitigation Strategies as described in the Rap Back Service Non-Criminal Justice Policy and Implementation Guide, Appendix 1: Approved NGI Rap Back Privacy Risk Mitigation Strategies. The key issues include validation/expiration and Rap Back Activity Notification Format. It is important that the Subscriber understand how those processes work and is able to decide which are most appropriate for the populations they serve.
- A detailed description of the Submitter's Privacy Risk Mitigation Strategy implementation processes, so that the Subscriber can determine how their processes fit in, and where they may need to change and augment their processes.
- Based upon the selected Privacy Strategy, the Submitter and Subscriber must agree on the appropriate Rap Back Activity Notification Format: will the Subscriber receive Pre-Notification, the Triggering Event and Identity History Summary, or just the Triggering Event within their Rap Back Activity Notifications.
    i. If they are going to receive pre-notification messages, it is recommended the Submitter and Subscriber consider the following questions:

1. How will the Submitter send the Rap Back Activity Notifications with pre-notification to the Subscriber?
2. How will the Subscriber be able to respond to them in a timely manner?
3. How will the Subscriber route Rap Back Activity Notifications to the right person within their organization?
4. How will they communicate the response back to the Submitter?
5. Does the Subscriber know they will get a reminder if they do not reply within 15 days?

- The correct use and execution of validation/expiration processes is critical to the Privacy Risk Mitigation Strategies. The policies and processes related to validation/expiration and the Rap Back Subscription Term are discussed in Item #6, below. Subscribers must understand the relationship between the Subscription Term and the Subscription Validation/Expiration period discussed in Item #6.

4. The Subscriber must send and receive Rap Back transactions to and from the Submitter using the Submitter's specific communications methodology.

The Submitter must identify and document both the communications methodology and the actual transactions that the Subscriber must send the Submitter to fulfill the Rap Back functions. Descriptions must also include the responses those transactions will generate from the Submitter back to the Subscriber. That communications methodology may be electronic, manual, or a combination.

It is recommended the information include:

- A plain language description of the communications methodology (secure email, secure website, overnight delivery service, by phone, etc.). Include whether certain transactions have different methodologies; for example, are pre-notifications performed via phone and the rest in the mail.
- Whether the Submitter has created any defined forms or messages that the Subscriber's internal processing must use to communicate the different transactions to the Submitter. If the Submitter is requiring the Subscriber to supply an electronic message that is in an excel spreadsheet or in the actual EBTS format, for example, the Submitter should provide clear guidance on the field definitions, formats, mandatory status, etc.
- All the NGI Rap Back functions, including any controls required at any point by the Submitter.
- The details of what must be included in each message, how they are to be sent, and how they are related to the Subscriber's internal processing.
- Discussion of controls within the communications methodology to ensure that the messages are sent, received, and processed in a timely manner from the Subscriber and by the Submitter. For example, does the Submitter have time frame requirements for sending update transactions, or are there certain acknowledgement responses that the Submitter sends or requires of the Subscriber to ensure transactions are received and processed.
- Whether all transactions will be passed through to the Subscriber. For example, does the Subscriber want to receive notice from NGI through the Submitter when each new subscription is successfully established, or rather just when the setting of a subscription fails?

5. The Subscriber and Submitter must ensure that the applicant receives appropriate Privacy Act Notifications.

The Submitting Entity and Subscriber must agree on how the applicants will be notified that his or her fingerprints will be retained in the national file and a summary of the intended uses. This is a combined responsibility of the Subscriber, the Submitter, and the FBI CJIS Division. Means by which this notification can happen include the fingerprinting process, including language on the fingerprint cards, through the livescan process, through the Subscriber's individual application process, or other verifiable means.

The Submitter and Subscriber must agree on a process that reliably ensures all applicants receive this notice. The FBI CJIS Division will provide the appropriate notification language.

6. Subscribers must understand the relationship between the Subscription Term and the Subscription Validation/Expiration period.

The Subscriber must understand the logic regarding the Subscription Term and the Subscription Expiration Date. Each NGI Rap Back subscription has two key dates: The Rap Back Term Date and the Subscription Expiration Date:

- The Rap Back Term Date reflects how long a subscription period has been purchased by the Subscriber through the payment of the fee.
- The Expiration Date is the date at which the subscription expires to fulfill the validation requirement, even if time still remains on the Subscription Term. If time does remain on the Subscription Term, the subscription may be "extended" with no additional fee.

The Subscriber must pay a fee for each NGI Subscription. The amount of the fee determines the length of time during which the subscription can be repeatedly "extended" without incurring an additional fee. The available Subscription Terms are as follows:

- 2-Year
- 5-Year
- Lifetime

Although the Subscriber pays a fee for a 5-year Subscription Term, for example, that does not mean that the subscription automatically remains active for five years. Each NGI subscription must be governed by one of the Privacy Risk Mitigation Strategies, as discussed in Item #3, above.

Those Privacy Risk Mitigation Strategies require that NGI Rap Back subscriptions be reviewed and validated at certain intervals in order to remain in NGI. That validation process is implemented for NGI Rap Back through the use of the Expiration Date field. That is, even though, a Subscriber pays for a 5-year Subscription Term, for example, if they participate in Privacy Risk Mitigation Strategy #4: One Year Validation/Expiration, they must validate the subscription every year. This means that they must set the Expiration Date of their subscriptions to one year from the date of entry.

The logic is as follows:

a. The Subscriber has paid for the Subscription to remain in NGI for a certain Subscription Term (2- year; 5-year; or lifetime), so they will not be charged again during that Term.
b. However, the approved Rap Back Privacy Risk Mitigation Strategies require that the Subscriber periodically verify that they are still in an authorizing relationship with the

subscribed person—the subscription must be validated at intervals determined by the Privacy Risk Mitigation Strategy chosen by the Subscriber and Submitter.

c. At the mandatory Expiration Date required by the chosen Privacy Risk Mitigation Strategy, the Subscriber must review their subscription, validate that it can still be in NGI Rap Back and, if it is still valid, "extend" it for a new validation/expiration period that is within the Subscription Term. If they do not extend the subscription, it is automatically removed from file at the Expiration Date.
d. The Subscription is "extended" by use of the Rap Back Maintenance "Replace" transaction, through which the Subscriber replaces the Expiration Date field with a new date that is consistent with the selected Privacy Strategy, and which does not extend the subscription past the Rap Back Term Date.
e. No fee is charged for the Rap Back Maintenance "Replace" transaction that replaces the Expiration Date field with a new "extended" Expiration Date that is less than or equal to the Subscription Term.
f. If the new Expiration Date would extend the Subscription past the Rap Back Term Date, the Subscriber must either:
    i. Use a different Expiration Date that is less than the Rap Back Term Date;
    Or
    ii. "Renew" the Subscription for a new Subscription Term. The renewal is accomplished by using the Rap Back Maintenance "Renew" transaction to renew the Subscription Term; automatically create a new Rap Back Term Date; enter a new Expiration Date; and incur a new subscription fee.
g. The Rap Back Maintenance "Renew" transaction which renews the Subscription causes the billing process to charge the Subscriber a new Rap Back subscription fee for the same Subscription Term as originally purchased.

As such, the Subscriber must decide upon the appropriate Subscription Term for their population of applicants. That decision will determine the fees they will pay and the Terms of the Subscriptions, but it is separate from the decision regarding the Privacy Risk Mitigation Strategies and the resulting Expiration Dates.

The Subscriber also must identify the appropriate Expiration Dates for all their subscriptions. The Expiration Dates are determined from the Privacy Risk Mitigation Strategy being employed by the Subscriber and Submitter. The Privacy Strategies drive Expiration Dates as follows:

Strategy 1: Pre-Notification with Mandatory Validation/Expiration within Three Years

This Strategy requires the Expiration Date field to contain a date within the Subscription Term and no later than three years from the date the subscription is established.

Strategy 2: Authority for Duration of a License

This Strategy requires the Expiration Date field to contain the end date of the term of license, or, if the licensing entity prefers, a date somewhat prior to that date. The Expiration Date must contain a date within the Subscription Term and no later than five years from the date the subscription is established.

Strategy 3: Statutory Authority for a Set Period of Time

This Strategy is equivalent to Strategy 2, and similarly requires the Expiration Date field to contain a date within the Subscription Term; no later than the end of the Set Period of Time

authorized in the statute; and no later than five years from the date the subscription is established.

Strategy 4: One-Year Validation/Expiration

This Strategy requires the Expiration Date to contain a date no later than one year from the date the subscription is established.

Strategy 5: Subscription Synchronization Through Automated or Formalized Procedures

This Strategy requires that the Expiration Date field to contain a date within the Subscription Term and no later than five years from the date the subscription is established.

The Subscriber should identify if there are variations in their populations that may require special processing and how those will be handled. In addition, the Subscriber should consider processes they will use to ensure updates are provided to the Submitter when a person's subscription needs to be removed before its Expiration Date, such as because of termination of employment, licensing, etc.

7. The Subscriber must process monthly Subscription Validation/Expiration Lists that will be provided to them from the Submitters.

Closely related to the Subscription Term Date and Expiration Date is the processing of the Monthly Validation/Expiration Lists. The Subscribers must prepare processes to handle the receipt of the NGI lists from the Submitter each month and their subsequent processing and response to the Submitter.

The flow is as follows:

1. CJIS provides the Submitters a list of all the subscriptions that will expire in the month that occurs approximately 45-75 days in the future (in November they send the January expiring records).
2. The list is sorted by Subscriber ORI. The Submitter separates the list and sends each Subscriber their portion through secure electronic means (or whatever is the agreed upon secure communications methodology).
3. The Subscriber must review all the subscriptions and verify whether they still have the authorizing relationship with each person and can therefore "extend" or "renew" the subscriptions. Then:
    a) They create a bulk response to the validation/expiration list, indicating which subscriptions should be extended, which ones should be renewed, and which ones are no longer valid or will expire at the date indicated on the list.
    b) For those that can be extended, they must include the new Expiration Date.
    c) If the new Expiration Date would extend the subscription past the Rap Back Term Date, the Subscriber must renew the Subscription and pay the fee that results from that transaction.
    d) If the subscription is no longer valid at present, the Subscriber should include in their response to the validation/expiration list that it should be canceled immediately.
4. For all the responses on the list from the Subscriber, the Submitter sends the updates to NGI.
5. Ten days prior to the expiration of each of the January subscriptions that were not extended or renewed by the Subscriber and Submitter through the monthly validation/expiration list process, NGI will send an EBTS Rap Back Renewal Notification as an additional reminder. (The Submitter can opt-out of receiving those reminders.) For each one, if no response is received by

NGI by the date of expiration, the NGI System deletes the subscription. The civil event associated with the subscription remains in file.

6. After the end of January, NGI sends the Submitter a list of all the January Subscriptions that expired or were canceled. As previously agreed upon by the Submitters and Subscribers, the Submitter sends those lists of expired and canceled records to the Subscribers for them to check for any errors.

The Submitters and Subscribers must coordinate closely on the processing of these lists to avoid subscriptions being inappropriately removed from NGI and to prevent subscriptions from remaining in NGI when they should not.

Note: The Submitter may create an alternative but equal validation/expiration strategy for the Subscriber's subscriptions, in which case the Subscriber will have to participate in that process.

8. The Subscriber may identify the triggers to be used in their subscriptions.

All Criminal Retain Submissions will trigger a Rap Back Activity Notification to be sent to the Submitter from NGI. The Subscriber must identify any additional triggers from the below list that should also cause Activity Notifications to be sent from NGI, and whether those are set by default by the Submitter (if the Submitter offers that option) or the Subscriber will provide them on each subscription transaction.

a. Criminal Retain Submission
   This trigger will activate whenever a retained criminal Tenprint Fingerprint Identification Submission transaction or NFF Criminal Print Identification (CPI) transaction matches against a subscribed NGI Identity. This trigger is automatically set for all subscriptions, regardless of whether it is requested or not.
b. Dispositions
   This trigger will activate whenever a reported disposition transaction is matched against a subscribed NGI Identity. The disposition transactions included are:
   - Disposition Fingerprint Search Request
   - Disposition Submission Request
   - Disposition Maintenance Request
c. Civil Retain Submission
   This trigger will activate whenever a retained civil Tenprint Fingerprint Identification Submission matches against a subscribed NGI Identity, and it will provide notification of civil event information. This trigger is limited to certain federal agencies that have specific statutory authority to receive this information [e. g. for Office of Personnel Management (OPM), Security Clearance Information Act (SCIA)].
d. Expunge/Partial Expungement
   This trigger will activate whenever all or a portion of a subscribed NGI Identity is expunged and provide notification of the information being removed from the record.
e. Warrant entry with FBI number included
   This trigger will activate whenever a record containing an FBI/UCN that matches a subscribed NGI Identity is entered into the NCIC Wanted Person file or Immigration Violator file.

f. Warrant Deletion
   This trigger will activate whenever a record containing an FBI/UCN that matches a subscribed NGI Identity is deleted from the NCIC Wanted Persons file or Immigration Violator file. This trigger will be activated by NCIC Cancel, Clear, or Locate transactions.
g. Warrant Modification
   This trigger will activate whenever a record containing an FBI/UCN that matches a subscribed NGI Identity is modified within the NCIC Wanted Persons file or Immigration Violator file.
h. Sex Offender Registry entry
   This trigger will activate whenever a record containing an FBI/UCN that matches a subscribed NGI Identity is entered in the NCIC Sex Offender Registry.
i. Sex Offender Registry Deletion
   This trigger will activate whenever a record containing an FBI/UCN that matches a subscribed NGI Identity is deleted from the Sex Offender Registry. This trigger will be activated by Cancel or Clear transactions.
j. Sex Offender Registry Modification
   This trigger will activate whenever a record containing an FBI/UCN that matches a subscribed NGI Identity is modified within the Sex Offender Registry. Transactions that will cause this trigger to activate are limited to modification of any of the following fields:
   - Name
   - Case Number
   - Registration Date
   - Registry Expiration Date
   - Registering Agency
k. Death Notices
   This trigger will activate whenever NGI receives a death notice and associates it with a subscribed NGI Identity. This will include both fingerprint-based and non-fingerprint-based death notice submissions. The Rap Back Activity Notification will include whether it was a fingerprint supported death notice or not. NGI does not remove the Rap Back subscription as result of a fingerprint based or non-fingerprint based death notice.

9. The Subscriber must internally link and process Rap Back Activity Notifications and all other Rap Back transactions.

For the Subscriber to realize the full value of Rap Back they must be able to receive and process Rap Back Activity Notifications in the near term or long after the original subscription was established.

As such, the Subscriber must establish a specific protocol for receiving and processing future Rap Back Activity Notifications, monthly validation/expiration lists, and all other Rap Back transactions.

The Subscriber and Submitter must identify the linking fields and what the Subscriber will send to NGI in the linking fields. That information will be returned to the Subscriber in the future Rap Back Activity Notifications. The information must have meaning to them at that time, so they can route that notice to the right person internally to quickly take the appropriate action.

The process must be robust enough that it will have meaning to new management and operational personnel who receive the message at a future time. Include discussion of the linking fields and how

they will be used, especially the Rap Back Attention field and the User Defined fields. If the Submitter has created a standardized use of the User Defined fields, they must communicate that to the Subscriber. Otherwise, the Subscriber can use them in any way that will assist their processing. The ten User Defined fields are 100 characters each and may include, among other data:

a. Initial Fingerprint Submission TCN;
b. Subscribing Entity OCA submitted at time of subscription;
c. Internal Subscriber reference information;
d. State SID, when appropriate.

10. The Subscriber must understand their role in keeping the NGI Rap Back Service accurate and up to date.

The Subscriber's role in keeping the national Rap Back Service accurate and up to date requires that they follow all NGI policies and requirements, and that they agree to use the processes and functions created for Rap Back to notify the Submitter in a timely manner of all changes to their local records that would affect the authority or accuracy of the corresponding NGI subscriptions. They must communicate to the Submitter the correct information to set, modify, extend, renew, or delete their subscriptions in a timely manner.

11. Subscribers must understand that when they receive a name search response after re-submission of rejected fingerprints no Rap Back Subscription will be established for that person based upon that set of fingerprints and name search result.

Since no fingerprint identification was made to an NGI Identity and no NGI Identity was created by that set of fingerprints, no subscription will be established. If better prints are received in the future and the person is identified to an NGI Identity or an NGI Identity is created, a subscription may be established at that time.