Appendix 1: Approved Rap Back Privacy Risk Mitigation Strategies Version 2.1 - June 1, 2014

Submitters must work with each one of their Subscribers to identify the Privacy Risk Mitigation Strategies that will be used for establishing and maintaining the Subscribers' subscriptions. This document first lists the Privacy Risk Mitigation Tools that are used to create the Privacy Risk Mitigation Strategies and then describes the Strategies from which the Subscribers and Submitters must choose.

Privacy Risk Mitigation Tools

1. *Training and Auditing*

As with all CJIS systems, an underlying system discipline must provide an environment of control and respect for the requirements that the APB, Compact Council, and FBI have instituted. Training and Auditing are key to the users' understanding that system discipline and the requirements that they must follow. With Privacy as a principal tenet of NGI's Rap Back Service, training and auditing will emphasize to the Submitters and Subscribers that they play a crucial role in upholding privacy values and implementing privacy protections. Subscribers will be provided specific guidance on how to use the data they receive, restrict its use to the authorized purposes, and prevent breaches. FBI and state audits will verify training and compliance in a manner similar to existing audit programs.

2. *Pre-notification*

Pre-notification requires that when there is a subsequent event, NGI and the Submitters must verify that the Subscriber is still authorized to receive the CHRI or other Rap Back information before releasing it to the Subscribing Entity. The Subscriber must affirm that they still have the authorizing relationship with the person whose record they are about to receive.

3. Validation through Mandatory Expiration Dates

Validation requires that the subscribing entity periodically affirm to the Submitter and NGI that their list of subscriptions is still valid. For NGI's Rap Back Service this privacy risk mitigation tool will be implemented through the use of mandatory Expiration Dates within all subscriptions. To administer this process, each month NGI will provide Subscribers, through their Submitting Entities, a list of their records about to expire. The Subscribers will review the records and advise their Submitting Entities which ones are still valid and need to remain in NGI. The Submitters will have to send Rap Back Maintenance transactions to extend or renew those subscriptions. The other subscriptions will automatically be deleted upon their Expiration Dates. That is, rather than having to periodically review and affirm the validity of their subscriptions to have them remain in file, Subscribers will have to review and affirm the validity of their subscriptions just prior to the Expiration Date in order to avoid their removal from file.

FBI CJIS will work with states and Federal Submitting Agencies that currently have validation functions in an effort to determine if it is possible to interface those existing validation activities with

NGI as a means of fulfilling the validation requirement. For example, it may be possible for a state or Federal Submitting Agency to use the outcome of its validation processes to send Rap Back Maintenance transactions to NGI that extend or renew their subscriptions prior to the monthly validation/expiration lists being generated, thereby allowing their existing validation process to prevent their subscriptions from being included in those monthly validation/expiration lists.

5. *Use of Specific Language to Notify Applicants of Use of Fingerprints and CHRI*

An important aspect of privacy is that the applicant is aware of the present and potential future uses of his or her fingerprints, including that they will remain in NGI and cause notices of future criminal or other activity. The applicant's awareness of these uses of the fingerprints and records helps mitigate the NGI Rap Back Service privacy risks.

6. *Use of Formalized Subscription Management Procedures*

Formalized procedures within the Subscribing Entity and between the Subscribing Entity and Submitting Entity for setting, modifying, extending, renewing, deleting, and synchronizing subscriptions can be an effective means of ensuring the NGI Rap Back subscription is an accurate reflection of the person's status with the Subscribing Entity. For example, a formalized process that requires a check off that the Rap Back Subscription has been set when the applicant becomes licensed, is employed, begins volunteer work, etc. is one way to ensure the Rap Back subscription is established in a timely manner. Likewise, the Subscriber must have a process whereby when the person is no longer under their license, employ, or other authority, the person's subscription is removed.

For this tool to be used as part of Privacy Strategy #5, below, the procedures must be well documented and auditable. In addition, to employ Strategy #5 for one or more of its Subscribers, the Submitter must demonstrate appropriate controls—whether automated or manual—and the associated time frames. Examples could include how a synchronization process with a particular Subscriber is implemented, how frequently that occurs, how errors are handled, etc.

Approved Privacy Risk Mitigation Strategies

The above tools have been used in different combinations to create the approved Privacy Risk Mitigation Strategies for use by the Submitters (State SIBs, Federal Submitting Agencies, Authorized CHRI Contractors) and the related non-criminal justice Subscribing Entities. The intention is to create a variety of acceptable Strategies to address the wide variety of Submitter and Subscriber situations.

These Strategies assume that different populations of Subscribers within a state or served by a Federal Submitting Agency will be treated differently. These Strategies are per-end user population and are not exclusive; they can be used in combination. A Submitting Entity must ensure that all its Subscribers and subscriptions are covered by at least one of the Strategies.

These Strategies all address Expiration Date as the means of validation. In addition, these Strategies all address Expiration Date as separate from Rap Back Term Date. Non-criminal justice Subscribers and

Submitters will have to address Rap Back Term Date for all their subscriptions, which interacts with the Expiration Date as discussed in Items #6, #7, and #8 under Key Start-Up Requirements of the Rap Back Policy and Implementation Guide.

The following minimum requirements must be implemented for each subscription in addition to the specific requirements for the chosen Privacy Risk Mitigation Strategy.

a. Appropriate notice is required, at a minimum notifying all applicants of the retention and uses of the fingerprints. FBI CJIS has provided appropriate language.
b. A signed agreement between the Submitter and the Subscribing Entity is required that lays out subscription management requirements, to include:
    i. Requiring the Subscribing Entity to only submit prints of persons who have an authorizing relationship with the Subscriber and who have received appropriate notice of the uses of the fingerprints and of their options for removing the information when appropriate.
    ii. Requiring the Subscribing Entity to notify the Submitter of all events requiring entry/modification/ cancellation/termination of subscriptions in a timely manner.
    iii. Requiring the Subscribing Entity to review the NGI Rap Back subscription (and the Submitter-level Rap Back subscription, if one exists and is being synchronized with the NGI subscription) at an appropriate time prior to expiration and determine whether the subscription should be extended, renewed, canceled or allowed to expire. The subscription should not be extended before the person is officially re-authorized under the language of the statute. If the subscription is not extended, renewed, or canceled, the subscription will expire and be removed from file.
    iv. The Submitter and Subscribing Entity agree that the mandatory *Expiration Date* is acting as a validation and that these requirements constitute a Privacy Strategy.
c. Subscribers will be trained on correct use, emphasizing that Rap Back does not create any new authority to receive or use criminal history record information.
d. Subscribers will be audited for correct use.

Privacy Risk Mitigation Strategy #1. Pre-Notification with Mandatory Validation/Expiration within Three Years

For any population of Subscribers, pre-notification with a mandatory validation/expiration of no more than three years is an acceptable Strategy. Prior to the expiration, entities may extend or renew the subscription, if appropriate, under the validation/expiration list process, as discussed in the Non-Criminal Justice Policy and Implementation Guide, NGI Rap Back Service Transactions, Item #5, Receiving and Responding to the Monthly Rap Back Subscription Validation/Expiration Lists.

Privacy Risk Mitigation Strategy #2. Authority for Duration of a License

For licensing agencies that are given statutory authority to receive CHRI on their applicants/licensees for the period of time a license is active, no pre-notification or validation is required during that period. 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. If the license period is greater than five years, this Strategy may be used for the five year period, at which time the subscription would have to be reviewed under the validation/expiration list process. If the license is still active, the Expiration Date could be extended for the remainder of the license time period, up to another five years. At the end of that remaining time period, the subscription would have to be reviewed again under the validation/expiration list process.

Privacy Risk Mitigation Strategy #3. Statutory Authority for Set Period of Time

A specific state statute authorizing a regulatory/oversight entity access to an applicant's CHRI for a set period of time creates an equivalency to the licensing situation described in Strategy #2, and, as such, the same rules apply.

For a Subscribing Entity that is given statutory authority to receive CHRI on their applicants, volunteers, etc. for a clearly defined period of time, no pre-notification or validation is required during that defined time period—if the time period is no greater than five years. The subscription Expiration Date field must 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.

An example would be a state statute that gives volunteers the ability to volunteer over the course of a year for separate seasonal opportunities with a single regulatory/oversight entity. The regulatory/oversight entity can receive the Identity History Summary without pre-notification even if the volunteer has ended one activity and has not yet begun another activity during the designated year.

Privacy Risk Mitigation Strategy #4. One-Year Validation/Expiration

For any population of Subscribers, a one-year validation/expiration can serve in lieu of the pre-notification requirement. This Strategy requires the Expiration Date to contain a date no later than one year from the date the subscription was established.

Privacy Risk Mitigation Strategy #5. Subscription Synchronization Through Automated or Formalized Procedures

For any population of Subscribers, a written agreement between the Subscriber and the Submitter that contains strict processing requirements to keep the Subscriber and Submitter subscription records synchronized, as listed below. Other listed controls must also be included.

This Strategy requires the Expiration Date field to contain a date within the Subscription Term and no later than five years from the date the subscription was established. The foundation of Rap Back Privacy Risk Mitigation Strategy #5 is that strictly controlled procedures at key points in the process provide assurances that the NGI Rap Back subscription records accurately reflect the current status of the applicant/employee/ licensee, etc. within the Subscribers' files. As such, the requirements are intended to ensure that those controlled procedures are in place.

Those controls can be implemented in such a way as they include processing against the Submitter-level Rap Back system, if one exists, or that the processing is passed directly to NGI, if no Submitter-level Rap Back system exists.

The processing can be established whether the Submitter has not yet submitted any subscriptions for the related Subscriber to NGI, or the Subscriber already has created subscriptions in NGI and wants to begin to use this as a Strategy at a certain point in time.

Since this Privacy Risk Mitigation Strategy is specific to synchronizing individual subscriptions between the Subscriber and NGI, it is not an appropriate Strategy for Submitters who employ Category Based Subscription Management. By definition, Category Based Subscription Management does not maintain a one-to-one relationship between all individual subscriptions and NGI. As such, this Privacy Risk Mitigation Strategy may not be used by Category Based Management Submitters as an NGI Privacy Risk Mitigation Strategy

Although this Privacy Risk Mitigation Strategy is not appropriate for Category Based Subscriptions, the controls described here may be an appropriate guide for a Category Based Submitter to use in establishing the processing between themselves and any of their Subscribers. These controls can help the Subscriber demonstrably ensure that the subscriptions they have in their Submitter-level Rap Back system are valid. That level of controlled processing can be one factor in the Submitter's fulfilling their responsibilities under the Category Based Subscription Management Plan.

General Requirements

1. The Subscriber and Submitter must create these processes or processes that are functionally equivalent to these requirements.
2. The Submitter must verify that the controls are in place at the Subscribing Entity.
3. If there is any question regarding the sufficiency of a set of processes, the Submitter must consult CJIS.
4. CJIS can individually review and enable implementation situations that are not directly addressed in these stated situations and requirements. The mandate to CJIS in that instance would be to ensure that controls at least as protective as those stated here are equally maintained in any other proposed processes prior to their being enabled.
5. These requirements are described as being implemented through automated processing, but Submitters can agree to allow some of these functions to be performed manually with Subscribers.

Start Up Processing Requirements

1. At start-up, Subscribers must provide Submitters with a current file of all its individuals who are to be subscribed initially.
    a. From that file, the Submitter will populate the Submitter's Rap Back Service, if they provide that function.
    b. The Submitter will also ensure that all those subscriptions are sent to NGI's Rap Back Service and provide the Subscriber the NGI responses for their review. It is anticipated that these would be bulk EBTS submissions and responses.
    c. The Subscriber will review those responses to ensure that all start-up subscriptions are included in NGI, and the Submitter's system, as appropriate.
2. Submitters may also use this strategy for a population which already has subscriptions in NGI. Instead of a start-up list of subscriptions to be placed in NGI, the Subscriber and Submitter will create a one-time validation of all of that population's NGI subscriptions. That process will ensure that all NGI subscriptions for that population are valid and will create a starting point for implementation of this Privacy Risk

Mitigation Strategy that is functionally equivalent to the start-up list of subscriptions described in Item #1.

On-Going Processing Requirements

1. The Subscriber and Submitter will adhere to a strict processing protocol to keep the NGI subscriptions up to date on at least a monthly basis. The Subscriber must establish in writing and follow standardized procedures that must contain controls appropriate to the following processes:
    a. Creating the subscription as a part of their applicant or operational flow shortly after the individual becomes eligible for subscription.
    b. Sending the request for subscription and all Rap Back transactions to NGI under the Submitter's communications methodology.
    c. Receiving messages from the Submitter and routing them internally for action.
    d. Modifying subscriptions when the individual's status changes in their normal operational flow, or due to unanticipated circumstances, especially for removing the subscription when the person is no longer eligible.
    e. Processing monthly validation/expiration lists or other validation processes employed by the Submitter.
    f. Handling exceptions on a timely ad hoc basis.
2. The Submitter must establish and follow written procedures for their processing of these transactions.
3. The Subscriber/Submitter transaction processes must follow at least this frequency, flow, and content:
    a. The Subscriber will create a file of subscription "adds" and subscription "deletes" to be processed against the NGI and Submitter's Rap Back subscription records on at least a monthly frequency.
    b. The Submitter will transform those files from the Subscriber into appropriate EBTS transactions and send them to update NGI as soon as practicable, and no longer than 30 days. The Submitter will provide the Subscriber the responses with all actions taken by NGI. It is anticipated that these would be batch EBTS transactions.
    c. The Subscriber must compare that response action file against their original submission and notify the Submitter within one week of any anomalies that appear. The Subscriber and Submitter must resolve all anomalies in a timely manner.
    d. The Subscriber agrees to send all modifications, revocations, cancelations or other status changes to the Submitter on the first monthly update file after they occur.