ACCESS/WACIC/NCIC
USER ACKNOWLEDGMENT

1) Introduction

Since its inception, the National Crime Information Center (NCIC) has operated under a shared management concept between the Federal Bureau of Investigation (FBI) and state users. The NCIC Advisory Policy Board established a goal of having a single state agency in each state assume responsibility as the NCIC CJIS System Agency (CSA) for the state, through and by which NCIC users in that state would access NCIC. The CSA is responsible for the planning of necessary hardware, software, funding, and training of all authorized agencies within the state for complete access to NCIC data services.

The Board approved the CSA concept in order to unify responsibility for system user discipline, and adherence to system procedures and policies within each state. The CSA also serves as a central point in its state for handling record validations, quality control matters, dissemination of manuals and other publications, security matters, user training, audits, and any other problems concerning system use that may arise.

The responsibilities of the NCIC CJIS Systems Officer (CSO) are detailed in several documents related to the ACCESS/WACIC/NCIC system. This agreement outlines the varied responsibilities of a CSO as they pertain to the NCIC system.

The FBI NCIC responsibilities under this shared management concept include provision of:

- Operational, technical, and investigative assistance to NCIC users.
- Telecommunications lines to a state interface.
- Legal and Legislative review of matters pertaining to NCIC.
- Timely information on all NCIC aspects of system usage by means of the NCIC Operating Manual, Technical and Operational Updates, and related documents.
- Staff research assistance.
- Training and training materials to the CSAs.

The following documents are incorporated by reference and made part of this user acknowledgment: WACIC Manual, ACCESS Manual, NCIC Computerized Criminal History (CCH) Program Background, Concept and Policy, as amended or superseded by implementation of the Interstate Identification Index (III) Program; code of Federal Regulations, Title 28, Part 20; NCIC Standards as recommended by the NCIC Advisory Policy board and approved by the FBI Director; applicable federal and state laws and regulations; ACCESS/WACIC rules, regulation, and policies as recommend by the ACCESS Section.

2) DEFINITIONS

a) **NCIC CJIS System Agency (CSA)**

In Washington, the CSA is the Washington State Patrol.

b) **NCIC CJIS System Officer (CSO)**

The NCIC CSO is the Commander of the Washington State Patrol's Criminal Records Division.

The CSO is responsible for monitoring system use, enforcing system discipline, and assuring ACCESS, WACIC, and NCIC operating procedures are followed by all users of the respective telecommunications lines, as well as other related duties as outlined by this document.

c) **Technical Agency Coordinator (TAC)**

A TAC is the Point of Contact (POC) for his/her agency. A TAC shall be appointed at each terminal location and be Level II certified. The TAC shall be responsible for ensuring his/her agency is in compliance with state and NCIC policies and regulations, including validation requirements.

d) **Timeliness**

WACIC/NCIC records must be entered promptly to ensure maximum system effectiveness.

A timely entry in the Wanted Person File is made immediately once:

(i) The decision to arrest or authorize arrest has been made.

(ii) The terms of extradition have been established.

The date of want or warrant must be the date on which all those decisions were made. A timely removal from the file means an immediate clearing of the record

once the originating agency has documentation the fugitive has been arrested or is no longer wanted.

Timely system inquiry means initiation of the transaction before an officer releases a subject or begins writing an arrest or citation document of any kind; inquiry prior to the release of a person who has been incarcerated; or inquiry upon those who appear at a custodial facility to visit inmates.

Timeliness of entry/modification in the missing person file is generally the same as in the Wanted Person File.

Timely entry/modification of vehicle, license plate, and vehicle part data matches the wanted person standard, less the extradition considerations. Entry should be made as soon as a cross-check of the Department of Licensing's Registration File has been completed.

Timely entry of gun, article, and securities information means within a few hours of the time complete information is available.

e) **Validation**

Validation (vehicles, plates, fugitives, protection orders, missing person entries) obliges the originating agency identifier (ORI) to confirm the record is complete, accurate, and still outstanding or active.

f) **Completeness**

Complete records of any kind include all information available on the person or property at the time of entry. The validation process should include a review of whether additional information has become available (missing from original entry) that could be added.

Complete inquiries on persons include numbers that could be indexed in the record (i.e., Social Security Number, passport, Vehicle Identification Number, license plates, drivers' license, etc.). Inquiries should, be made on all names/aliases used by the suspect. Complete vehicle inquiries include VIN and license plate numbers.

g) **Accuracy**

The accuracy of WACIC/NCIC data must be double-checked by a second party. The verification should include assuring the data in the WACIC/NCIC record matches the data in the investigative report and that other checks (VIN and/or license numbers) were made. Agencies lacking support staff for this cross-checking should require the case officer to check the record, as he/she carries primary responsibility for seeking the fugitive or the stolen property.

or a notice of a specific amount of time necessary to provide a response to the request for record confirmation.

ii) **PRIORITY 2: ROUTINE** Confirm the hit within one hour. Generally, this priority will be used when the person is being held on local charges, property has been located under circumstances where immediate action is not necessary, or an urgent confirmation is not required.

Each agency must within one hour, furnish to an agency requesting a record confirmation, a response indicating a positive or negative confirmation or a notice of a specific amount of time necessary to provide a response to the request for record confirmation.

An agency requesting confirmation which fails to receive a response to the first request shall generate a second request with a copy to the CSO. The CSO will institute appropriate action to ensure proper response to a hit confirmation request and to comply with system standards. This appropriate action may include canceling the record by the CSA.

5) QUALITY ASSURANCE RESPONSIBILITIES

a) Introduction

i) Criminal justice agencies have a specific duty to maintain records that are accurate, complete, and up-to-date. The CSA will ensure there are standards for security, audits, and personnel training; which would allow the dissemination of accurate and up-to-date records.

b) Record Quality

i) Errors discovered in WACIC/NCIC records are classified as serious errors, form errors, or an error trend.

- Serious errors: WACIC/NCIC will advise the ORI via teletype message of an apparently erroneous record and request it be verified, changed, or canceled within 24 hours. The record will be canceled if neither a response is received nor corrective action has been taken during the allotted time.

- Form errors or error trends: the CSA will notify the ORI by letter of the corrective action to be taken. No further notification or action will be taken by the CSA.

c) **Record Validation**

i) NCIC/WACIC periodically prepares listings of records on file for validation purposes. Validation listings are prepared pursuant to a schedule, as published in the WACIC Operating Manual. These listings are mailed to the originating agency.

Validation requires the originating agency to confirm the record is complete, accurate, and still outstanding or active. Validation is accomplished by reviewing the original entry and current supporting documents, and by recent consultation with any appropriate complainant, victim, prosecutor, court, motor vehicle registry files, or other appropriate source or individual. In the event the ORI is unsuccessful in its attempts to contact the victim, complainant, etc., the entering authority must make a determination based on the best information and knowledge available whether or not to retain the original entry in the file. Validation procedures must be formalized and copies of these procedures must be on file for review during an NCIC/WACIC/ACCESS audit.

d) **Definition of Validation Certification**

i) The records contained on the validation listing have been reviewed by the originating agencies.

ii) The records which are no longer current have been removed from WACIC/NCIC and all records remaining in the system are valid and active.

iii) All records contain all available information.

iv) The information contained in each of the records is current and accurate, including appropriate extradition information.

If the CSA has not received a certification response from an agency within the specified period of time, the CSA will purge from WACIC/NCIC all records which are the subject of that agency's validation listings. (NOTE: If a CSA fails to certify any validation listing to the NCIC within the specified time, all invalidated records from that state will be purged by the NCIC).

6) SECURITY RESPONSIBILITIES

a) **General**

i) Security guidelines, relating to WASIS and NCIC III criminal history record information, are set forth in the NCIC Computerized Criminal History (CCH) Program Background Concept and Policy as superseded by the III program, the CJIS Security Policy in Code of Federal Regulation, Title 28, Part 20,

Subparts A and C and by state statute in RCW 10.97 and Washington Administrative Code, chapter 446-20.

All agencies participating in ACCESS must comply with and enforce system security.

b) **Originating Agency Identifier (ORI)**

i) The assignment of an ORI to an agency is not a guarantee of access to the systems. The CSA decides who may access WACIC/NCIC.

The CSO will coordinate the assignment of new ORI numbers, the change in ORI location or address, any other changes, cancellations, or retirements of ORIs accessing WACIC/NCIC. The agency shall notify the CSO of any such changes.

Application for assignment of new ORI's shall be made directly to the CSO. Such application shall contain documentation of the agency's statutory authority as a criminal justice agency and a statement that indicates the agency allocates more than 50 percent of its annual budget to the administration of criminal justice. Non-criminal justice agencies will be denied an ORI, unless under management control of a criminal justice agency, a copy of the management control agreement must be submitted to the CSO.

7) COMPUTERIZED CRIMINAL HISTORY RECORD INFORMATION (CHRI) RESPONSIBILITIES

a) Each agency shall conform to system policies, as established by the ACCESS/ WACIC manual, before access to CHRI is permitted. This will allow for control over the data and give assurance of system security.

b) The CSA is responsible for the security throughout the system it services, including all places where terminal devices are located. Upon determination that a terminal is in non-conformance with system management or security policy, the CSA has the authority to impose sanctions, including termination of service.

c) The rules and procedures governing direct terminal access to criminal history record information shall apply equally to all participants in the system.

d) All criminal justice agencies having direct access to computerized CHRI data from the system shall permit an NCIC or WACIC audit team to conduct appropriate inquiries with regard to any allegations of security violations. Agencies must cooperate with these audits and respond promptly.

e) All computers and manual terminals interfaced directly with the ACCESS/WACIC/NCIC systems for the exchange of criminal history record

information must be under the management control of a criminal justice agency, as defined by the NCIC CCH background and policy document.

f) Each agency shall have in place a system for logging all inquiries of the III, which log shall include the name of the individual within the criminal justice agency to whom the response was given. Logs must contain at least one of the following:

   i) First initial and last name of individual requesting the information or

   ii) Badge or personnel number unique to the individual (does not change with promotions etc.).

g) CHRI logs must also contain a specific reason for the request i.e. burglary investigation, criminal justice applicant.

h) Each agency receiving an III response shall record any secondary dissemination. These logs shall be maintained for at least 12 months from the date of inquiry.

i) Agencies must institute a program of systematic self-audits as a means of guaranteeing the completeness and accuracy of the information in the system. These self-assessments should be on a continual basis to ensure both quality assurance and compliance with standards.

j) The TAC must keep on file a signed dissemination statement of all users (see example of dissemination statement in section IV).

k) Compliance audits will cover the following areas of the III, WACIC/NCIC stolen property, and person records:

   i) **Accuracy**

   All WACIC/NCIC entries shall contain no erroneous data.

   ii) **Completeness**

   All information contained in a WACIC/NCIC entry or in a criminal history record shall contain the most pertinent information available.

   iii) **Timeliness**

   All entries, modifications, updates, and removals of information shall be completed, processed, and transmitted as soon as possible, in accordance with established standards.

iv) **Locates**

All wanted/missing persons, and property records, which are apprehended or recovered, shall be promptly placed in "located" status, except those found outside of the stated area of extradition or return. ***Instances where a jail is full and unable to accommodate a prisoner locates shall not be used.***

v) **Security**

It is the responsibility of an agency to protect its information against unauthorized access, ensuring confidentiality of the information in accordance with laws, policies, regulations, and established standards.

vi) **Dissemination**

All information released shall be in accordance with applicable laws and regulations, and a record of dissemination of criminal history records shall be maintained for one year and made available for NCIC/WACIC audit review.

For those agencies providing ACCESS Services through regional computer systems to outside agencies, the TAC shall be responsible for the dissemination of all administrative messages received on the 24 hour printer to those agencies

8) ADMINISTRATIVE RESPONSIBILITIES

a) The agency shall respond to requests for information by the FBI NCIC or WACIC in the form of questionnaires, surveys, or similar methods, to the maximum extent possible, consistent with any fiscal, time, or personnel constraints of that agency.

b) The CSO shall offer system training to agencies accessing WACIC/NCIC through the state computer system. Agencies shall assign appropriate employees to attend classes when offered. If employees are using inquiry only functions, they must attend Level I certification training. Employees entering information into the NCIC/WACIC system and Technical Agency Coordinators (TAC) must attend Level II certification training. All certifications must be renewed biennially.

c) The CSO will distribute, within the state criminal justice community, the ACCESS/WACIC manuals, NCIC Code Manuals, and as requested, miscellaneous publications in order to enhance effective use of the WACIC/NCIC system. The agency shall incorporate such changes upon receipt.

h) **Operational Responsibilities**

To ensure the proper operation of WACIC/NCIC the standards, procedures, formats, and criteria, as contained in ACCESS/WACIC operating manuals, will be followed. A specific operational situation is:

3) REQUIREMENTS FOR TELETYPE HIT CONFIRMATION:

a) Every terminal agency that enters records destined for NCIC/WACIC must ensure teletype hit confirmation is available for all records, except III, 24 hours per day either at the agency or through a written agreement with another agency at its location.

b) The terminal agency printer must be monitored 24 hours per day. In the event that 24 hour per day hit confirmation coverage is not available, the terminal agency printer must be capable of being forwarded to a 24 hour a day facility.

c) Terminal agencies that are not available 24 hours per day must place instructions for after hour hit confirmation in the miscellaneous field to include a 24 hour telephone number of the agency responsible for confirming hits.

d) WSP recommends agencies use the NLETS network for hit confirmation. Even if the initial confirmation is handled by telephone, NLETS should be used for documentation. NLETS created an inquiry (YQ) message and a response (YR) message for hit confirmation. Responsibilities for the hit confirmation process are shared between the agency that received the hit and the agency that entered the record.

e) The arresting agency must place a computer locate message on all confirmed hits.

f) The Originating Agency must clear the hit after it has been located.

4) HIT CONFIRMATION POLICY

a) The agency that obtains a hit has the ability to designate to the entering agency one of two priorities for confirmation.

i) **PRIORITY 1: URGENT** Confirm the hit within 10 minutes. In those instances where the hit is the only basis for detaining a suspect or the nature of a case requires urgent confirmation of a hit, the highest level of priority should be specified.

Each agency must, within 10 minutes, furnish to an agency requesting a record confirmation, a response indicating a positive or negative confirmation

ACKNOWLEDGMENT

As an agency head/director serving in the ACCESS/WACIC/NCIC system, I hereby acknowledge the duties and responsibilities as set out in this document, as well as those documents incorporated by reference. I acknowledge that these duties and responsibilities have been developed to ensure the reliability, confidentiality, completeness, and accuracy of all records contained in or obtained by means of the WACIC/NCIC system. I also acknowledge that a failure to comply with these duties and responsibilities will subject my agency to various sanctions. These sanctions may include the termination of ACCESS/WACIC/NCIC services to my agency.

Agency Head — JOHN T. CALKINS (Print Name)

Signature

Agency Name — CITY OF PACIFIC

Today's Date — 2/1/06

Return this signature sheet to the State Patrol

ACCESS/WACIC/NCIC
USER ACKNOWLEDGMENT
ADDENDUM

9) Encryption Requirements

The Criminal Justice Information Services (CJIS) requires "all CJIS data transmitted through any public network segment, over dial-up, or internet connections shall be immediately protected with a minimum of 128 bit encryption".

All agencies that connect to a regional management system to receive ACCESS information must provide Federal Information Processing Standards (FIPS) 140-2, 128 bit encryption to all users. The Washington State Patrol, as the CSA, provides the encryption standard to all regional management systems through a Cisco 3030 Concentrator located at the WSP Information Technology Division. Agencies must complete encryption to any additional users of their regional systems (i.e. mobile data terminals, wireless, blackberries etc.) See the Criminal Justice Information Services (CJIS) Security Policy for detailed standards. All agencies currently using the WEBMSS application meet the current encryption requirements.

As the agency head/director , I hereby acknowledge my agency responsibility to provide 140-2 FIPS compliant 128 bit encryption to all users of my regional system to maintain compliance with CJIS standards. Encryption standards are verified through a triennial security audit conducted by the WSP Information Security Officer.

I also acknowledge that failure to comply with these equipment upgrades and the maintenance thereof, will subject my agency to various sanctions. These sanctions may include termination of ACCESS/WACIC/NCIC services to my agency.

Agency Head JOHN T. CALKINS _____
(Print name) (Signature)

Agency Name Pacific Police Date 1/26/06

Information Technology (IT)
Contact Person: Brian Ferrill

Contact Number: 425-442-8069