Table of Contents

Procedure #:	01.01.000	**Effective Date:**	June 1, 2012
Supersedes:	ACCESS Manual, TAC Guide, Ready Reference Guide, WACIC Manual	**See Also:**	
Applies To:	All ACCESS Users	**CALEA:**	

I. DEFINITIONS

A. A Central Computerized Enforcement Service System (ACCESS)

1. A Central Computerized Enforcement Service System (ACCESS) is a computer controlled communications system located at the Washington State Patrol (WSP) Information Technology Division (ITD) in Tumwater.

2. Through the use of special interfacing equipment, ACCESS extracts data from multiple repositories including the Washington Crime Information Center (WACIC), Washington State Identification System (WASIS), the National Crime Information Center (NCIC), the Department of Licensing (DOL), the Department of Corrections Offender File (DOC), The International Justice & Public Safety Network (Nlets), and PARKS. ACCESS provides a direct connection with NCIC when WACIC is non-operational.

3. By legislative act covered in the Revised Code of Washington (RCW) 43.89.010, 43.43.785, and 43.43.800, the Chief of the WSP is vested with the authority to administer all operating phases of ACCESS and WACIC.

4. Agencies retain local responsibility for proper operator performance and training, strict adherence to regulations, and prompt handling of traffic.

B. Washington State Crime Information Center (WACIC)

1. WACIC is a statewide computerized repository for multiple types of entries including wanted persons, vehicles, persons of interest and others. All entries are completed and managed by the contributing agencies. This state repository was established as an information source for all criminal justice agencies.

2. WACIC stores criminal justice information that can be instantly retrieved and furnished to any authorized criminal justice agency. For WACIC purposes, criminal justice information is defined as "information collected by criminal justice agencies that is needed for the performance of their legally authorized, required function."

3. WACIC generates a number for every entry into the system. This number is called a WAC. It contains a two-character year designator, a one-letter file designator, and a seven-digit sequential number.

C. National Crime Information Center (NCIC)

1. The NCIC system provides a similar function to that of WACIC, but on a national level. NCIC generates a unique ten digit number for every entry into the system. This is called a NIC number. The NIC number consists of a file designator and the remaining nine denote the message sequence number.

II. ROLES AND RESPONSIBILITIES

A. The Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Division manages the NCIC system. The FBI CJIS Division establishes rules to maintain system integrity, which all user agencies must abide by. These rules are defined in the NCIC Operating Manual and the CJIS Security Policy. Each CJIS Systems Agency (CSA) that accesses NCIC shall be audited at least once every three years by the FBI CJIS audit staff. This audit shall include a sample of state and local criminal justice agencies. The objective of this audit is to verify adherence to FBI CJIS policy and regulations and is termed a compliance audit.

B. The Washington State Patrol (WSP) is designated by the FBI as the CSA. The CSA is a criminal justice agency which has overall responsibility for the administration and usage of the FBI's CJIS Division programs within their jurisdiction. The WSP is the manager of the ACCESS system. The CSA is also responsible for establishing and administering an information technology security program. The CSA may impose more stringent protection measures than defined by the NCIC Operating Manual and CJIS Security Policy.

C. The head of each CSA shall appoint a CJIS Systems Officer (CSO). The CSO is an individual located within the CSA responsible for the administration of the CJIS network for the CSA. The CSO for Washington State is the WSP Criminal Records Division Administrator. The ACCESS Section is designated to train, audit and provide assistance to all Criminal Justice Agencies (CJA) within the state.

D. The Terminal Agency Coordinator (TAC) serves as the point-of-contact at the local agency for matters relating to CJIS information access. The TAC administers CJIS systems programs within the local agency and oversees the agency's compliance with ACCESS and CJIS systems policies.

E. An Information Technology (IT) point of contact must be designated at each criminal justice agency. The technical point of contact administers CJIS systems programs within the local agency and oversees the agency's compliance specifically related to the technical requirements with ACCESS and CJIS systems policies.

F. A CJA is defined as a court, a governmental agency, or any subunit of a governmental agency which performs the administration of criminal justice

pursuant to a statute or executive order and which allocates a substantial part of its annual budget to the administration of criminal justice.

G. A Non-criminal Justice Agency (NCJA) is defined (for the purposes of access to Criminal Justice Information [CJI]) as an entity or any subunit thereof that provides services primarily for purposes other than the administration of criminal justice.

III. SYSTEM DESCRIPTION

A. WACIC system participants include local, state, and federal criminal justice agencies throughout the state of Washington. NCIC system participants include local, state, and federal criminal justice agencies.

B. Most records are placed directly into the WACIC and NCIC systems by an originating agency (agency holding a warrant, missing person report, or theft report, etc.) through a terminal tied into the network. Some types of records (i.e. immigration violators, foreign fugitives etc.) are entered by a specific agency.

C. Below is a list of files contained and databases available through the ACCESS Switch. This manual explains each file and database in detail.

ACCESS Operations Manual	WACIC	NCIC
Article File		X
Boat File		X
Criminal History File	X	X
Dental Data File	X	X
Department of Corrections (DOC) File	Database	
Department of Licensing (DOL) File	Database	
Foreign Fugitive File		X
Gang File		X
Gun File		X
Identity Theft File		X
Image File	X	X
Immigration Violator File		X
License Plate File	X	X
Marijuana File	Database	
Missing Person File		X
Monitored Population Registration	X	
National Instant Criminal Background Check Systems (NICS)	Database	
Non-Criminal Justice Agency (NCJA)	N/A	N/A
National Sex Offender Registry File		X
Park File	Database	
Pawned and Recovered File	X	
Person of Interest File	X	
Protection Order File	X	X
Protective Interest File		X
Securities File		X

ACCESS Operations Manual	WACIC	NCIC
Supervised Person File	X	X
Threat Screening Center (TSC)		X
Unidentified Person File		X
Vehicle File	X	X
Vehicle/Boat Part File		X
Violent Person File		X
Wanted Person File	X	X

IV. ACCESS POLICY

A. All users must conform to the policies and procedures as a condition of their participation in the ACCESS/WACIC system. Any questions regarding policies and procedures may be referred to:

Washington State Patrol
Criminal Records Division – ACCESS Section
PO Box 42619
Olympia WA 98501-2619
Telephone: (360) 534-2010
Email: access@wsp.wa.gov

B. System Use

1. Information obtained via ACCESS can only be used by criminal justice agencies for criminal justice purposes. Obtaining information through ACCESS for private business or personal reasons, or furnishing any WACIC, NCIC, DOL, DOC, Nlets, WASIS, PARKS and III information to another person for such uses, is prohibited.

2. The originating agency assumes total responsibility for the credibility of information transmitted through ACCESS or entered into any criminal justice databases. Agencies maintain the responsibility for record accuracy, updates, and prompt clearance of those records.

V. USE OF ACCESS AND DISSEMINATION

A. This manual contains instructions designed to guide participants in the use of WACIC and NCIC systems. All users must observe any restrictions related to the use or dissemination of the information obtained through ACCESS. The WSP and the ACCESS Section retains the responsibility to notify agencies of the restrictions and regulations.

B. Dissemination of WACIC and NCIC information to the public must be completed through the public disclosure process. Should the public request information from WACIC or NCIC, agency personnel may answer “yes” or “no” regarding the status of a record but may not disclose additional information in the query outside of the public disclosure process.

C. When using a facsimile to send Criminal Justice Information ensure the individual receiving the information is authorized and the area where the

facsimile will be received is a secure location as defined by the CJIS Security Policy.

VI. STATUTES RELATED TO ACCESS

A. The following laws regulate the use of ACCESS and CJI data. Refer to this section when questions arise regarding proper dissemination and rules relating to ACCESS use.

1. WAC 446-20-270 Establishment of procedures
2. WAC 446-20-220 Physical security
3. WAC 446-20-230, 250, 280 Personnel Clearances
4. WAC 446-20-240 Training
5. RCW 43.43.500, 510 WACIC
6. RCW 10.97 Criminal history
7. RCW 10.97.030 Definition of a criminal justice agency
8. RCW 42.56.240 Investigative, law enforcement, and crime victims
9. RCW 46.52.120 Case record of convictions and infractions- cross-reference to accident reports
10. RCW 46.52.130 Abstract of driving record –access -fees- violations
11. RCW 46.12.640 Disclosure, violations, and penalties
12. RCW 10.99 Protection orders
13. RCW 26.50 Protection orders
14. RCW 10.14 Protection orders
15. RCW 7.90 Protection orders
16. RCW 74.34 Protections orders
17. 5 USC 552 Freedom of Information Act (FOIA)
18. 18 USC 1030 Fraud and related activity in connection with computers
19. 28 USC 534 Acquisition, preservation, and exchange of identification records and information; appointment of officials
20. 28 CFR 20.3 Definitions (criminal justice agency)
21. 28 CFR 20.33 Dissemination of criminal history information
22. 28 CFR 105.27 (b), (c) and (d) Miscellaneous provisions
23. Pub. L 92-544
24. Pub. L 101-630
25. Pub. L 105-276/42 USC 1437d (q)(1) Housing and urban development
26. Criminal Justice Information Services (CJIS) Security Policy

B. Criminal History and Dissemination

1. 28 CFR 20.33 Dissemination of criminal history information
2. 28 USC Part 20, 534
3. 28 USC 552
4. Pub. L 92-544
5. Pub. L 101-630
6. Pub. L 105-276/42 USC 1437d (q)(1) Housing and urban development
7. WAC 446-20-270
8. RCW 10.97

C. Department of Licensing information through ACCESS

1. RCW 42.56.240(1)
2. RCW 46.52.120 (ADR)
3. RCW 46.52.130 (ADR and CCDR)
4. RCW 46.12.640 (Disclosure, violations, and penalties)

D. Some files within NCIC are considered sensitive and non-disclosable. Those files include:

1. Supervised Release
2. Gang
3. Known or Suspected Terrorist (KST)
4. Protective Interest
5. Inactive Protection Order
6. NICS Denied Transactions
7. Violent Person
8. Identity Theft
9. National Sex Offender Registry (NSOR)
10. Interstate Identification Index (III)
11. Immigration Violator

Procedure #:	01.02.000	**Effective Date:**	June 1, 2012
Supersedes:	ACCESS Manual, TAC Guide, Ready Reference Guide, WACIC Manual	**See Also:**	
Applies To:	All ACCESS Users	**CALEA:**	

I. AUTHORIZATION TO INSTALL ACCESS TERMINALS

A. Authorized agencies who obtain computer terminal connections and access CJI must fall under the definition of a criminal justice agency or subunit within an agency that performs the administration of criminal justice.

B. All agencies requesting ACCESS connectivity or requesting terminals must have a completed and approved application on file and a billing account prior to receiving service. Within the application process, agencies will be required to provide their statutory authority, reason for access, and verification of the system security.

II. REGIONAL SYSTEMS

A. All regional criminal justice information systems must notify the ACCESS Section should they decide to provide ACCESS services through their regional to another criminal justice agency. No regional system will authorize or install a terminal which has the capability to access ACCESS without prior authorization from the ACCESS Section.

III. ISSUANCE OF ORIS

A. Agencies who have submitted applications and have been approved for ACCESS services and access to CJI will receive their own primary Originating Agency Identifier (ORI) from the FBI. The FBI assigns ORIs based on the agency designation (i.e. court, communications center, police department, prosecutor's office, etc.). For more information on the issuance of ORIs, refer to the NCIC Operating Manual.

B. Additional ORIs are issued for each terminal that will connect to the ACCESS System. Each ORI is unique and provides the technical route for messages to be sent or received to the proper destination.

1. Example:
Olympia Police Department runs a wanted persons check using their ORI WA0340115. The response will route back to the ORI WA0340115 where the query originated.

C. ACCESS edits the ORI Field in all transactions to ensure ORI validity and the terminal submitting the transaction is allowed to use the ORI. If the ORI Field in a transaction is left blank, ACCESS inserts the default ORI assigned to the terminal.

D. ORIs are also subject to validations to ensure they remain current and the applicable agency information is accurate. They are validated on a biennial basis. Each CSA is responsible for verifying the accuracy of every ORI accessing Nlets and NCIC through the respective state/federal system. The validation process includes verifying an agency's status and authority, as well as the other information listed in the ORI record.

1. Example:
   Verifying the telephone number, street address, etc. are correct.

E. Each agency that has access to NCIC/WACIC is responsible to maintain current information in the ORION File maintained by Nlets and the ORI File maintained by NCIC. The fields that can be updated by the agency include:

1. Street address
2. PO Box
3. Zip code
4. Telephone number
5. Hit confirmation phone number
6. Fax number

IV. AGENCY REQUESTS FOR ADDITIONAL ORIS

A. Agencies may request additional ORIs at any time. They must make the request through the WSP ITD Customer Services Unit at emailing the completed form to ITDHelp@wsp.wa.gov. The following information is required to submit your request:

1. Agency ORI
2. Terminal locations
3. Number of terminals requested
4. Type of terminal (wireless, laptop, desktop)
5. Type of application (Spillman, New World, Omnixx, etc.)

B. A work order will be created and sent to the ACCESS Section. The ACCESS Section, will conduct a short audit of the agency to verify compliance standards are being met. The following areas are checked:

1. Criminal history logs
2. User certifications are current with no expired users
3. No outstanding audit issues
4. Validations are current

C. If the new ORIs are for terminals located in a new physical location, then a site security visit must be conducted. ACCESS Section Staff will conduct

site security visit to ensure the new terminal location is secure. The following areas will be reviewed during the site security visit:

a. Who has access, including unescorted access, to the site
b. Who performs the cleaning/facilities maintenance at the site
c. Method of disposal for CJI media
d. Review what terminals will be located at the new site

V. ORI INQUIRIES

A. Should an agency need assistance locating an ORI or updating agency information, accessing information via Nlets can provide telephone numbers, addresses, faxes, etc. for other terminal agencies.

1. Example:

a. By ORI L;TQ..CA.ORI/CA0371100
b. By Location (LOC) L;TQ..CA.LOC/SAN DIEGO
c. By Type (TYP) and LOC L;TQ..CA.TYP/JJ.LOC/SAN DIEGO

Nlets ORION Agency Type (TYP) Codes			
	Law Enforcement		**Criminal Justice**
PD	Any agency of city government	JA	Any prosecutor
SO	Any agency of county government	JC	Any corrections agency
SA	Any state agency with statewide jurisdiction	JG	Any probation agency
FE	Federal agency	JJ	Any court agency
LE	Any agency not fitting above categories	JF	Any federal non-law enforcement
	Miscellaneous	CJ	Other misc criminal justice agencies
FN	Foreign departments not located in a state, DC, or Puerto Rico	NJ	Non-criminal justice agencies

2. Example:

a. By FED L;TQ..CA.FED/FBI
b. By FED LOC L;TQ..CA.FED/FBI SAN DIEGO

Nlets ORION Federal Agency Location (FED) Codes			
ATF	Alcohol, Tobacco, Firearms	IRS	Internal Revenue Service
BIA	Bureau of Indian Affairs	MSC	All others not listed refer to the Nlets Wiki/User Manual
DEA	Drug Enforcement Administration	NIS	Naval Investigative Service
DOI	Dept of Interior	OSI	Air Force Office of Special Investigation
DOJ	Dept of Justice	PIS	Postal Inspection Service
DOS	Dept of State	SSA	Secret Service
FAA	Federal Aviation Administration	USA	U.S. Army
FBI	Federal Bureau of Investigation	USC	U.S. Customs
INS	Immigration and Naturalization Service	USM	U.S. Marshals Service

Procedure #:	01.03.000	**Effective Date:**	June 1, 2012
Supersedes:	ACCESS Manual, TAC Guide, Ready Reference Guide, WACIC Manual	**See Also:**	
Applies To:	All ACCESS Users	**CALEA:**	

I. SYSTEM RESPONSIBILITY

A. The WSP, as the state CSA, is responsible for system security and its enforcement for all other agencies it services.

B. The WSP and the FBI use hardware and software controls to help ensure system security. However, final responsibility for ensuring the protection of criminal justice information rests with the individual agencies with a connection to the ACCESS system. Further information regarding system security may be obtained from the FBI's CJIS Security Policy. The policy can be found at https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center.

C. CJI is the term used to refer to all of the FBI CJIS provided data necessary for law enforcement and civil agencies to perform their missions including, but not limited to biometric, identity history, biographic, property, and case/incident history data. It is the agency's responsibility to protect CJI from unauthorized access or viewing.

D. The data stored in the WACIC and NCIC databases is documented criminal justice information and must be protected to ensure correct, legal, and efficient dissemination and use. Information may be obtained from WACIC and NCIC both directly and indirectly.

1. **Direct access** – the ability to make queries of CJI via the ACCESS system.

2. **Indirect access** – having the ability to view CJI in a local system (from a previous direct access query), but not able to make queries.

E. The individual receiving a request for CJI must ensure that the person requesting the information is authorized to receive the data. Unauthorized requests or receipt of WACIC or NCIC material may result in criminal proceedings or state or federal sanctions brought against the agencies and/or the individuals involved.

II. TARGET AREAS FOR SECURITY

A. System Security

1. ACCESS strictly adheres to the CJIS Security Policy.

2. The CJIS Security Policy defines and requires all agencies must have a physically secure location.

3. Law enforcement sensitive facilities and restricted/controlled areas shall be prominently posted and separated from non-sensitive facilities and restricted/controlled areas by physical barriers that restrict unauthorized access.

4. Every physical access point to sensitive facilities or restricted areas housing information systems that access, process, or display CJI data shall be controlled/secured in a manner which is acceptable to the CSO during both working and non-working hours.

5. Terminal locations must be secure from unauthorized access and all employees authorized to access files via the ACCESS system must be instructed on proper use and dissemination of information.

6. The screens of terminals must be located where CJI displayed cannot be read by unauthorized persons.

B. Personnel

1. WSP adheres to the CJIS Security Policy standards regarding personnel. Agencies must conduct a state of residency and national fingerprint-based background check for all personnel who have unescorted access to unencrypted CJI or unescorted access to physically secure locations or controlled areas (during times of CJI processing) prior to employment, assignment or providing CJI to individuals that are not escorted.

    a. For example, a city attorney who does not have an ACCESS connection, but is receiving CJI from your agency.

2. If the person resides in a different state than that of the assigned agency, the agency shall conduct state (of the agency) and national fingerprint-based record checks.

3. The agency Terminal Agency Coordinator (TAC) must retain the State Identification Number (SID) of each employee who uses ACCESS or maintains the application or network connection. Below is a list of personnel that may fall under the background check requirements:

    a. Law enforcement officers
    b. Communications/Dispatcher
    c. Records personnel
    d. Corrections personnel
    e. Court personnel
    f. Probation personnel
    g. Prosecutor’s office personnel
    h. Information Technology staff
    i. Technical vendors for applications and/or network assistance
    j. Contractors

4. All visitors to computer centers and/or terminal areas must be escorted by authorized personnel at all times. This would include:

    a. The public
    b. Prospective employees
    c. Custodial staff (that have not received a fingerprint-based background check)
    d. Contractors (that have not received a fingerprint-based background check)
    e. Vendors
    f. Non-criminal justice county and city employees who access the building or area where CJI information is available

5. All terminal operators and IT personnel who have direct access to CJI and those who have direct responsibility to configure and maintain computer systems and networks with direct access to CJI must have their proficiency reaffirmed annually. Refer to the Certification Section of this chapter for further clarification.

    a. These requirements must be met regardless of whether a terminal is in full-time or part-time operation. This also includes Mobile Data Terminal units (MDTs) mounted in patrol cars.

6. All unescorted personnel that would have access to the secure location would be required to have a state (of the agency) and national fingerprint-based background check completed. The unescorted personnel would also be required to view security awareness training and complete the test annually. The security training and test are found within CJIS online.

7. ACCESS requires all personnel who use or work on the connection to ACCESS to have a rebackground investigation conducted every five years. This follows the CJIS Security Policy recommendation. The required rebackground investigations include IT personnel. The agency TAC must conduct the rebackground checks.

    a. The following checks must be conducted to complete the rebackground checks:

        (1) QWH – Inquire on the Name and Date of Birth.

            (a) Use Purpose Code J.
            (b) Use rebackground as the reason.

        (2) QR – Inquire on the SID and/or FBI obtained from the QWH transaction.

            (a) Use Purpose Code J.
            (b) Use rebackground as the reason.

        (3) The date of the rebackground investigation must be documented for future ACCESS audits.
        (4) The TAC must notify the Washington State Patrol (WSP) ACCESS Section of any findings and request a variance for any of the following:

(a) Any conviction (Felony, Gross Misdemeanor or Misdemeanor).
(b) Any arrest without a final disposition.

(5) Unless otherwise determined by the ACCESS Section, it will be up to the discretion of our agency whether to limit the use of ACCESS.
(6) Do not retain the rapsheet information.

8. The TAC must notify ACCESS of any personnel with unescorted access to unencrypted CJI or unescorted access to physically secure locations who have any convictions, any arrest history other than 'dismissed', or who is a fugitive. If the agency chooses to allow the person continued unescorted access, they must ask for a variance. The ACCESS Section Manager will review the request and notify the TAC if the subject is allowed to be around CJI or not.

a. To request a variance, the TAC completes the Variance Request form in the WSP Watch Portal.

C. Disposal of Media

1. Electronic media

a. The agency shall destroy or sanitize all electronic media used for processing or storing of CJI before final disposal for reuse. The agency shall maintain written documentation of the steps taken to sanitize or destroy electronic media. Agencies shall ensure the sanitization or destruction is witnessed or carried out by authorized personnel.

2. Physical media

a. Physical media shall be securely disposed of when no longer required, using formal procedures. Formal procedures for the secure disposal or destruction of physical media shall minimize the risk of sensitive information being compromised by unauthorized individuals. Physical media shall be destroyed by shredding or incineration.

3. The disposal process must be observed by a fingerprinted criminal justice employee.

a. The disposal process does not need to be observed if the contracted company has all been fingerprinted, viewed security awareness training and signed a CJIS Security Addendum. A copy of the Addendum must be provided to the ACCESS Section during the audit.

III. ENCRYPTION STANDARDS

A. WSP adheres to the CJIS Security Policy standards for encryption ensuring the cryptographic modules used are Federal Information Processing Standard (FIPS) 140-2 certified and use a symmetric cipher key strength of at least 128 bit strength.

B. All local agency users are responsible to complete end-to-end encryption. The cryptographic module used shall be FIPS 140-2 certified and use a

symmetric cipher key strength of at least 128 bit strength.

C. Refer to the most current CJIS Security Policy for additional clarification of encryption standards.

II. FIREWALLS

A. Agencies must adhere to the CJIS Security Policy with regard to the required firewalls.

III. IDENTIFICATION AND AUTHENTICATION

A. Each individual's identifier/password shall be authenticated at either the local interface agency or CSA level. Agencies need to adhere to the current CJIS Security Policy for logon ID and/or password standards.

B. Multifactor authentication is required for all personnel accessing CJI.

IV. NETWORK DIAGRAM

A. The agency shall ensure that a complete topological drawing depicting the interconnectivity of the agency network, to criminal justice information, systems and services is maintained in a current status and marked "For Official Use Only (FOUO)". Refer to the CJIS Security Policy for further clarification.

V. MOBILE/REMOTE DEVICES

A. The agency shall: (i) establish usage restrictions and implementation guidance for wireless technologies; and (ii) authorize, monitor, and control wireless access to the information system. Wireless technologies, in the simplest sense, enable one or more devices to communicate without physical connections—without requiring network or peripheral cabling.

1. Examples of wireless technologies include, but are not limited to: 802.11x, cellular networks, Bluetooth, satellite and microwave.

B. Wireless technologies require at least the minimum security applied to wired technology and, based upon the specific technology, may require some additional security controls. Refer to the CJIS Security Policy for further standards.

VI. SECURITY INCIDENTS OF CJI DATA

A. The agency shall promptly report incident information to appropriate authorities. Information security events and weaknesses associated with information systems shall be communicated in a manner allowing timely corrective action to be taken. Formal event reporting and escalation procedures shall be in place. Wherever feasible, the agency shall employ automated mechanisms to assist in the reporting of security incidents. All employees, contractors, and third party users shall be made aware of the procedures for reporting the different types of event and weakness that might have an impact on the security of agency assets and are required to report any information security events and weaknesses as quickly as possible to the designated point of contact. Refer to the CJIS Security Policy for further clarification.

B. All agencies are required to have a data breach reporting policy in place,

that at a minimum requires all data breaches involving CJI to be reported to the ACCESS ISO using the current reporting form found on the ACCESS webpage.

Procedure #:	01.04.000	**Effective Date:**	June 1, 2012
Supersedes:	ACCESS Manual, TAC Guide, Ready Reference Guide, WACIC Manual	**See Also:**	
Applies To:	All ACCESS Users	**CALEA:**	

I. DEFINITIONS

A. The ACCESS System journal contains a log of all transactions (sent and received) for the past three years plus current. This type of journal search will include any transaction where the requested information was run through a terminal within Washington State.

C. The FBI provides the capability of running a journal search throughout the entire country. These journal searches will include any instance where the information requested was run through the NCIC database by any state. The III database can also be searched. The offline search by NCIC searches:

1. All inquiries as far back as 1990.
2. All records within a specified file as far back as when the file was created.
    a. For example, the Missing Person File was created in 1975. The NCIC offline search can search any missing person record back to 1975.

II. REASONS TO RUN A JOURNAL SEARCH

A. Journal search requests can be made for the following reasons:

1. Investigative Tool: Agencies can request a journal search to assist with an investigation. For example, a police department is investigating a missing person case and would like to know if a vehicle or name has been inquired on during a given period of time.
2. Public Disclosure: The public is allowed to request a journal search to obtain information on messages that were sent and received by law enforcement. For example, a citizen believes they are being harassed by an officer and wants to know if their information has been inquired upon during a given period of time.
3. ACCESS Misuse Investigations: Agencies can request a journal search to assist in determining if an employee(s) has misused Criminal Justice Information (CJI). For example, an officer is accused of running his own license plate and criminal history

through ACCESS. For more information on misuse, refer to the ACCESS Misuse Section of this file.

III. JOURNAL SEARCH REQUESTS

A. ACCESS System journal search requests must be made to the WSP Customer Services Group at ITDHelp@wsp.wa.gov or call (360) 705-5999.

1. The following information should be included with your request:

   a. Requestor's name, telephone number, email, and address where the results should be sent.
   b. Information for the inquiry (full name, date of birth, terminal number, plate number, the time frame, etc.).
   c. The requestor should advise that the journal search is for an investigation, public disclosure, or ACCESS misuse.

B. NCIC offline searches are available through the FBI's Investigative and Operational Assistance Unit (IOAU). To request a search, contact IOAU at ioau@leo.gov or call (304) 625-3000.

1. The following information should be included with your request:

   d. Agency name and ORI
   e. Requestor's name, telephone number, email, and address where the results should be sent.
   f. Information for the inquiry (full name, date of birth, terminal number, plate number, the time frame, etc.).
   g. The requestor should advise what type of investigation the journal search is being requested for (murder, burglary, etc.).
   h. If a search of the III is requested, then it must be specified within the request.

Procedure #:	01.05.000	**Effective Date:**	June 1, 2012
Supersedes:	ACCESS Manual, TAC Guide, Ready Reference Guide, WACIC Manual	**See Also:**	
Applies To:	All ACCESS Users	**CALEA:**	

I. REGULATIONS

A. If an agency suspects an employee of obtaining information from any of the systems available through ACCESS for non-criminal justice purposes, the ACCESS Section must be immediately notified. Some examples are:

1. Running criminal history on family or friends
2. Running a vehicle registration for personal use
3. “Visiting” or sending inappropriate administrative messages across a mobile data terminal ACCESS connection

II. REPORTING

A. The ACCESS Section will provide the agency with an ACCESS Violation Incident Report to complete and return. The agency must investigate the alleged misuse and provide all data requested to ACCESS via the Incident Report.

B. Agencies may request an ACCESS System Journal Search as part of the investigation. Make all requests to the WSP Customer Services Group at ITDHelp@wsp.wa.gov or call (360) 705-5999. The following information should be included with your request:

1. Requestor’s name, telephone number, email, and address where the results should be sent.
2. Information for the inquiry (full name, date of birth, terminal number, plate number, the time frame, etc.).
3. The requestor should advise that it is an investigation for misuse.

D. If the misuse is confirmed, the agency may choose their own disciplinary actions (training, time off, termination, etc.). A report of the disciplinary action must be provided to the ACCESS Section.

E. ACCESS has the authority to apply further sanctions including decertifying a person for reasons of misuse or arrest record findings. Decertification may be considered for a specific time period or indefinitely. The ACCESS Section Manager, in consultation with the WSP Criminal Records Division Administrator, will determine if a misuse warrants further sanctions to the person or agency.

Procedure #:	01.06.000	**Effective Date:**	June 1, 2012
Supersedes:	ACCESS Manual, TAC Guide, Ready Reference Guide, WACIC Manual	**See Also:**	
Applies To:	All ACCESS Users	**CALEA:**	

I. TERMINAL AGENCY COORDINATOR (TAC)

A. All terminal agencies that use the ACCESS system must designate a point of contact within their agency who will serve as a liaison for matters relating to CJIS/ACCESS information. This person is referred to as the TAC.

II. TAC REQUIREMENTS

A. The TAC can be named the TAC for the agency they work for plus one or two of the following entities that have a connection to ACCESS:

1. Like Agency that has multiple ORI's – example DSHS Fraud Accountability has a terminal in Pierce County and one in Moses Lake
2. City Attorney
3. Probation
4. Pre-Trial
5. Task Force
6. Fire Marshal

B. The TAC must be ACCESS Level 2 certified and maintain the certification.

C. All assistant TAC's must be ACCESS Level 2 certified and maintain the certification.

D. The TAC must attend one New TAC training session within six months of assignment and TAC Review every three years thereafter.

F. Must maintain an agency issued email address.

G. A Memo 550 must be completed whenever there is a TAC, agency head, or technical point of contact change; address change; telephone number change; etc.

III. TAC RESPONSIBILITIES

A. The TAC is required to ensure the monthly NCIC validations are completed, if applicable.

B. The TAC acts as the point of contact for ACCESS/NCIC/WACIC matters.

C. The TAC must be available for the audit.

1. ACCESS Auditors will contact the TAC during the triennial audit process.

D. The TAC is required to be aware of the required contracts and agreements with ACCESS, NCIC, and other criminal justice agencies, if applicable.

F. TACs are required to advise the ACCESS Section of any changes in personnel who use ACCESS terminals (retirements, resignations, transfers, or name changes). If there is a name change, a Correction Notice should be sent to ACCESS@wsp.wa.gov. A copy of the Correction Notice can be found on the ACCESS webpage.

G. The TAC must advise the ACCESS Section immediately of any alleged ACCESS misuse. For more information, refer to the ACCESS Misuse Section of this chapter.

H. The TAC must maintain current records of Security Awareness Training for all personnel who have access to CJI.

I. Periodic self-audits of all records entered into NCIC/WACIC and on the agency criminal history log are recommended. Self-audits must be requested by the TAC through the ACCESS Section.

J. The TAC must review and update required written procedures.

K. The TAC is required to conduct a background re-investigation every five years for all personnel who use or work on the connection to ACCESS. For more information, refer to the System Security Section of this chapter.

L. Those agencies that provide ACCESS services through regional computer systems to outside agencies must ensure dissemination of administrative messages. The TAC must disseminate all administrative messages received on the 24-hour printer to all outside agencies.

M. The TAC must respond to requests for information by the FBI NCIC or ACCESS in the form of questionnaires, surveys, or other methods.

N. The TAC should refer to and provide personnel with the most updated copies of all manuals. They are accessible via the ACCESS webpage:

http://wsp.wa.gov/access/manuals

O. The TAC must advise the ACCESS Section of all personnel who use a terminal with access to ACCESS/NCIC/WACIC files.

1. The following information on new users must be provided to the ACCESS Section:

a. User name
b. User SID
c. Agency ORI
d. Certification level

P. The TAC must maintain a rebackground list of all IT personnel that are not ACCESS certified.

1. The list must include:

   a. Employee's full name
   b. State Identification Number (SID)
   c. Rebackground investigation date

2. The TAC may delegate or share certification responsibilities by assigning an assistant TAC in nexTEST.

R. The TAC or the assistant TAC must ensure personnel are certified at the proper level and recertify prior to the users expiration date.

Procedure #:	01.07.000	**Effective Date:**	June 1, 2012
Supersedes:	ACCESS Manual, TAC Guide, Ready Reference Guide, WACIC Manual	**See Also:**	
Applies To:	All ACCESS Users	**CALEA:**	

I. CERTIFICATION REQUIREMENTS

A. Below is a list of requirements related to the training and use of ACCESS. These requirements have been established by the FBI as a minimum for terminal operators and personnel who have access to CJI and are subject to audit.

1. Security awareness training shall be required prior to employment or assignment and annually thereafter. This training is required as soon as possible for all users who have unescorted access to CJI and/or to a physically secure location. This includes IT personnel who have direct responsibility to configure and maintain computer systems and networks with direct access to CJI to ensure compliance with state and FBI CJIS policy and regulations.
2. Within six months of completing security awareness training, become ACCESS certified.
    a. If ACCESS certification was obtained from prior employment, that certification can be transferred to the new agency the user works for now.
3. Provide all sworn law enforcement personnel and other practitioners with continuing access to information concerning NCIC/state systems using methods such as roll call and in-service training.
4. Make available appropriate training on WACIC and NCIC system use for criminal justice practitioners other than sworn personnel.
5. The CSA will annually review all curricula for relevancy and effectiveness.

II. ACCESS TRAINING

A. The FBI and WSP require all criminal justice personnel who use data from NCIC, WACIC, III, WASIS, etc. to receive training on available information and system security. The FBI and WSP also require reaffirmation of that

training every year. The WSP complies with FBI standards by offering two certification levels for users:

1. Level 1 — Inquiry, locates, and administrative messages
2. Level 2 — Includes all abilities of Level 1 and includes entry, clearing, canceling of records within the databases

B. ACCESS complies with FBI standards for reaffirmation by offering an online self-paced review and test annually available through nexTEST.

C. All employees must recertify annually. There are no grace periods to complete the recertification. If an employee fails to recertify by their expiration date, or fails their recertification test, they must recertify as soon as possible within nexTEST.

1. Once an employee fails their certification or expires, they are prohibited from using the system until they recertify.

III. SECURITY AWARENESS TRAINING

A. Security awareness training is required as soon as possible for all users who have unescorted access to CJI and/or to a physically secure location

1. ACCESS certified users must complete security awareness training through nexTEST prior to becoming ACCESS certified.
2. Non-ACCESS certified users must complete security awareness training through CJIS Online. This includes agency employees, custodial staff, IT staff, contractors, etc. Records of individuals required to view the training via CJIS Online must be kept at the agency for review during the audit.

Procedure #:	01.08.000	**Effective Date:**	June 1, 2012
Supersedes:	ACCESS Manual, TAC Guide, Ready Reference Guide, WACIC Manual	**See Also:**	
Applies To:	All ACCESS Users	**CALEA:**	

I. MAINTAINING SYSTEM INTEGRITY

A. Agencies are responsible for the entry and maintenance of accurate, timely, and complete records. However, the CSA assumes administrative responsibility, and possible legal liability, for the maintenance of the criminal justice information system.

B. The CSA must institute appropriate and reasonable quality assurance procedures for all state system users. Criminal justice agencies specifically have a duty to maintain records that are accurate, complete, and up to date. To ensure reasonably sufficient record management, for electronic and/or hardcopy case management systems, each CSA ensures there are security standards, audit standards, and personnel training standards that allow accurate and current records and proper/secure dissemination of the same.

C. These standards have been established and approved by the CJIS Advisory Policy Board and are followed by the WSP in its role as the state CSA with regard to security, auditing, and training.

II. RECORD ACCURACY

A. All NCIC/WACIC/NICS entries must be double checked by someone other than the person entering the record (second party checks) against the WACIC and NCIC hit. All second party checks must be documented with the date and initials of the person conducting the check. The checks must be done within seven days of the initial entry. Agencies lacking staff support for this verification should require the case officer to check the accuracy of the record, as the case officer carries the primary responsibility.

III. TIMELINESS

A. Users must enter records in a timely manner. Promptness in modifying, locating, or clearing records in these systems will help to keep the systems free of outdated information.

B. To ensure maximum system effectiveness, NCIC/WACIC records must be entered immediately when the conditions for entry are met, 72 hours, upon receipt (electronic or hard copy format) by the entering agency. The only

exceptions to immediate entry are when otherwise prescribed by federal law or when documentation exists to support delayed entry.

C. Records must be immediately cleared out of NCIC/WACIC upon notification that the property has been recovered or a person has been found or placed into custody.

IV. COMPLETENESS

A. Complete records include all information that was available about the person or property at the time of entry. Validation should include a review of whether additional information is missing from the original entry and could be added to the record.

B. Complete inquiries on persons include numbers (i.e. social security number, passport, vehicle identification number, license plate, driver's license, etc.) that could be indexed in the record. Inquiries should be made on all names/aliases used by the suspect. Complete vehicle queries include vehicle identification numbers and license plate numbers.

1. The following sources are recommended to be used when gathering information on a subject:

   a. Department of Licensing
   b. Department of Corrections
   c. WASIS
   d.III
   e. Court systems such as Judicial Information System (JIS), Superior Court Management Information System (SCOMIS), or Judicial Access Browser System (JABS)
   f. Agency maintained systems, such as a records management system
   g. Agency case files, such as a missing person report

C. Packing the record means including all known identifying information related to the subject in an entry. All known aliases; scars, marks, and tattoos; social security numbers; vehicle information, etc. should be included in the record to assist in proper identification of the subject.

1. All known aliases on a subject should be entered. This includes all aliases found while gathering information from the sources listed above.

2. Particular attention should be paid to discrepancies in height, age, etc. when gathering information to pack the record. When uncertain if the information pertains to the subject of the record being entered, do not include the additional information in the record and maintain documentation in the case file.

V. QUALITY CONTROL

A. FBI CJIS and WSP personnel periodically check records entered in the NCIC system for accuracy. Errors discovered in records are classified as serious errors or non-serious errors. This classification determines the type of action that is taken by FBI CJIS and WSP. Even though periodic

checks are conducted, the ORI is responsible for the accuracy, completeness, and current status of its records entered in NCIC/WACIC.

VI. VALIDATIONS

A. NCIC records are subject to validation. Validation obliges the originating agency to confirm records (vehicle, boat, wanted persons, protection orders, articles, missing persons, parts, gun entries, etc.) are complete, accurate, and still outstanding or active.

B. WSP must certify to NCIC that records subject to validation have been properly validated. Each agency must first certify to the WSP as the CSA that their records have been validated. Validation certification requires:

1. Each month, NCIC produces a file and sends it to the CSA. The CSA, in turn, emails each agency notifying that the records are available for validation.

2. On a monthly basis, the NCIC system extracts active records on file for validation purposes. The validation includes a portion of each file and includes those records 60-90 days old. In addition, it includes any person records (Wanted, Protection Order, Gang, Missing, Unidentified, Violent Person, Supervised Person, and Identity Theft Files) 14-15 months old, 26-27 months old, 38-39 months old, etc. The validation schedule is as follows:

Validation Month	Entries Made In
January	October
February	November
March	December
April	January
May	February
June	March
July	April
August	May
September	June
October	July
November	August
December	September

3. These records are included in the validation listing:

a. Article
b. Wanted/Gang/Terrorist Member
c. Missing/Unidentified
d. Violent Person
e. Vehicle/License Plate/Part/Boat
f. Gun
g. Securities
h. Protection Order
i. Supervised Person
j. Identity Theft

C. National Sex Offender Registry (NSOR) records are selected for validation under an alternative procedure. NSOR records that have been validated within the last 11 months, based on the Date of Last Validation (VLD) Field, will not be selected for validation. This provides a mechanism by which jurisdictions can perform record validation as part of the verification process. When an entering agency updates the Name of Validator (VLN) Field, the record will not be selected by NCIC for validation for at least another year. Records that have not been validated within the last 11 months would represent noncompliant, out of state, incarcerated, and deceased offenders. This allows the jurisdiction to validate its NSOR records on its schedule, and not the NCIC System's schedule.

1. For validation purposes, the appropriate source of the information in the NSOR record is considered the jurisdiction's registry.

D. NCIC chooses the records by date of entry, Eastern Standard Time (EST). Agencies located in a different time zone must realize that the validation will include records entered after midnight EST on the first of the month through midnight on the last day of the month.

E. There are two files within WACIC that are subject to yearly validations.

1. Monitored Population Registration (MPR) File

a. MPR records will be validated once per year in July. Records not validated within 60 days from the date they are placed in the FTP folders will be purged.

2. Person of Interest File

a. Person of Interest records will be validated once per year in January. Records not validated within 60 days from the date they are placed in the FTP folders will be purged. The Continuum of Care records and the Denied Firearms Applicant will not be subject to validation.

VII. REQUIREMENTS FOR MONTHLY VALIDATIONS

A. The TAC or designee(s) must review all records on the validation list found within CJIS Validations.

B. CJIS Validations will send both an AM message to the main device ID and an email notification to the TAC when validations are ready for the month.

1. The TAC or their designee needs to log on to CJIS Validations to process the records: https://cjisvalidations.wsp.wa.gov/validations/

a. User Name and password are the same as Omnixx and/or nexTEST
b. For login issues, contact ITDHelp@wsp.wa.gov or (360) 705-5999
c. There is a CJIS Validations user guide available on the ACCESS webpage for common issues and questions.

C. The TAC or their designee click on “reports” and utilize the various methods for validations

D. The TAC or their designee must go back the next day after validations are completed for the month, run the “summary report” and see if any records are stuck in “Pending ACK” status. If they are, the record must be reviewed and either modified and resubmitted or 'confirmed' for removal from the validation list before your validations are finished

1. Validations are not done until the summary report shows 100% in the “validated” column
2. For step by step instructions for handling “Pending ACK” please refer to the CJIS Validations User Guide.
3. For records that you cannot determine why they failed to validate, email access@wsp.wa.gov

E. The TAC or designee(s) must remove all invalid or inaccurate records from NCIC/WACIC.

F. The information contained in each entry must be accurate and complete. Any errors must be corrected immediately.

G. Validation efforts must be well documented. Validation efforts include what was done to complete the validation of the individual record. Documentation of phone calls, emails, letters, dates and dispositions need to be included with each record that was validated. Many agencies document this information in the case file.

1. For each record validation, your agency must document the following:
   a. Who conducted the validation
   b. The date the validation was completed
   c. Who was contacted to validate the record
   d. How the record was validated (phone, letter, email, etc.), and
   e. If the record is still valid
2. If an agency is having trouble contacting a reporting party to validate a record, it is up to the agency to determine to leave the record in the system or have it removed. This decision must be well documented.
   a. It is recommended that all missing persons and stolen guns be kept in the system. If an agency is having trouble validating these records, the agency head should determine whether or not to leave them in the system. A note must be made in the case file indicating the decision that was made.
3. Documentation of validation efforts must be available during the ACCESS audit.

H. Failure to validate records on may result in purging of those records.

I. Repeated failure to validate records may result in purging of all agency entries.

J. Retention on all validations is the current year plus one year.

VIII. PROCESS FOR COMPLETING VALIDATIONS

A. Warrants and Protection Orders

1. For the first 60-90 day validation of the record you must do the following:

   a. Pull the original warrant or protection order and check all relative information or source documents regarding accuracy of the entry.
   b. Send the warrant or protection order back to the court or prosecutor for verification of validity and any changes in extradition or expiration. Agencies may also use court systems such as Judicial Information System (JIS), Superior Court Management Information System (SCOMIS), and Judicial Access Browser System (JABS) to validate entries.
   c. It is recommended that a cover sheet be created for the validations of warrants and protection orders. This cover sheet can be used each month and attached to the validation paperwork sent by ACCESS. Example cover sheets can be found on the ACCESS webpage or by contacting the ACCESS Section.

2. For each subsequent validation of the record you must verify the validity of the record only.

B. All Other Hot Files

1. For the first 60-90 day validation of the record you must do the following:

   a. Pull the original case report and check all relative information or source documents regarding accuracy of the entry.
   b. The reporting party, victim or investigating officer must be contacted to verify validity and accuracy. Contact may be made by telephone, letter, email, or personal visit and must be documented.
   c. If the agency is unable to contact the reporting party, the department must use its best judgment whether to cancel the record or retain it in the system. This decision must be documented.

2. For each subsequent validation of Gang, Missing, Unidentified, Violent Person, Supervised Person, Sex Offender, and Identity Theft Files, you must verify the validity of the record only.

3. No subsequent validation on property records (Boat, Gun, License Plates, Securities, Vehicle and Vehicle/Boat Parts) will be required as they will not show up on the validation list after the first 60-90 day validation.

IX. TEST RECORDS

A. A list of available test records is available on the ACCESS webpage under "Test Records":
http://wsp.wa.gov/access

B. Agencies may enter test records into NCIC and WACIC for training purposes. Test records must have "TEST" as the first four characters of the Originating Agency Case Number (OCA) field and "TEST ENTRY" in the Miscellaneous (MIS) field. ACCESS recommends only fictitious names, license numbers, and other identifiers be used to prevent any confusion if another agency receives a hit on a test record.

C. Test records must be removed (cancelled) from NCIC/WACIC immediately.

X. SELF AUDITS

A. ACCESS encourages agencies to perform self-audits on their records in order to verify the information that is entered or inquired on in WACIC and NCIC is accurate.

B. WACIC Self Audit Record Requests

1. You can request the following WACIC files/entries:

a. License plates
b. Monitored population
c. Pawned articles and guns
d. Person of interest
e. Protection orders
f. Vehicles
g. Wanted persons

C. NCIC Self Audit Record Requests

1. You can request the following NCIC files/entries:

a. Articles
b. Boats
c. Gangs
d. Guns
e. Identity theft
f. License plates
g. Missing persons
h. Protection orders
i. Protective interest
j. Securities
k. Unidentified persons
l. Vehicles
m. Vehicle/boat parts
n. Violent persons
o. Wanted persons

D. Criminal history logs must be requested for a particular time frame (ex: the month of February or March 15-23, and the year).

E. E-mail the ACCESS Section to request a copy of your records and/or criminal history logs at ACCESS@wsp.wa.gov.

1. Include the following information in your e-mail:

a. Requestor’s name

b. ORI
c. Type of file you want (warrants, missing persons, etc.)
    (1) All records provided, unless otherwise listed in the request, will be from WACIC only. Agencies must ask for NCIC records specifically within their request.
    (2) Requests for “all records on file” will include all records except for license plate. In order to obtain license plate records, agencies must ask for them specifically within their request.

F. Once you have received a copy of your records, check them against your agency case files and court documents.

Procedure #:	01.09.000	**Effective Date:**	June 1, 2012
Supersedes:	ACCESS Manual, TAC Guide, Ready Reference Guide, WACIC Manual	**See Also:**	
Applies To:	All ACCESS Users	**CALEA:**	

I. AUDIT STANDARDS

A. The ACCESS and technical security triennial audits conform to FBI and state standards.

1. To ensure the integrity of the ACCESS System, certain policies and standards must be completed, adopted, and followed. Audit compliance includes, but is not limited to, NCIC, NICS, WACIC, III, WASIS and N-DEx.

2. All standards set forth in the technical audit questionnaire originate from the CJIS Security Policy which provides CJAs/NCJAs with a minimum set of security requirements for access to FBI CJIS Division systems and information to protect and safeguard CJI. This minimum standard of security requirements ensures continuity of information protection.

B. Audits focus on two areas:

1. Agency compliance

2. Recommendations to lessen agency liability

C. The triennial audit calendar is located on the ACCESS webpage. The audit schedule is subject to change without advance notice.

http://www.wsp.wa.gov/access/resources

II. ACCESS AUDIT

A. ACCESS Business Audit Process

1. Approximately two months prior to the agency audit, the ACCESS Auditor will send a notification of the upcoming audit to the TAC and agency head.

2. Approximately one month prior to the agency audit, the ACCESS Auditors will ask the agency to submit procedures, user acknowledgment, statutory authority, if NCJA, NICS questionnaire (if applicable) and the agency's abbreviations list, if applicable.

3. Approximately one week prior to the audit the auditor will contact the TAC to confirm the time of the audit, provide any corrections to

be made to the procedures given and advise which missing person case files will be reviewed (if applicable).

4. The ACCESS audit is conducted with the TAC for each agency.
    a. If a TAC has not been assigned, then the agency head will be contacted to complete the audit.
5. Auditors will review the following, if applicable:
    a. System Administration
    b. System Integrity
    c. Hit Confirmation
    d. Record Integrity
        (1) 1 % of active Protection Orders, Wanted Persons, and Missing Persons records, up to 20 records
        (2) 1 % of Criminal History Record Identification (CHRI) inquiries
            • Subject to auditor discretion.
    e. Criminal History
    f. National Instant Background Check System (NICS)
    g. National Data Exchange (N-DEx)
    h. Written Procedures
    i. Validations
6. Auditors will conduct site security visits to ensure terminal locations and physical CJI is secure. The following areas will be reviewed during the site security visits:
    a. Who has access, including unescorted access, to the site
    b. Who performs the cleaning/facilities maintenance at the site
    c. Method of disposal for CJI media
    d. Review what terminals are located at each site
7. Upon completion of the audit, the auditor will complete an exit interview with the TAC and the agency head, if available. The auditor will provide the final compliance report at this time.
8. Agencies must respond to the numbered compliance discrepancies in writing within the assigned due date which is at least 30 days from the date the audit was conducted, either the 1st or 15th of the next month.
9. Once the auditor receives the agency's response through CJIS Audit, the auditor will review all findings to ensure all compliance issues have been addressed.
    a. If the due date lapses and the agency has not responded to the original report, the auditor will contact the agency to check on the status of the response. The ACCESS Section Manager and/or Information Security Officer (ISO) will be advised.
    b. If the agency still has not responded, the auditors will turn the audit file over to the ACCESS Section Manager and/or the ISO. The Section Manager or ISO will work with the

Criminal Records Division (CRD) Administrator to reach the agency and complete the audit process.

c. Follow up audits may be conducted depending on findings. This will be at the discretion of the WSP whether it is a telephone conference or an additional on-site sanction audit.

B. ACCESS Audit Non-Compliance

1. Failure to comply with established policies and procedures may be cause for sanctions. Sanctions will be determined by the ACCESS Auditor, ACCESS Section Manager, and the CRD Division Administrator. Possible sanctions may include, but are not limited to:

a. A formal letter to agency head
b. Purging of records
c. Decertification of an employee
d. Discontinuance of service

C. ACCESS Audit Recommendations

1. Although the following procedures are not required, ACCESS recommends them to lessen agency liability:

a. Maintain documentation in the case file of information gained from other sources.
b. Clear all entries using a WAC or NIC number.
c. Inquire again after removing a record from NCIC.
d. Agencies are encouraged to validate records entered only in WACIC. A list of records entered into the system can be obtained by contacting the ACCESS Section.

D. Agencies will receive a certificate of completion indicating that the audit has been completed once all compliance issues have been addressed.

E. ACCESS Audit Questions

1. For questions or concerns related to the ACCESS audit, contact the ACCESS Auditors at (360) 534-2010.

III. TECHNICAL SECURITY AUDIT

A. The technical security audit is conducted remotely via Teams to review the submitted questionnaire and correspondence received through email prior to the scheduled audit.

B. Technical Security Audit Process

1. The auditor will send notification of the upcoming audit via email to the Information Technology (IT) point of contact, TAC and the agency head two months prior to the audit that contains instructions for accessing CJIS Audit, how to complete the audit questionnaire and the scheduled date and time of the audit. The audit questionnaire must be completed prior to the scheduled date.

2. The auditor will contact the agency IT point of contact as reported by each agency for all technical security audit related questions.

a. If an IT point of contact has not been assigned, then the TAC will be contacted to complete the audit.
b. If the IT point of contact changes a Memo 550 must be sent in to ACCESS@wsp.wa.gov so that we can update our records

3. The auditor will review the following, if applicable:

a. Personnel security
b. Security incidents
c. Configuration management
d. Media protection
e. Physical protection
f. Session lock
g. System and communications protection and information integrity
h. Boundary protection
i. Malicious code
j. Event logging
k. System use notification
l. Patch management
m. Identification and authentication
n. Access control – wireless
o. Handheld mobile devices
p. Cloud computing
q. Services

4. Upon completion of the audit, the auditors will provide the agency with a final compliance report and recommendations.

5. The auditor provides a date the agency must respond regarding any needed changes.

a. Agencies must respond to the compliance discrepancies within 30 days of the final summary report.
b. If the original 30 days lapses and the agency has not responded to the original report, the auditor will call the agency to check on the status of the response.
c. If the agency still has not responded, the auditor will turn the audit file over to the ACCESS Section Manager and/or the ISO. The Section Manager or ISO will work with the Criminal Records Division (CRD) Administrator to reach the agency and complete the audit process.
d. Follow up audits may be conducted depending on findings.

C. Technical Security Audit Non-Compliance

1. Failure to comply with established policies and procedures may be cause for sanctions. Sanctions will be determined by the auditor, ISO, ACCESS Section Manager, and the CRD Division Administrator. Possible sanctions may include, but are not limited to:

a. A formal letter to agency head
b. Discontinuance of service

D. Agencies will receive a certificate indicating that the audit has been completed once all compliance issues have been addressed.

E. Technical Security Audit Questions

1. For questions or concerns related to the technical security audit, contact one of your technical auditors at access@wsp.wa.gov or (360) 534-2010.

Procedure #:	01.10.000	**Effective Date:**	June 1, 2012
Supersedes:	ACCESS Manual, TAC Guide, Ready Reference Guide, WACIC Manual	**See Also:**	
Applies To:	All ACCESS Users	**CALEA:**	

I. AGREEMENTS AND ACKNOWLEDGMENTS

A. The ACCESS User Acknowledgment encompasses several agreements into one based on agency needs. All applicable acknowledgments and agreements must be signed by the current administrator (chief, sheriff, etc.). They must be updated when there is a change in administration. If there is a change a copy of the new acknowledgment must be provided to the ACCESS Section.

B. All agencies that use ACCESS to obtain NCIC/WACIC data must retain the following current, signed agreements:

1. ACCESS User Acknowledgment

   a. This acknowledgment is an agreement with ACCESS/NCIC/WACIC regarding the proper use and dissemination of CJI. The agreement must be signed by the agency head (chief, sheriff, etc.).
   b. The **24x7 Hit Confirmation, Attachment A,** must be completed if an agency provides 24x7 teletype printer coverage for another agency or receives messages 24x7 on behalf of another agency.
   c. The **Holder of the Record Agreement, Attachment B,** must be completed if an agency uses its ORI to enter another agency's records or has their records entered under another agency's ORI number.
   d. The **Inter-Agency Agreement, Attachment C,** must be completed if an agency provides criminal justice services to another agency or if an agency receives criminal justice services from another agency.
   e. The **Management Control Agreement, Attachment D.1,** must be completed if an agency has a city or county Information Technology (IT) department handling IT services for the criminal justice agency.
   f. The **Management Control Agreement for Personnel Determinations, Attachment D.2,** Must be completed between a combined 911/dispatch center (ORI ends in "N") with at least one of the criminal justice agencies (CJA) to which they provide service.

g. The **Information Exchange Agreement, Attachment E**, must be completed if an agency provides CJI to contracted prosecutors.

h. The **Addendum for Criminal Justice Agency (CJA) using a Non-Criminal Justice (NCJA) ORI, Attachment F,** must be completed by agencies who have been issued an NCJA ORI to conduct fingerprint submissions for licensing, non-criminal justice employment, CASA/GAL and/or purpose code X/emergency placement of children.

II. PRIVATE CONTRACTOR USER AGREEMENTS

A. Private contractors are permitted access to CJI pursuant to an agreement which specifically identifies the contractor's purpose and scope of services.

B. Private contractors must complete a Washington State fingerprint-based background check and meet the same criteria as criminal justice employees.

C. Private contractors must review the security awareness training once annually.

D. Private contractors must sign a CJIS Security Addendum. This may be found on the ACCESS webpage or in the CJIS Security Policy.

III. REFERENCE

A. Refer to the ACCESS webpage for acknowledgments and agreements:

http://wsp.wa.gov/access/forms

Procedure #:	01.11.000	**Effective Date:**	June 1, 2012
Supersedes:	ACCESS Manual, TAC Guide, Ready Reference Guide, WACIC Manual	**See Also:**	
Applies To:	All ACCESS Users	**CALEA:**	

I. POLICIES AND PROCEDURES REQUIREMENTS

A. Formal written procedures assist agencies in proper practices and understanding. Agencies must have written procedures on file. The ACCESS Auditors will limit their verification to ensuring the procedures comply with state and federal policy.

B. The ACCESS Section has templates available on the ACCESS webpage for criminal history use and dissemination, media disposal, ACCESS misuse, physical protection, rebackground investigations, validations, data breach reporting, hit confirmation and NICS appeal.

http://wsp.wa.gov/access/forms

1. If used, templates must be modified to reflect agency policies.

C. All written procedures must contain the following:

1. Date the procedures were completed
2. The agency name or letterhead indicated in/on the procedure
3. Details of how a task must be completed

D. ACCESS recommends that all written procedures be reviewed yearly by the agency.

II. REQUIREMENTS FOR THE ACCESS AUDIT

A. ACCESS requires written procedures for the following:

1. Validations
2. Hit confirmation
3. Criminal history use and dissemination
4. Rebackground investigations
5. ACCESS misuse
6. Media disposal
7. Physical protection
8. Fingerprinting

process

9. Entry work for all records entered into NCIC/WACIC, such as:

   a. Articles
   b. Boats
   c. Gangs
   d. Guns
   e. Identity theft
   f. License plates
   g. Missing persons
   h. Monitored population registration
   i. NICS
   j. Person of interest
   k. Protection orders
   l. Securities
   m. Supervised persons
   n. Unidentified persons
   o. Vehicles
   p. Vehicle/boat parts
   q. Violent persons
   r. Wanted persons

III. REQUIREMENTS FOR THE TECHNICAL SECURITY AUDIT

A. ACCESS requires written procedures for the following:

1. Password management
2. Media disposal
3. Data breach reporting

Procedure #:	01.12.000	**Effective Date:**	June 1, 2012
Supersedes:	ACCESS Manual, TAC Guide, Ready Reference Guide, WACIC Manual	**See Also:**	
Applies To:	All ACCESS Users	**CALEA:**	

I. 24 HOUR REQUIREMENTS

A. To facilitate compliance with hit confirmation requirements, the originating agency must be available 24 hours a day to confirm record entries. Originating agencies must place a 24x7 hit confirmation phone number in the Miscellaneous (MIS) Field of all entries.

1. If an entering agency is not available 24 hours, then they must contract for hit confirmation services with another 24 hour agency and sign a 24x7 Hit Confirmation Agreement. This includes the requirement to monitor the teletype printer 24 hours a day.

2. Non-terminal agencies must sign a Holder of the Record Agreement if the holder uses their own ORI.

B. Any agency that enters a record into NCIC/WACIC has the duty to promptly respond with the necessary confirmation of the hit and other details. They must furnish a response within a specific time period. Valid hit confirmation is based on two levels of priority: urgent or routine.

1. Priority 1: Urgent.

   The hit must be confirmed within ten 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, priority 1 should be specified.

2. Priority 2: Routine.

   The hit must be confirmed 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.

C. The response will confirm the information contained in the record or set a specific time when further information will become available. When a specific time is stated, this time will not be later than 0900 local time the next normal work day.

1. If the agency requesting confirmation does not receive a substantive response within the designated timeframe, the agency should generate a second request with a copy to the WSP Customer Service Group.

2. If the agency still fails to receive a response, the agency should then notify the NCIC Quality Control staff by a third message with a copy to the WSP Customer Service Group. Failure on the part of any agency to ensure such compliance will be brought to the attention of the Advisory Policy Board with the FBI.

II. CONFIRMING A HIT

A. A WACIC or NCIC hit alone is not probable cause to arrest a subject, but indicates a stolen property report, missing person report, or warrant, etc., may have been filed.

B. An inquiring agency must contact the originating agency of the hit for confirmation of data. To confirm a hit means to contact the agency that entered the record to:

1. Ensure that the person or property inquired upon is identical to the person or property identified in the record.

2. Ensure that the warrant, missing person report, protection order, or theft report is still outstanding.

3. Obtain a decision regarding:

   a. The extradition of a wanted person when applicable.
   b. The return of the missing person to the appropriate authorities.
   c. The return of stolen property to its rightful owner.
   d. The terms and conditions of a protection order.

4. The source documents used for hit confirmation may be electronic if the agency has implemented the proper controls for electronic documents supporting WACIC and/or NCIC records.

C. A confirmed hit can be adequate grounds to arrest the wanted person, detain the missing person, seize the stolen property, or charge the subject with violating a protection order, etc.

D. When an agency receives a record(s) in response to an inquiry and no enforcement action is contemplated or possible because of extenuating circumstances, the hit should not be confirmed and the record ***must not*** be located. If, for example, local jails are unable to house misdemeanor prisoners because of overcrowding hit confirmation is not necessary.

III. OUT OF STATE HIT CONFIRMATION

A. Agencies should use Nlets for hit confirmation of out of state records. Nlets should be used for documentation, even if the initial confirmation is handled by a telephone call/fax.

B. Nlets cannot be used for hit confirmations between two agencies within the state of Washington. While the same information and time constraints apply, a normal terminal message should be sent via ACCESS.

IV. NLETS HIT CONFIRMATION REQUESTS (YQ)

Field Name	Required?	Message Field Code	Field Length	Data
Header	Mandatory	HDR	10-62	Alphabetic, numeric, special characters. Example: T.XXXXX,NLTAP;YQ.your ORI. Destination ORI. The XXXXX in the header is for the destination mnemonic code.
Request type	Mandatory	RTY	2-2	Alphabetic. SV – Stolen Felony Vehicle WP – Wanted Person PO – Protection Order MP – Missing Person SL – Stolen License Plate SG – Stolen Gun SA – Stolen Article SS – Stolen Security SB – Stolen Boat SP – Stolen Part
Request Number	Mandatory	RNO	1-1	Numeric. Must be 1, 2, or 3.
Priority Destination	Mandatory	PRI	1-1	Alphabetic. Must be U (urgent) or R (routine).
Originating Agency Case Number	Mandatory	OCA	1-20	Alphabetic, numeric, special characters
NCIC Number	Mandatory	NIC	10-10	Alphabetic, numeric. When sending a YQ to Canada, fill in the NIC Field with “NONE.”
AND ONE OF THE SETS OF DATA ELEMENTS BELOW:				
Stolen License Plate Set				
License Plate Number	Conditional	LIC	10-10	Alphabetic, numeric
License State	Conditional	LIS	2-2	Alphabetic. Only valid on request type SL.
License Year of Expiration	Optional	LIY	1-4	Numeric. Only valid on request type SL.
License Type	Optional	LIT	2-1	Alphabetic. Only valid on request type SL.
Stolen Vehicle Set				
License Plate Number	Conditional	LIC	10-10	Alphabetic, numeric

Vehicle Identification Number	Conditional	VIN	1-20	Alphabetic, numeric
Vehicle Year	Conditional	VYR	2-4	Numeric
Vehicle Make	Conditional	VMA	2-4	Alphabetic
Wanted Person, Missing Person or Protection Order Set				
Name	Conditional	NAM	1-30	Alphabetic, special characters. Last name, First name middle.
Date of Birth	Conditional	DOB	6-8	Numeric. MMDDYY or CCYYMMDD
Sex	Conditional	SEX	1-1	Alphabetic. Male (M) or Female (F).
Warrant Number	Conditional	WNO	1-20	Alphabetic, numeric
Court ORI	Conditional	CTI	1-9	Alphabetic, numeric
Stolen Gun Set				
Serial Number	Conditional	SER	1-20	Alphabetic, numeric
Caliber	Conditional	CAL	1-4	Numeric. Listed in Gun Data Codes, NCIC Code Manual.
Make	Conditional	MAK	1-23	Alphabetic. Listed in Gun Data Codes, NCIC Code Manual.
Model	Conditional	MOD	1-20	Alphabetic, numeric
Stolen Article Set				
Article Type	Conditional	TYP	4-7	Alphabetic
Serial Number	Conditional	SER	1-20	Alphabetic, numeric
Brand Name	Conditional	BRA	2-6	Alphabetic, numeric, special characters. Listed in Article Data Codes, NCIC Code Manual.
Stolen Security Set				
Security Type	Conditional	TYP	2-2	Alphabetic. Listed in Security Data Codes, NCIC Code Manual.
Serial Number	Conditional	SER	1-20	Alphabetic, numeric
Denomination	Conditional	DEN	1-9	Alphabetic, numeric, special characters
Stolen Boat Set				
Boat Registration Number	Conditional	REG	1-8	Alphabetic, numeric
Boat Hull Number	Conditional	BHN	1-18	Alphabetic, numeric.

Boat Make	Conditional	BMA	1-24	Alphabetic, numeric. The first four characters must be a valid NCIC code. Listed in Boat Data Codes, NCIC Code Manual. Positions five through 24 must include the manufacturer's full name.
Stolen Vehicle Part or Stolen Boat Part Set				
Stolen Part Serial Number	Conditional	SER	1-20	Alphabetic, numeric.
Brand Name	Conditional	BRA	2-4	Alphabetic, numeric. Listed in Boat Data Codes or Vehicle Date Codes, NCIC Code Manual.
Category	Conditional	CAT	2-2	Alphabetic. Listed in Boat Data Codes or Vehicle Date Codes, NCIC Code Manual.
Requesting/Recovering Agencies Information				
Requestor's Name	Mandatory	RNA	1-30	Alphabetic
Requestor's Agency	Mandatory	RAG	1-30	Alphabetic
Phone Number	Optional	PHO	10-10	Numeric
Phone Number Extension	Optional	EXT	1-4	Numeric
Fax Number	Optional	FAX	10-10	Numeric
Remarks	Optional	REM	1-500	Free text

A. Example:

T.XXXXX,NLTAP;YQ.WA0340500.CA0194200.RTY/WP.RNO/1.PRI/U.
OCA/12-1234.NIC/W123456789.NAM/SMITH, JEAN.DOB/051575.SEX/F.
RNA/SGT JIM FRANKLIN.RAG/PD LITTLEROCK.PHO/3605554321.
EXT/321.FAX/3605554323.REM/BEING DETAINED PENDING
CONFIRMATION NO LOCAL CHARGES

V. NLETS HIT CONFIRMATION RESPONSES (YR)

Field Name	Required?	Message Field Code	Field Length	Data
Header	Mandatory	HDR	10-62	Alphabetic, numeric, special characters. Example: T.XXXXX,NLTAP;YR.your ORI. Destination ORI. The XXXXX in the header is for the destination mnemonic code.

Request type	Mandatory	RTY	2-2	Alphabetic. SV – Stolen Felony Vehicle WP – Wanted Person PO – Protection Order MP – Missing Person SL – Stolen License Plate SG – Stolen Gun SA – Stolen Article SS – Stolen Security SB – Stolen Boat SP – Stolen Part
Confirmation Status	Mandatory	CON	1-1	Alphabetic. Y – Yes confirmed N – No not confirmed P – In process of being confirmed E – Valid but awaiting a decision on extradition
Hours for Confirmation	Conditional	HRS	1-3	Numeric. Hours to complete confirmation of record. Required if CON is P or E
Originating Agency Case Number	Mandatory	OCA	1-20	Alphabetic, numeric, special characters
NCIC Number	Mandatory	NIC	10-10	Alphabetic, numeric. When sending a YQ to Canada, fill in the NIC Field with “NONE.”
AND ONE OF THE SETS OF DATA ELEMENTS BELOW:				
Stolen License Plate Set				
License Plate Number	Conditional	LIC	10-10	Alphabetic, numeric
License State	Conditional	LIS	2-2	Alphabetic. Only valid on request type SL.
License Year of Expiration	Optional	LIY	1-4	Numeric. Only valid on request type SL.
License Type	Optional	LIT	2-1	Alphabetic. Only valid on request type SL.
Stolen Vehicle Set				
License Plate Number	Conditional	LIC	10-10	Alphabetic, numeric
Vehicle Identification Number	Conditional	VIN	1-20	Alphabetic, numeric
Vehicle Year	Optional	VYR	2-4	Numeric

Vehicle Make	Optional	VMA	2-4	Alphabetic
Wanted Person, Missing Person or Protection Order Set				
Name	Conditional	NAM	1-30	Alphabetic, special characters. Last name, First name middle.
Date of Birth	Conditional	DOB	6-8	Numeric. MMDDYY or CCYYMMDD
Sex	Optional	SEX	1-1	Alphabetic. Male (M) or Female (F).
Stolen Gun Set				
Serial Number	Conditional	SER	1-20	Alphabetic, numeric
Caliber	Conditional	CAL	1-4	Numeric. Listed in Gun Data Codes, NCIC Code Manual.
Make	Conditional	MAK	1-23	Alphabetic. Listed in Gun Data Codes, NCIC Code Manual.
Model	Optional	MOD	1-20	Alphabetic, numeric
Stolen Article Set				
Article Type	Conditional	TYP	4-7	Alphabetic
Serial Number	Conditional	SER	1-20	Alphabetic, numeric
Brand Name	Optional	BRA	2-6	Alphabetic, numeric, special characters. Listed in Article Data Codes, NCIC Code Manual.
Stolen Security Set				
Security Type	Conditional	TYP	2-2	Alphabetic. Listed in Security Data Codes, NCIC Code Manual.
Serial Number	Conditional	SER	1-20	Alphabetic, numeric
Denomination	Optional	DEN	1-9	Alphabetic, numeric, special characters
Stolen Boat Set				
Boat Registration Number	Conditional	REG	1-8	Alphabetic, numeric
Boat Hull Number	Conditional	BHN	1-18	Alphabetic, numeric.
Boat Make	Optional	BMA	1-24	Alphabetic, numeric. The first four characters must be a valid NCIC code. Listed in Boat Data Codes, NCIC Code Manual. Positions five through 24 must include the manufacturer's full name.

Stolen Vehicle Part or Stolen Boat Part Set				
Stolen Part Serial Number	Conditional	SER	1-20	Alphabetic, numeric.
Brand Name	Optional	BRA	2-4	Alphabetic, numeric. Listed in Boat Data Codes or Vehicle Date Codes, NCIC Code Manual.
Category	Optional	CAT	2-2	Alphabetic. Listed in Boat Data Codes or Vehicle Date Codes, NCIC Code Manual.
Requesting/Recovering Agencies Information				
Confirming Name	Mandatory	CNA	1-30	Alphabetic. Name of person confirming the record.
Confirming Agency	Mandatory	CAG	1-30	Alphabetic. Name of confirming agency.
Phone Number	Optional	PHO	10-10	Numeric. Phone number of confirming agency.
Phone Number Extension	Optional	EXT	1-4	Numeric
Fax Number	Optional	FAX	10-10	Numeric. Fax number of confirming agency.
Remarks	Optional	REM	1-500	Free text

A. Example:

T.XXXXX,NLTAP;YR.WA0340500.CA0194200.RTY/WP.CON/E.HRS/4.
OCA/06-1234.NIC/W123456789.NAM/SMITH, JENNIFER.DOB/051555.
SEX/F.CNA/SGT JIM FRIDAY.CAG/PD LITTLEROCK.PHO/3605554321.
EXT/321.FAX/3605554323.REM/WARRANT VALID DECISION TO
EXTRADITE PENDING

Procedure #:	01.13.000	**Effective Date:**	June 1, 2012
Supersedes:	ACCESS Manual, TAC Guide, Ready Reference Guide, WACIC Manual	**See Also:**	
Applies To:	All ACCESS Users	**CALEA:**	

I. ADMINISTRATIVE MESSAGES

A. Administrative messages follow NCIC and Nlets guidelines, which state these types of messages are free text and are directed to individuals or agencies and not to a computer database. Administrative messages are restricted to material directly related to a criminal justice function.

B. The following types of messages are considered appropriate:

1. Messages regarding training or meetings on recognized criminal justice matters may be sent by authorized personnel.

2. Routine stolen vehicle messages if:

   a. The message contains specific information that the vehicle is in route to that state.
   b. The theft takes place near the state line and it may be assumed that the vehicle has been taken into the adjacent state.
   c. Emergency related messages like attempt to locate persons due to medical reasons and/or death.

3. Funeral announcements are permitted only in the following instances:

   a. Officers killed in line of duty
   b. Death of an officer or employee of a law enforcement agency not in line of duty
   c. Death of retired officers or employees of a law enforcement agency

C. The following messages do not pertain to the administration of criminal justice and ***would not*** be acceptable as an administrative message:

1. No social announcements (i.e., holiday messages or retirements).

2. No recruitment of personnel.

3. No messages supportive or in opposition to political issues or announcements of meetings relative to such issues.

4. No messages supportive or in opposition to labor management issues or announcements relative to such issues.

5. No messages supportive or in opposition of legislative bills.

6. No messages relating to requests for information concerning salary, uniforms, personnel, or related items that can be routinely obtained by correspondence or other means.

7. No messages relating to the advertisement or sale of equipment.

D. The NCIC system automatically generates a variety of administrative messages, which are identified by the "$." Sign followed by a letter to indicate the type of message. For more information on these messages, refer to the NCIC Operating Manual.

II. LAW ENFORCEMENT OFFICER FLYING ARMED (LEOFA)

A. There are specific requirements for a Law Enforcement Officer (LEO) to be permitted to fly armed:

1. Be a LEO employed by a government agency; sworn and commissioned;

2. Be authorized by their employer to have a weapon in connection with their assigned duties;

3. Complete the training program (Flying While Armed) available from the US Transportation Security Administration (TSA):

https://www.tsa.gov/travel/law-enforcement

4. The Escorted Individual Type (EIT) is a mandatory field that ensures the operational need for armed travel, from check-in to deplaning, and has been met under title 49 Code of Federal Regulation (CFR) § 1544.219 carriage of accessible weapons, consistent with one of the following:

a. PROTECTIVE DETAIL: The officer must be assigned to a protective duty or on travel required to be prepared to engage in a protective function.
b. SURVEILLANCE: Hazardous surveillance activity, from the time the officer would otherwise check their weapon until the time the weapon would be claimed after deplaning.
c. ENFORCEMENT OR INVESTIGATION: Official police activity that requires the officer to be “armed and prepared for duty”. The armed LEO must have an operational need to have the weapon accessible on the aircraft.
d. PRISONER: The primary purpose of travel for the officer must be escorting or picking up a prisoner.

(1) Each must be typed as noted.
EXAMPLE: EIT/protective detail

B. A message must be sent for all legs of travel that would require passing the TSA.

C. Each message sent will generate a response with specific codes that the officer will need to provide to TSA each time they pass through security.

D. Prior to submitting a flying armed request, please ensure the authorizing official has determined and approved that the request meets 49 CFR 1544.219 (Carriage of accessible weapons).

E. For questions or comments regarding the LEOFA program or problems with submission of LEOFA request messages via Nlets, please contact the office of law enforcement/federal air marshal service, flight operations division, liaison section, at leofa@ole.tsa.dhs.gov or by calling 1-855-fly-leos, and follow the prompts.

III. MESSAGE FORMATS

A. To send an administrative message, enter the following:

1. ACCESS/Nlets message header. See Message Formats for more information. ACCESS/Nlets header: Furnished by the originating terminal, includes transaction code (T) and station address(es).

   a. Sender's ORI (9 character ORI is mandatory) agency identifier followed by a period.
   b. The destination ORI for the agency that is to receive the message, followed by a period. If the intended receiver of the message is a state control terminal, a 2-character ORI may be used. In all other cases the ORI(s) must be 9 characters.
   c. Control field - optional.
   d. The three characters – "TXT"

      (1) In-state message headers

         (a) Single address: T.XXXXX;MESSAGE TEXT

            1. XXXXX is the destination terminal mnemonic(s).

         (b) Multiple addresses: T.XXXXX,XXXXX,XXXXX;

            1. XXXXX is the destination terminal mnemonic(s).

      (2) Out-of-state message headers

         (a) Single address: T.NLTAP,YYYYY;AM..CA0192000.*LASO062699.

            1. If you would like a copy of the message, include your terminal mnemonic in YYYYY.
            2. The Optional Control Field (OCF), if used, is preceded by an asterisk (*) and ended with a period (.). When answering a message that contains the OCF, it **must** be included as received in the response.

(b) Multiple addresses:
T.NLTAP,YYYYY;AM.CA0194200,OR0260200

1. If you would like a copy of the message, include your terminal mnemonic in YYYYY.

(3) The terminal address for out-of-state AM messages via is “NLTAP.” This is an ACCESS system mnemonic for Nlets. DO NOT use “Nlets” as the terminal address in your out-of-state AM messages, they will be sent to an error queue and will not reach their intended destination.

2. Message reference number is the number that will be referenced in all responses or future references to this message.

3. Name of originating agency.

4. Date message was originated.

5. Name of destination agency (address).

a. APBs must be limited to the minimum area necessary to achieve the desired coverage so as not to reduce the effectiveness of this type of message. An APB directed to another state must follow the Nlets procedure for requesting a state broadcast as outlined in the Nlets Wiki/User Manual.

6. If the message is additional information, continuation, correction, reply or cancellation, the message text should reference the previous message using the date and reference number of the previous message.

7. Narrative portion of the text.

8. Last name or initials of the terminal operator or author of the message and his/her location.

9. Time is indicated by using the 24-hour clock and must include the time zone (ex: 0945PST).

10. IMG. The ability to add an image to the message.

B. Example of an administrative message:

T.XXXXX,YYYYY,ZZZZZ,NLTAP;AM..OR0260200.	1. ACCESS/Nlets Header
REFERENCE 14	2. Reference Number
SEATTLE PD	3. Originating Agency
01/01/2012	4. Date of Message
ESTES PARK PD, COLORADO	5. Destination Agency
REF NUM 147	6. Previous Reference Number
SUBJECT WEARING GRAY HAT - DARK SUIT DRIVING DK GREEN 83 BUICK SEDAN	7. Narrative

GA LIC UNKNOWN. BELIEVED ENROUTE TO ESTES PARK, CO OR GRAND LAKE, CO **SUBJECT IS DIABETIC AND WILL REQUIRE TREATMENT.** **FELONY WARRANT WILL EXTRADITE** **SEATTLE PD J SMITH** **0945PST**	8. Agency and Operator 9. Time 10. Image attached

IV. COMPUTER MESSAGES

A. Computer messages must conform to a specific format and are directed to a specific computer database. These messages originate from a user and are transmitted to the WACIC and/or NCIC systems.

1. Inquiry messages to WACIC and/or NCIC search the data for any matching records containing the search elements submitted.
2. Entry messages place a new record in NCIC/WACIC or append supplemental records to those already on file.
3. Modification messages add, delete, or change a portion of data that is part of a base record. A record may be modified only by the agency that entered the record, as long as the record is in active status. Modification messages and acknowledgments are further explained in the Modification section of each ACCESS Operations Manual file chapter.
4. Locate messages indicate (until the originating agency clears the record) the wanted person has been apprehended or the property has been located. In the Missing Person File, a locate message indicates a missing person has been found and, in the case of NCIC, retires the record from the file. Locate messages must be sent once a record has been confirmed with the entering agency. A locate message cannot be used by the agency that placed the record in WACIC or NCIC.
    a. If an agency receives a hit containing “NOEX” in the Miscellaneous (MIS) field and they are outside the specified extradition, the record ***must not*** be located.
    b. If a record is located twice, the record will automatically clear from the system.
5. Clear messages indicate the location of a apprehension of a wanted person, or recovery of property on file in WACIC or NCIC. Cleared missing person records will be removed by NCIC upon receipt of the clear message. Protection order and sexual offender records remain in an inactive status for the remainder of the year plus five additional years. During that time, the records are still accessible via QPO and QXS transactions. NCIC removes all other

records and places them in retired file status. Records may only be cleared by the originating agency.

6. Cancellation messages remove an entire record or supplemental record(s) from any file. When a record is cancelled, all supplemental records appended to it are also automatically cancelled. A record may be cancelled only by the agency that entered the record. A record should be cancelled when it is determined to be invalid (i.e. the warrant which was the basis for the record has been dismissed or the record is the result of a fictitious theft report).

B. Positive Responses to On-Line Inquiries

1. Positive responses to on-line inquiries are transmitted when records are found in WACIC or NCIC. A positive response contains a header and the ORI of the inquiring agency followed by an alert(s) and the record on file.

C. Negative Responses to On-Line Inquiries

1. Negative responses to on-line inquiries are transmitted when no record match is found in WACIC or NCIC. A negative response to an inquiry contains a header and the ORI of the inquiring agency followed by an indication that no record was found for each searchable identifier inquired upon.

V. ERROR MESSAGES

A. Error messages advise an agency of an error in a WACIC or NCIC transaction. Error messages are frequently referred to as reject messages, since the first word is always REJECT. Some error messages contain Message Field Codes (MFCs) to identify the field containing the error. A brief explanation of the error(s) follows the message. In general, error messages should be self-explanatory and should readily indicate the error that caused the message generation. If the operator is unable to determine the cause of the error message, ACCESS Customer Services Group may be called at (360) 705-5999.

B. Examples of serious errors:

1. Wanted person records that indicate a subject is wanted for questioning only.

2. Records entered for cashier's checks, bank drafts, bank officer's checks, certified checks, checks issued to card holder by credit card companies, company checks, government checks (local, state, and federal), personal checks, personal notes, promissory notes, and stolen credit cards.

3. A missing person, wanted person, license plate, or vehicle record that contains inaccurate vehicle and/or license data (verified by the state Department of Licensing).

4. Stolen property records entered with a non-unique number such as a stock number, model number, an owner-applied number in the Serial Number (SER) field, a non-unique boat hull number (BHN), or a non-unique boat registration number (REG), etc.

C. The FBI CJIS cancels records that have serious errors. They send a $.E. administrative message to the entering agency. If a record contains a non-serious error, the FBI CJIS mails a letter to the CSA. The CSA must forward a copy of the letter to the originating agency for the record for corrective action. Non-serious errors are those not included in the serious error list above.

D. Before entry of a new record into ACCESS, the system verifies a duplicate entry does not exist. If a duplicate record is found, WACIC rejects the entry request and returns the record that is already in the file. NCIC rejects entry of new records if mandatory fields match existing data i.e. SER and/or OAN. NCIC sends a message REJ ON FILE. NCIC also furnishes the possible duplicate record on file. NCIC accepts a duplicate record if the ORI or the OCA in the second entry is different. If accepted, the first entry (record on file) will be furnished.

E. The NCIC acknowledgments are forwarded to the WACIC system so the NIC number can be added to the corresponding WACIC record. This is done so that subsequent transactions involving the record (clears, cancels, modifies, etc.) can use the NIC number in the resulting NCIC transaction. In some rare instances, the WACIC system will be unable to match the NCIC acknowledgment with the proper WACIC record. Therefore, a NIC number will not be associated with the WACIC record. This can either be due to duplicate records on file with the same ORI and record identifier(s) contained in the NCIC acknowledgment or because WACIC was unable to locate the record with the ORI and record identifier(s) contained in the NCIC acknowledgment.

VI. NCIC CONVERSION OF ALPHABETIC “O” TO ZERO

A. NCIC converts the alphabetic character "O" to numeric zero in all identifying data elements in both entries and inquiries. WACIC does not make this conversion and treats alphabetic Os and zeros as separate and distinct characters. Therefore, if a record is entered with an identifier containing an alphabetic O and a subsequent inquiry is made using a zero (or vice versa), WACIC will not return a hit on the previously entered record; however, NCIC will. This is significant in situations, such as pawned articles, where the record is entered in WACIC only. An inquiry containing alphabetic Os or zeros will not produce a hit on a record entered with the opposite character. Thus, it is recommended that when an identifier in an inquiry contains alphabetic Os or zeros, multiple inquiries should be made with each possible combination of Os and zeros.

VII. POINT-TO-POINT MESSAGES

A. Messages are acknowledged or rejected by ACCESS immediately after they are sent.

1. Example of an acknowledgment:

XMIT MSGT#: 420 TIME: 1010 DATE: 052912
SENT TO: ABDPD

VIII. MESSAGE TERMINOLOGY

A. Station Address/Mnemonic: All network stations are assigned a four to five character station address code to uniquely identify the terminal. All out of state messages routed through Nlets use the five character mnemonic, “NLTAP”. All in state messages use the agency specific mnemonic. NCIC ORIs are used as station addresses on the Nlets network. For a list of Washington State agencies, refer to the Agency Directory Section of this chapter.

B. Group Codes: Group codes target a specific region. By employing a group address code, the operator may transmit the same message to several departments without the need of individual coding.

C. Message Numbers: Message numbers or input sequence numbers are assigned by the ACCESS computer. Each point to point message originating from each terminal will be assigned a number running from 0001 to 9999. This message number will appear in the message acknowledgment immediately following message transmission.

D. Output Header: The output header precedes the message text as received by the addressee.

IX. DELAYED INQUIRY HIT NOTIFICATIONS

A. WACIC Delayed Inquiry Hit Notifications

1. WACIC stores all vehicle and person inquiries for a period of three days to compare against any subsequent entries or modifications. When a record is entered or modified in WACIC and a matching inquiry from the previous three-day period is found, WACIC will append a notice to the normal entry or modify acknowledgment. It is then up to the entering agency to contact the inquiring agency to determine if the delayed hit is significant and can provide any investigative leads.

2. WACIC generates a delayed inquiry hit whenever the entry or modify references a person or vehicle that was queried if there is an exact match on any one of the following data elements: NAM, SOC, MNU, LIC, VIN, FBI, and SID. A delayed inquiry hit is only generated when the ORI in the inquiry is different from the ORI in the record being entered or modified.

3. Example of a WACIC delayed inquiry hit:

WWCIC (E772SP055)WAWSP2000
ENTERED EVI LIC/188UQS VIN/JH4KA9650VC001473
WAC/12V0036713 OCA/5659
04/03/2012 AT 00/05
BE ADVISED THAT SP CAD BELLEVUE PREVIOUSLY
INQUIRED ON: LIC/188UQS
AT 23:44 ON 04/02/2012 FROM SP054 MNE(SP054)

B. NCIC Delayed Inquiry Hit Response

1. NCIC stores all inquiries for a period of five days for comparison against any subsequent entries or modifies. When a record is entered or modified in NCIC and a matching inquiry from the

previous five-day period is found, NCIC automatically generates a notice to both the inquiring agency and the agency that entered or modified the record. It is then up to the two agencies involved to communicate to determine if the delayed hit is significant and can provide any investigative leads.

2. Example of an NCIC delayed inquiry hit:

WAKCS0000
YOUR RECORD WITH NIC/G862677510 OCA/77055821 IS A POSSIBLE DELAYED INQUIRY MATCH
PLEASE ASSURE YOUR ENTRY IS A REASONABLE MATCH WITH THE INQUIRY ON 1225 EDT 20120330 CONTAINING:
1N01DKCC QURYH
SER/286213
INQUIRING ORI/WAKCS0027 ATR/KING COUNTY SHERIFFS OFFICE
206 296-0970

X. FORMAT TERMINOLOGY

A. Station Directory: All network stations are assigned a four or five character station address code to uniquely identify the terminal. All out of state messages routed through Nlets use the five character mnemonic, “NLTAP”. All in state messages use the agency specific mnemonic. NCIC ORIs are used as station addresses on the Nlets network. For a list of Washington State agencies, refer to the Agency Directory Section of this chapter.

B. Group codes target a specific region. By employing a group address code, the operator may transmit the same message to several departments without the need of individual coding.

C. Message Numbers: Message numbers or input sequence numbers are assigned by the ACCESS computer. Each point to point message originating from each terminal will be assigned a number running from 0001 to 9999. This message number will appear in the message acknowledgment immediately following message transmission.

D. Acknowledgments: Point to point messages are acknowledged or rejected by ACCESS immediately after they are sent. They will conform to the following message:

XMIT MSGT#: 420 TIME: 1010 DATE: 052912
SENT TO: ABDPD

E. Output Header: The output header precedes the message text as received by the addressee.

XI. BENEFITS AND EFFECTIVENESS DATA

A. Benefits and effectiveness data are collected by the NCIC System to provide users with a means of collecting data associated with solving cases. This information is sent directly to NCIC. Monthly summaries of benefits and effectiveness data may be obtained by performing an RBED transaction. For more information, refer to the NCIC Operating Manual.

B. Entry of benefits and effectiveness data is not mandatory. However, users are encouraged to include it in locate, clear, and cancel transactions as it provides valuable information.

Procedure #:	01.14.000	**Effective Date:**	June 1, 2012
Supersedes:	ACCESS Manual, TAC Guide, Ready Reference Guide, WACIC Manual	**See Also:**	
Applies To:	All ACCESS Users	**CALEA:**	

I. RETENTION OF TERMINAL PRODUCED PRINTOUTS

A. When an inquiry yields a hit, the terminal employee making the inquiry should note on the terminal-produced printout precisely how, when, and to whom the information was given, initial and date this notation, and forward the printout to the inquiring officer or agency for retention in the case file. This procedure establishes the chain of evidence should the arresting officer need to substantiate actions in a judicial proceeding.

B. The printout should be retained for as long as there remains any possibility that the defendant will challenge the arrest, search, or other law enforcement action taken because of the information contained on the printout. The printout should be retained until all possible levels of appeal are exhausted or the possibility of a civil suit is no longer anticipated.

II. WACIC PURGE SCHEDULE

A. WACIC purges records in two processes:

1. The daily purge

   a. Refer to the individual chapter for retention on each record type.

2. The annual purge

   a. WACIC will purge records automatically when the record has met retention. WACIC sends purge notifications to the primary device ORI via MKE/RSP.

      - Due to the WACIC upgrade in June 2021, we are no longer sending excel lists of purged records since this is now an automated process.

III. NCIC PURGE SCHEDULE

A. NCIC sends a $.P. notification to the ORIs, informing them their record has been "retired." They retire records according to the retention period explained in each file chapter.

Procedure #:	01.15.000	**Effective Date:**	June 1, 2012
Supersedes:	ACCESS Manual, TAC Guide, Ready Reference Guide, WACIC Manual	**See Also:**	
Applies To:	All ACCESS Users	**CALEA:**	

I. COUNTY DIRECTORY

County Number	County	Terminal	City
01	Adams	RITSO	Ritzville
02	Asotin	ASOSO	Asotin/Clarkston
03	Benton	KENSO	Kennewick
04	Chelan	WENSO	Wenatchee
05	Clallam	PTASO	Port Angeles
06	Clark	VANSO	Vancouver
07	Columbia	DAYPS	Dayton
08	Cowlitz	KELSO	Kelso
09	Douglas	EWESO	East Wenatchee
10	Ferry	REPSO	Republic
11	Franklin	PASPS	Pasco
12	Garfield	POMSO	Pomeroy
13	Grant	EPHSO	Ephrata
14	Grays Harbor	MONSO	Montesano
15	Island	CPVSO	Coupeville
16	Jefferson	PTTSO	Port Townsend
17	King	SEASO	Seattle
18	Kitsap	PTOSO	Port Orchard
19	Kittitas	ELLSO	Ellensburg
20	Klickitat	GOLSO	Goldendale
21	Lewis	CHESO	Chehalis
22	Lincoln	DAVSO	Davenport
23	Mason	SHESO	Shelton
24	Okanogan	OKASO	Okanogan
25	Pacific	SOBSO	South Bend
26	Pend Orielle	NEWSO	Newport
27	Pierce	TACSO	Tacoma
28	San Juan	FRISO	Friday Harbor

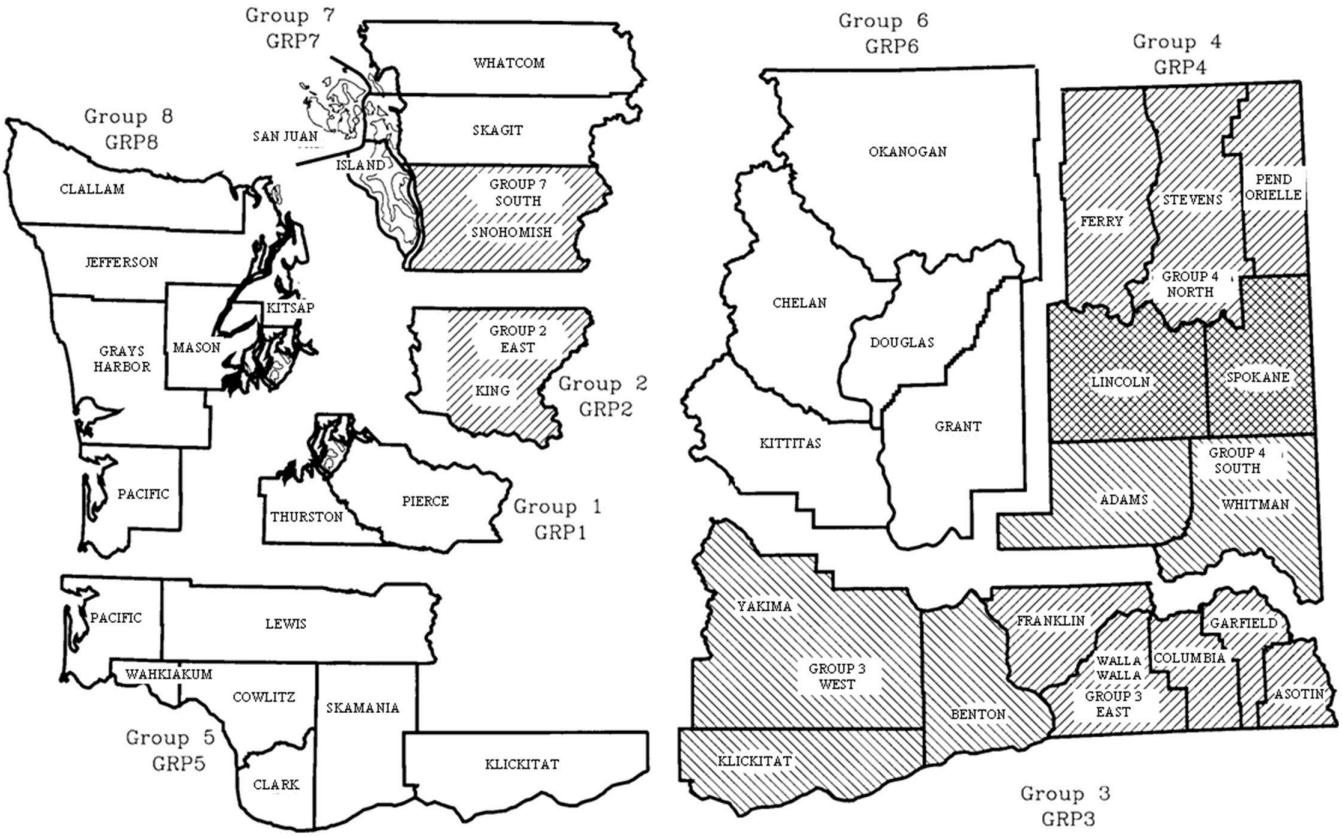
29	Skagit	MTVSO	Mount Vernon
30	Skamania	STESO	Stevenson
31	Snohomish	EVESO	Everett
32	Spokane	SPOPS	Spokane
33	Stevens	CLVSO	Colville
34	Thurston	OLYSO	Olympia
35	Wahkiakum	CATSO	Cathlamet
36	Walla Walla	WWASO	Walla Walla
37	Whatcom	BELSO	Bellingham
38	Whitman	COLSO	Colfax
39	Yakima	YAKSO	Yakima

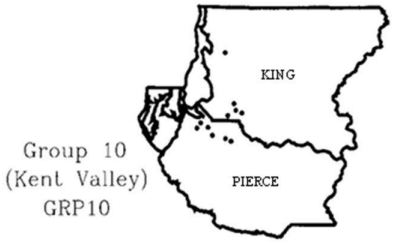
II. STATE AND PROVINCE CODES

United States and Territories					
Alabama	AL	Kentucky	KY	Ohio	OH
Alaska	AK	Louisiana	LA	Oklahoma	OK
American Samoa	AM	Maine	ME	Oregon	OR
Arizona	AZ	Maryland	MD	Pennsylvania	PA
Arkansas	AR	Massachusetts	MA	Puerto Rico	PR
California	CA	Michigan	MI	Rhode Island	RI
Colorado	CO	Minnesota	MN	South Carolina	SC
Connecticut	CT	Mississippi	MS	South Dakota	SD
Delaware	DE	Missouri	MO	Tennessee	TN
District of Columbia	DC	Montana	MT	Texas	TX
Florida	FL	Nebraska	NB	Utah	UT
Georgia	GA	Nevada	NV	Vermont	VT
Hawaii	HI	New Hampshire	NH	Virginia	VA
Idaho	ID	New Jersey	NJ	Washington	WA
Illinois	IL	New Mexico	NM	West Virginia	WV
Indiana	IN	New York	NY	Wisconsin	WI
Iowa	IA	North Carolina	NV	Wyoming	WY
Kansas	KS	North Dakota	ND		
Canadian Provinces					
Alberta	AB	Newfoundland	NF	Quebec	PQ
British Columbia	BC	Northwest Territories	NT	Saskatchewan	SN
Manitoba	MB	Nova Scotia	NS	Yukon Territory	YT
Namavut	XN	Ontario	ON		
New Brunswick	NK	Prince Edward Island	PE		

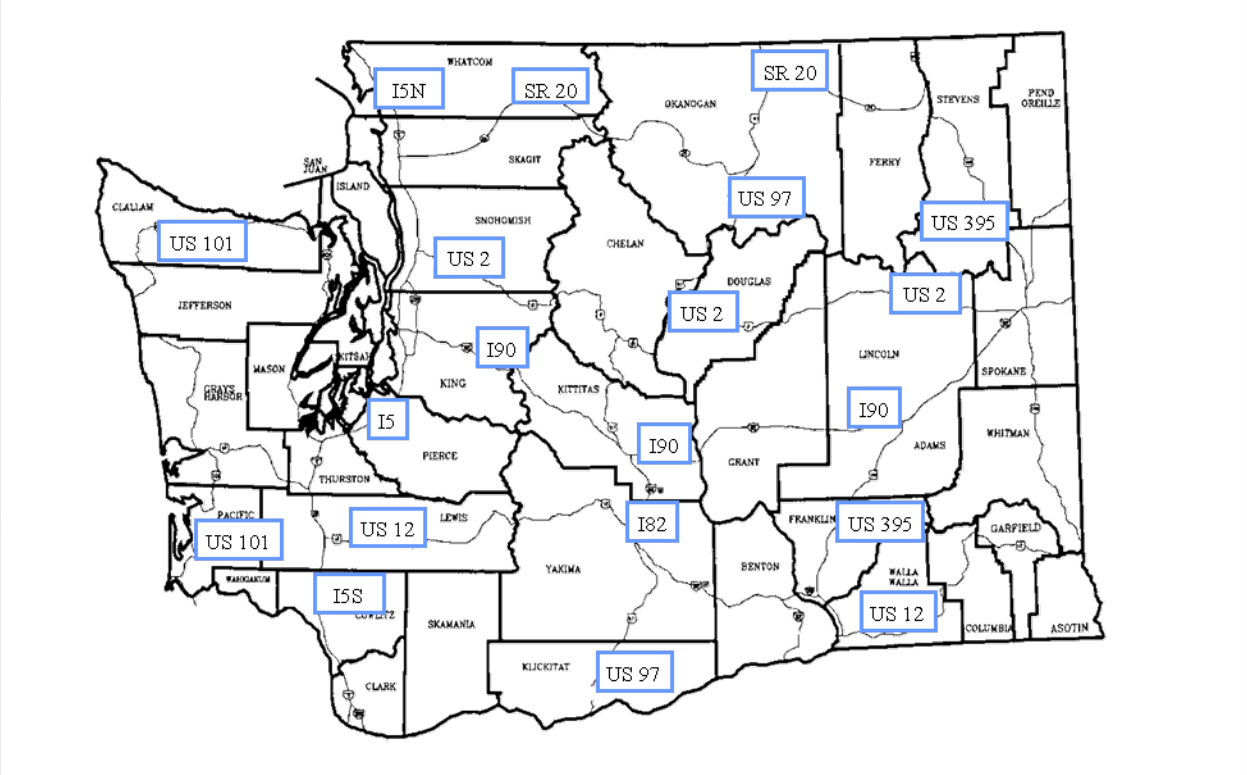
Note: For a list of federal codes, refer to the Nlets Wiki/User Manual.

III. STATE GROUP CODES





Group Name	Group Mnemonic	Group Members
Group 1	GRP1	Pierce and Thurston
Group 2	GRP2	King
Group 2 East	GRP2E	East King
Group 3	GRP3	Asotin, Benton, Columbia, Franklin, Garfield, Klickitat, Walla Walla, and Yakima
Group 3 East	GRP3E	Asotin, Columbia, Franklin, Garfield, and Walla Walla
Group 3 Tri-Cities	GRP3T	Tri-Cities Agencies
Group 3 West	GRP3W	Benton, Klickitat, and Yakima
Group 4	GRP4	Adams, Ferry, Lincoln, Pend Orielle, Spokane, Stevens, and Whitman
Group 4 North	GRP4N	Ferry, Lincoln, Pend Orielle, Spokane, and Stevens
Group 4 South	GRP4S	Adams, Lincoln, Spokane, and Whitman
Group 5	GRP5	Clark, Cowlitz, Klickitat, Lewis, Pacific, Skamania, and Wahkiakum
Group 6	GRP6	Chelan, Douglas, Grant, Kittitas, and Okanogan
Group 7	GRP7	Island, San Juan, Skagit, Snohomish, and Whatcom
Group 7 South	GRP7S	Snohomish
Group 8	GRP8	Clallam, Grays Harbor, Jefferson, Kitsap, Mason, and Pacific
Group 9	GRP9	King, Kitsap, Pierce, Snohomish, and Thurston
Group 10	GRP10	King and Pierce
Group 13	EAST	Eastern Washington
Group 14	WEST	Western Washington
All Agencies	ALL1 and ALL2	Various Agencies
Jail	JAIL	All Jail Terminals
Police Depts. East and West	PDSOE and PDSOW	Various Police Departments
Port	PORT	All Ports
State Patrol	WSPAP	All State Patrol Terminals
State Patrol Comm. Centers	WSPCC	All State Patrol Communications Centers



Group Name	Group Mnemonic	Group Members
Interstate 5	I5	Agencies Along Interstate 5 Corridor
Interstate 5 North	I5N	Agencies Along Interstate 5 North Corridor
Interstate 5 South	I5S	Agencies Along Interstate 5 South Corridor
Interstate 82	I82	Agencies Along Interstate 82 Corridor
Interstate 90	I90	Agencies Along Interstate 90 Corridor
State Route 20	SR20	Agencies Along State Route 20 Corridor
United States 101	US101	Agencies Along United States 101 Corridor
United States 12	US12	Agencies Along United States 12 Corridor
United States 2	US2	Agencies Along United States 2 Corridor
United States 395	US395	Agencies Along United States 395 Corridor
United States 97	US97	Agencies Along United States 97 Corridor

IV. **NLETS REGIONAL CODES**

Nlets Regional Codes							
Region A	Code: A1	Region B	Code: B1	Region C	Code: C1	Region D	Code: D1
Connecticut		District of Columbia		Kentucky		Alabama	
Maine		Delaware		Norht Carolina		Arkansas	
Massachusetts		Maryland		South Carolina		Florida	
New Hampshire		New Jersey		Tennessee		Georgia	
Rhode Island		New York		Virginia		Louisiana	
Vermont		Pennsylvania		West Virginia		Mississippi	
FBI/NCIC		FBI/NCIC		FBI/NCIC		Puerto Rico	
TECS		TECS		TECS		FBI/NCIC	
Interpol		Interpol		Interpol		TECS	
TSA		TSA		TSA		Interpol	
GSA		Army		Army		TSA	
Army		Navy		Navy		Army	
Navy		Department of Interior		Department of Interior		Navy	
Department of Interior		Department of Justice		Department of Justice		Department of Interior	
Department of Justice						Department of Justice	
Region E	Code: E1	Region F	Code: F1	Region G	Code: G1	Region H	Code: H1
Indiana		Iowa		Arizona		Alaska	
Illinois		Minnesota		Colorado		California	
Michigan		Montana		Kansas		Hawaii	
Missouri		Nebraska		New Mexico		Idaho	
Ohio		North Dakota		Oklahoma		Nevada	
Wisconsin		South Dakota		Texas		Oregon	
FBI/NCIC		Wyoming		Utah		Washington	
TECS		FBI/NCIC		FBI/NCIC		FBI/NCIC	
Interpol		TECS		TECS		TECS	
TSA		Interpol		Interpol		Interpol	
Army		TSA		TSA		TSA	
Navy		Army		Army		Army	
Department of Interior		Navy		Navy		Navy	
Department of Justice		Department of Interior		Department of Interior		Department of Interior	
		Department of Justice		Department of Justice		Department of Justice	

V. AGENCY DIRECTORY

AGENCY NAME	MNE-MONIC	ORI
A		
ABERDEEN PD	GH200	WA0140100
ADAMS CO DISTRICT COURT RITZVILLE	RITDC	WA001023J
ADAMS CO SO	RITSO	WA0010000
ADAMS COUNTY PROS.	ACPR3	WA001013A
AIRWAY HEIGHTS PD	AWHPD	WA0320600
ALGONA PD	ALGPD	WA0171400
ANACORTES PD	ANAPD	WA0290100
ARLINGTON PD	EVECC	WA0310100
ASOTIN CO SO	ASOSO	WA0020000
ASOTIN PD	CLAPD	WA0020200
ATF SEATTLE	ATFSE	WAATFSE00
ATTORNEY GENERAL OLYMPIA	OLYAG	WA034015A
ATTORNEY GENERAL SEATTLE	SEAAG	WA017015A
ATTORNEY GENERAL SPOKANE FRAUD	SPOAG	WA032015A
AUBURN PD	AUBPD	WA0170100
B		
BAINBRIDGE ISLAND PD	CC01	WA0180700
BATTLEGROUND PD	BATPD	WA0060100
BELLEVUE CITY PROBATION	BLVPR	WA017041G
BELLEVUE PD	BLVPD	WA0170200
BELLINGHAM PD	BELPD	WA0370100
BELLINGHAM MUNICIPAL COURT	BELMC	WA037011J
BENTON COUNTY CORRECTIONS	BCCOR	WA003013C
BENTON COUNTY DISTRICT COURT	BCD13	WA003013J
BENTON CO DIST CT PROB.	BCDCP	WA003013G
BENTON CO SO	KENCJ	WA0030000
BENTON-FRANKLIN CO JUV JUSTICE CTR	BFCJC	WA003073J
BIA CHEHALIS TRIBAL PD	GH014	WADI06700
BIA COLVILLE TRIBAL PD	CLVTP	WADI05700
BIA COWLITZ INDIAN TRIBAL PUBLIC SAFETY DEPARTMENT	VA150	WADI01500
BIA JAMESTOWN S'KALLAM TRIBAL PD	JSK00	WADI08200
BIA KALISPEL TRIBAL PD	KALTP	WADI06100
BIA KALISPEL TRIBAL COURT	KAC01	WADI0057J
BIA KALISPEL TRIBAL COURT PROBATION	KAP01	WADI0037G
BIA LA PUSH TRIBAL PD	LPT00	WADI07000
BIA LUMMI TRIBAL PD	BELCC	WADI05900
BIA MAKAH TRIBAL PD	NEAPD	WADI05600
BIA NISQUALLY TRIBAL	OLYCC	WADI00800
BIA PORT GABLE SKLALLAM TRIBAL PD	CC01	WADI06600
BIA PORT GAMBLE DNR	CM840	WADI08400
BIA PUYALLUP TRIBAL PD	PUYTP	WADI06200
BIA QUINAULT INDIAN NATION	QUITP	WADI05400
BIA SHOALWATER BAY TRIBAL PD	SOBSO	WADI01200
BIA SQUAXIN ISLAND TRIBAL PD	MACE	WADI05500
BIA STILLAGUAMISH TRIBAL PD	SCC01	WADI01300
BIA SUQUAMISH PD	CC01	WADI00900
BIA SWINOMISH TRIBAL PD	SWTB7	WADI06400
BIA TULALIP TRIBAL PD	TULPD	WADI06800
BIA UPPER SKAGIT TRIBAL PD	UPSTP	WADI06500
BIA SPOKANE DIVISION OF LAW ENFORCEMENT TRIBAL PD	SPOTP	WADI05100
BIA YAKIMA TRIBAL PD	YAKTP	WADI05800
BINGEN-WHITE SALMON PD	GOLSO	WA0200600
BLACK DIAMOND PD	BDIPD	WA0171500
BLAINE PD	BLAPD	WA0370200
BONNEY LAKE PD	BLKPD	WA0271400
BOTHELL PD	BOTPD	WA0170300
BREMERTON PD	BREPD	WA0180100
BREWSTER PD	BRW00	WA0240100
BRIER PD	MLTCC	WA0310800
BUCKLEY PD	BUCPD	WA0270400
BUREAU OF ALCOHOL, TOBACCO, FIREARMS AND EXPLOSIVES	STA00	WAATF0100
BUREAU OF ALCOHOL, TOBACCO, FIREARMS AND EXPLOSIVES	ATFYA	WAATF0200
BURLINGTON PD	BURPD	WA0290400
C		
CAMAS PD	CAMPD	WA0060200
CASTLE ROCK PD	KELSO	WA0080300
CENCOM	CC01	WA018013N
CENTRALIA PD	CENPD	WA0210100
CHEHALIS PD	CHEPD	WA0210200
CHELAN COUNTY DISTRICT COURT	CHDC1	WA004013J

AGENCY NAME	MNE-MONIC	ORI
CHELAN CO REGIONAL JUSTICE CTR	WENCJ	WA004013C
CHELAN CO SO	WENSO	WA0040000
CHELAN COUNTY PROBATION	WENPR	WA004013G
CHENEY MUNICPAL COURT	CH05	WA032011J
CHENEY PD	CHNPD	WA0320100
CHEWELAH PD	CLVSO	WA0330100
CLALLAM BAY CORR CTR	OLYDC	WA005035C
CLALLAM CO SO	PTASO	WA0050000
CLARK CO COMM CENTER	VANCC	WA006013N
CLARK CO JUVENILE COURT	VN25J	WA006025J
CLARK CO SO	VANSO	WA0060000
CLARK COUNTY SUPERIOR COURT	VN15J	WA006015J
CLARK CTY DIST CT PROBATION	VN132	WA006013G
CLARK CTY PROSECUTOR	VN131	WA006013A
CLARKSTON PD	CLAPD	WA0020100
CLE ELUM PD	ELLCC	WA0190200
CLYDE HILL PD	CLYPD	WA0172500
COLFAX PD	COLSO	WA0380100
COLLEGE PLACE PD	CPLPD	WA0360200
COLUMBIA CO PUBLIC SAFTEY COMM	DAYPS	WA007013N
COLUMBIA CO SO	DAYPS	WA0070000
COLVILLE PD	CLVSO	WA0330200
CONNELL PD	CNLPD	WA0110100
COSMOPOLIS PD	GH600	WA0140600
COUPEVILLE TOWN MARSHAL'S OFFICE	CPVSO	WA0150200
COVINGTON PD	SEASO	WA0174800
COWLITZ CO COMM CENTER	KLA47	WA008013N
COWLITZ CO CORRECTIONS	KELCJ	WA008013C
COWLITZ CO DIST COURT PROB	KELC4	WA008013G
COWLITZ CO SO	KELSO	WA0080000
COWLITZ COUNTY PROSECUTOR	KELSO	WA008013A
COWLITZ WAHKIAKUM NARCOTICS	KELSO	WA0080700
CWU PD	CWUPD	WA0190800
D		
DARRINGTON PD	EVECC	WA0310900
DEA BELLINGHAM	DEABL	WADEA0100
DEPT OF VET AFFAIRS MEDICAL CTR POLICE	VASEA	WAVA00200
DOUGLAS CO SO	EWESO	WA0090000

AGENCY NAME	MNE-MONIC	ORI
DEPT OF HEALTH	OLYHE	WA034265Y
DEPT OF LABOR & INDUSTRIES FRAUD	OLYLI	WA034085Y
DEPT OF NATURAL RESOURCES	DNR00	WA0342100
DEPT OF REVENUE OLYMPIA	OLYDR	WA034075Y
DES MOINES PD	DEMPD	WA0171700
DHS ICE FEDERAL PROTECTIVE SVS DENVER	FPSS2	WAFPS1100
DIRECTORATE OF EMERGENCY SERVICES	FTLCC	WAUSA0200
DOC AIRWAY HEIGHTS CORRECTIONS	AWHIN	WA032055C
DOC CEDAR CREEK CORRECTIONS	OC2T	WA034015C
DOC CORRECTIONS FOR WOMEN	PURIN	WA027055C
DOC COYOTE RIDGE CORR CTR	COYIN	WA011015C
DOC EVERETT REGIONAL OFFICE	ERJ35	WA031065C
DOC HEADQUARTERS	HQ595	WA034595C
DOC HUMAN RESOURCES RECRUITMENT UNIT	RU425	WA034425C
DOC HEARQUARTERS HUMAN RESOURCES	HR605	WA034605C
DOC INDETERMINATE SENTENCE REVIEW	OC08	WA034035G
DOC LARCH MOUNTAIN	SHEIN	WA006015C
DOC MISSION CREEK CORR CTR	MC015	WA023015C
DOC OLYMPIA REGIONAL OFFICE	ACCHA	WA034035C
DOC OLYMPIC CORR CTR	OC8J	WA016035C
DOC REYNOLDS WORK RELEASE	OCRWR	WA017285C
DOC SEATTLE REGIONAL OFFICE	RO045	WA017045C
DOC SHELTON CORR CTR	SHEIN	WA023025C
DOC SPOKANE RECORDS	SR575	WA032045C
DOC STAFFORD CREEK CORR CTR	SD015	WA014015C
DOC STATE REFORMATORY MONROE	MONIN	WA031015C
DOC STATEWIDE RECORDS TACOMA	OC03	WA027075C
DOC WALLA WALLA STATE PENITENTIARY	WWAIN	WA036015C
DOC YAKIMA REGIONAL OFFICE	OC10	WA039025C
DOL HEADQUARTERS	OLYDL	WA034335Y
DSHS CHILD SUPPORT	SHESSE	WA034015U

AGENCY NAME	MNE-MONIC	ORI
DSHS CHILDREN'S ADMINISTRATION	DSAW1	WA034015F
DSHS FRAUD AND ACCOUNTABILITY TACOMA	SHSST	WA027085Y
DSHS FRAUD AND ACCOUNTABILITY OLY	SHSSI	WA034025Y
DSHS GREEN HILL SCHOOL	GRHIN	WA021015C
DSHS SPECIAL COMMITMENT CENTER	SCCMI	WA027A15C
DSHS WESTERN STATE HOSPITAL	WSHOS	WA027025M
DUPONT PD	TACSO	WA0271600
DUVALL PD	DUVPD	WA0171800
E		
EAST WENATCHEE PD	EWEPD	WA0090200
EASTERN ST HOSP OFNDR UNIT	MDLES	WA032015M
EASTERN WA UNIVERSITY PD	CHNPD	WA0320900
EATONVILLE PD	FIFPD	WA0270500
EDGEWOOD PD	TACSO	WA0272500
EDMONDS PD	MLTCC	WA0310200
ELLENSBURG PD	ELLPD	WA0190100
ELMA PD	GH800	WA0140200
ENUMCLAW PD	ENUPD	WA0170400
EPHRATA PD	EPHPD	WA0130100
EVERETT CITY ATTORNEY	EVECC	WA031031A
EVERETT PD	EVEPD	WA0310300
EVERGREEN COLLEGE PD	ESCPD	WA0341900
EVERSON PD	BELCC	WA0370300
F		
FBI SEATTLE	FBISE	WAFBISE00
FEDERAL RESERVE BANK POLICE	FEDRB	WAFRB0000
FEDERAL WAY PD	FWYPD	WA0173600
FERNDALE PD	FERPD	WA0370400
FERRY CO SO	REPSO	WA0100000
FIFE PD	FIFPD	WA0270700
FIRCREST PD	FIRPD	WA0271700
FISH & WILDLIFE ENFORCEMENT	OLYFW	WA0349900
FORKS PD	FORPD	WA0050200
FRANKLIN CO SO	PASPS	WA0110000
G		
GAMBLING COMMISS OLYMPIA	OLYGC	WA0341000
GAMBLING COMMISS SPOKANE	SPOGC	WA0321700
GARFIELD CO SO	POMSO	WA0120000
GIG HARBOR PD	GIGPD	WA0271800
GOLD BAR PD	EVECC	WA0311000
GOLDENDALE PD	GOLSO	WA0200100
GRAND COULEE PD	GCP00	WA0130700
GRANDVIEW PD	GRAPD	WA0390100
GRANGER PD	YAKSO	WA0390700
GRANITE FALLS PD	OC22	WA0311100
GRANT CO SO	EPHSO	WA0130000
GRAYS HARBOR CO SO	MONSO	WA0140000
GRAYS HARBOR CO COMM	GH911	WA014013N
H		
HOQUIAM PD	GH300	WA0140300
I		
ISLAND CO COMM CENTER	OAKCC	WA015013N
ISLAND CO JUVENILE DETENTION	ICJDC	WA015035J
ISLAND CO SO	CPVSO	WA0150000
ISLAND CO PROSECUTOR	ICP00	WA015013A
ISSAQUAH PD	ISSPD	WA0170600
J		
JEFF COMM 911	JEF01	WA016023N
JEFFERSON CO SO	PTTSO	WA0160000
K		
KALAMA PD	KALPD	WA0080400
KELSO PD	KESO3	WA0080100
KENMORE PD	SEASO	WA0174900
KENNEWICK PD	KENPD	WA0030100
KENT CITY ATTORNEY	KNTCA	WA017061A
KENT JAIL	KNTCJ	WA0170702
KENT PD	KNTPD	WA0170700
KETTLE FALLS PD	CLVSO	WA0330300
KING CO DIST COURT PROB	SEADC	WA017023G
KING CO JUVENILE COURT	DKGA5	WA017045J
KING CO SO	SEASO	WAKCS0000
KING CO YOUTH SERVICES	DKGQ	WA017023C
KING CO JAIL	SEACJ	WA017033C
KIRKLAND MUNICIPAL COURT	KIJ0	WA0174K1J
KIRKLAND PD	KIRPD	WA0170800
KITSAP CO CORONER OFFICE	KCCR	WA018013K

AGENCY NAME	MNE-MONIC	ORI
KITSAP CO JUVENILE COURT	BRJ00	WA018025J
KITSAP CO SO	PTOSO	WA0180000
KITSAP 911	CC01	WA018013N
KITSAP CO PROSECUTOR	PTOPA	WA018013A
KITTCOMM COMM CENTER	ELLCC	WA019063N
KITTITAS CO SO	ELLSO	WA0190000
KITTITAS CO PROBATION	ELLPR	WA019013G
KITTITAS CO PROSECUTOR	KIT1A	WA019013A
KITTITAS PD	ELLCC	WA0190600
KLICKITAT CO SO	GOLSO	WA0200000
L		
LA CENTER PD	VANCC	WA0060600
LACEY PD	OLYCC	WA0340400
LAKE FOREST PARK PD	LFPPD	WA0172600
LAKE STEVENS PD	SED8	WA0311900
LAKEWOOD CITY ATTORNEY	TACSO	WA027111A
LAKEWOOD MUNICIPAL COURT	TACSO	WA027201J
LAKEWOOD PD	TACSO	WA0272300
LANGLEY PD	CPVSO	WA0150300
LAW ENFORCEMENT AGAINST DRUGS	YL000	WA0391700
LEWIS CO COMM CENTER	CHECC	WA021013N
LEWIS CO DISTRICT COURT PROB	LCH6	WA021013G
LEWIS CO JAIL	CHSO2	WA0210001
LEWIS CO PROSECUTOR	LC90	WA021013A
LEWIS CO SO	CHESO	WA0210000
LIBERTY LAKE PD	LIBPD	WA0321300
LINCOLN CO SO	DAVSO	WA0220000
LIQUOR AND CANNABIS BOARD OLYMPIA	OLYLC	WA0341100
LONG BEACH PD	LOBPD	WA0250400
LONGVIEW PD	LONPD	WA0080200
LOTTERY COMMISSION OLYMPIA	OLYLT	WA0341200
LYNDEN PD	LDNPD	WA0370500
LYNNWOOD PD	LYNPD	WA0310400
M		
MABTON PD	YAKSO	WA0390900
MAPLE VALLEY PD	SEASO	WA0174700
MARYSVILLE PD	MARPD	WA0310500
MASON CO EMERGENCY COMM	MACE	WA023013N
MASON CO SO	SHESO	WA0230000
MATTAWA PD	MLKCC	WA0130900
MCCLEARY PD	GH900	WA0140400
MEDINA PD	MEDPD	WA0172000
MERCER ISLAND PD	MEIPD	WA0170900
MILL CREEK PD	MCRPD	WA0312100
MILTON PD	FIFPD	WA0270900
MONROE PD	EVECC	WA0311200
MONTESANO PD	GH700	WA0140500
MORTON PD	CHECC	WA0210300
MOSES LAKE PD	MLKPD	WA0130200
MOSSYROCK PD	CHECC	WA0210400
MOUNTLAKE TERRACE PD	MLTCC	WA0310600
MOXEE PD	YAKSO	WA0391400
MT VERNON PD	MTVPD	WA0290200
MUKILTEO PD	MLTCC	WA0311300
MULTI -AGENCY COMM CENTER	ML01	WA013013N
N		
NAPAVINE PD	CHECC	WA0210700
NATL PARK SVC MT RAINIER	NPSMR	WADI00100
NATL PARK SVC OLYMPIC	NPSPA	WADI00200
NEWCASTLE PD	KCM14	WA0174200
NEWPORT PD	NEWSO	WA0260200
NORCOM	NOR01	WA017A03N
NORMANDY PARK PD	NPKPD	WA0171000
NORTH BEND PD	SEASO	WA0171100
NORTHWEST HIDTA TASK FORCE	HIDTA	WADEA0264
NORTHWEST REGIONAL DRUG TASK FORCE	WMS11	WA0371000
O		
OAK HARBOR PD	OAKPD	WA0150100
OCEAN SHORES PD	GH400	WA0140800
OKANOGAN CO SO	OKASO	WA0240000
OLYMPIA CITY ATTORNEY	OP31	WA034011A
OLYMPIA PD	OLYPD	WA0340100
OLYMPIA PROBATION	OP94	WA034011G
OMAK PD	OMKPD	WA0240300
OROVILLE PD	OROPD	WA0240400
ORTING MUNICIPAL COURT	OMC01	WA027061J
ORTING PD	TACSO	WA0271300
OTHELLO PD	OTHPD	WA0010100

AGENCY NAME	MNE-MONIC	ORI
P		
PACIFIC CO SO	SOBSO	WA0250000
PACIFIC PD	PACPD	WA0172100
PALOUSE PD	PALPD	WA0380900
PASCO PD	PASPD	WA0110200
PEND OREILLE CO SO	NEWS0	WA0260000
PIERCE CO CORRECTIONS	LEC00	WA027013C
PIERCE CO JUVENILE COURT	LES00	WA027053J
PIERCE CO PRETRIAL SERVICES	TACSO	WA027013B
PIERCE CO PROSECUTORS OFFICE	TACSO	WA027013A
PIERCE CO SO	TACSO	WA0270000
PIERCE TRANSIT DIVISION OF PUBLIC SAFETY	LE055	WA027025Y
PORT ANGELES PD	PTAPD	WA0050100
PORT OF SEATTLE PD	POSPD	WA0173200
PORT ORCHARD PD	CC01	WA0180400
PORT TOWNSEND PD	PTTPD	WA0160100
POULSBO PD	CC01	WA0180500
PROSSER PD	PROPD	WA0030300
PUGET SOUND REGIONAL FIRE AUTH INVEST UNIT	VCV3	WA0175400
PULLMAN PD	PULPD	WA0380300
PUYALLUP PD	PUYPD	WA0270100
Q		
QUINCY PD	QUIPD	WA0130300
R		
RAINIER PD	OLYCC	WA0340600
RAYMOND PD	RAYPD	WA0250100
REARDAN PD	BVVB3	WA0220700
REDMOND CITY ATTORNEY	RD42	WA017121A
REDMOND PD	REDPD	WA0171200
RENTON PD	RENPD	WA0171300
RICHLAND PD	RICPD	WA0030200
RIDGEFIELD PD	VANSO	WA0060500
RIVERCOM	RC000	WA004013N
ROYAL CITY PD	RCPD0	WA0131000
ROY PD	TACSO	WA0271000
RUSTON PD	TACSO	WA0271900
S		
SAMMAMISH PD	SEASO	WA0175000
SAN JUAN CO SO	FRISO	WA0280000
SEATAC PD	SEASO	WA0173700
SEATTLE CITY ATTORNEY	SEAPD	WA017031A
SEATTLE COMMUNITY SAFETY AND COMMUNICATIONS CENTER	SEACC	WA017T53N
SEATTLE FIRE DEPT	SEAPD	WA0175300
SEATTLE MUNI CT PROBATION	SEMC2	WA017021G
SEATTLE MUNI CT PRETRIAL SVS	SMCPS	WA017011B
SEATTLE MUNICIPAL COURT	UD000	WA017331J
SEATTLE PD	SEAPD	WASPD0000
SEATTLE PD WARRANT DIVISION	SEAWT	WA017071J
SEDRO WOOLLEY PD	SEDPD	WA0290300
SELAH PD	SELPD	WA0391100
SEQUIM PD	SEQPD	WA0050300
SHELTON PD	MAS44	WA0230400
SHORELINE PD	SEASO	WA0174300
SKAGIT 911 COMM CENTER	MTVCC	WA029013N
SKAGIT CO SO	MTVSO	WA0290000
SKAMANIA CO SO	STESO	WA0300000
SNOHOMISH CO 911	SCC01	WA031W93N
SNOHOMISH CO FIRE MARSHALS	EVESO	WA0312700
SNOHOMISH JUVENILE CRT SERVICES	SE223	WA031063J
SNOHOMISH CO PROSECUTOR	EVEPA	WA031013A
SNOHOMISH CO SO	EVESO	WA0310000
SNOHOMISH PD	SESNO	WA0310700
SNOHOMISH REGIONAL DRUG AND GANG TASK FORCE	SET00	WA0322300
SNOQUALMIE PD	SNQPD	WA0172200
SOAP LAKE PD	ML77	WA0130400
SOUTH BEND PD	SOBPD	WA0250200
SOUTH CORRECTIONAL ENTITY (SCORE)	SCO90	WA017021C
SOUTH SOUND 911	LES00	WA027013N
SOUTHEAST COMM CENTER	KENCC	WA003013N
SP ACCESS CUSTOMER SERVICE	ZLQUE	WAWSP0001
SP ACCESS OPERATIONS	ZLQUE	WAWSP0000
SP BREMERTON	BRESP	WAWSP8000
SP EVERETT (MARYSVILLE)	EVESP	WAWSP7000
SP IDENTIFCATION	IDENT	WAWSP0099
SP MISSING PERSONS UNIT	MCCH2	WAWSP0090

AGENCY NAME	MNE-MONIC	ORI
SP SEATTLE (BELLEVUE)	SEASP	WAWSP2000
SP SPOKANE	SPOSP	WAWSP4000
SP SYSTEM ADMINISTRATOR	ACCSS	WAWSP0007
SP TACOMA	TACSP	WAWSP1000
SP VANCOUVER	VANSP	WAWSP5000
SP WENATCHEE	WENSP	WAWSP6000
SP YAKIMA	YAKSP	WAWSP3000
SPOKANE AIRPORT PD	STM10	WA0321200
SPOKANE CITY PROBATION SVS	ST01F	WA032011G
SPOKANE CITY PROS OFFICE	ACCS1	WA032041A
SPOKANE CO PROSECUTOR	ST13A	WA032013A
SPOKANE CO DETENTION SERVICES	STN22	WA032753C
SPOKANE CO DISTRICT COURT	ST13J	WA032013J
SPOKANE CO DISTRICT COURT PROB	ST23J	WA032013G
SPOKANE CO JUVENILE COURT	ST35J	WA032035J
SPOKANE CO PRETRIAL SVS	ST01D	WA032013B
SPOKANE CO SO	SPOPS	WA0320000
SPOKANE CO 911	STC00	WA032013N
SPOKANE FIRE DEPT	STSFD	WA0322000
SPOKANE PD	SPOPS	WA0320400
SPOKANE REGIONAL DRUG TASK FORCE	STOW4	WA0321100
SPOKANE REGIONAL EMERGENCY COMM	SRECC	WA032343N
SPOKANE VALLEY FIRE DEPT	ST070	WA0321400
STANWOOD PD	EVECC	WA0311400
STEILACOOM PD	STEPD	WA0271100
STEVENS CO SO	CLVSO	WA0330000
SULTAN PD	EVECC	WA0311500
SUMAS PD	BPBLA	WA0370700
SUMNER PD	SUMPD	WA0270200
SUNCOMM YAKIMA PUBLIC SAFETY COMM CENTER	SUNCO	WA039013N
SUNNYSIDE PD	SUNPD	WA0390200
T		
TACOMA CITY PROSECUTOR	LEAJ8	WA027031A
TACOMA MUNICIPAL COURT	TACPD	WA027101J
TACOMA PD	TACPD	WA0270300
TENINO PD	OLYCC	WA0340800
THURSTON CO JUVENILE COURT	TCJUV	WA034043J
THURSTON CO NARCOTICS TASK FORCE	OLYCC	WA0341800
THURSTON CO PROSECUTOR	OLYSO	WA034013A
THURSTON CO SO	OLYSO	WA0340000
THURSTON CO COMM 911	OLYCC	WA034013N
THURSTON CO JAIL	OLJ13	WA034013C
THURSTON CO SUPERIOR CRT PRETRIAL SERVICES	TCPTS	WA034013B
TIETON PD	YAKSO	WA0391200
TOLEDO PD	CHECC	WA0211000
TOPPENISH PD	TOPPD	WA0390300
TUKWILA PD	TUKPD	WA0172300
TUMWATER PD	OLYCC	WA0340200
TWISP PD	OKASO	WA0240900
U		
U.S. ARMY YAKIMA TRAINING	MPYAK	WA039017N
U.S. DOE SECURITY AND SAFEGUARDS	DOE01	WADOE0200
UNION GAP PD	UGPPD	WA0390400
UNIVERSITY PLACE PD	TACSO	WA0272400
UNIVERITY OF WASHINGTON (UW) PD	UOWPD	WA0172400
V		
VALLEY COMM CENTER	KNTCC	WA017013N
VANCOUVER CITY ATTORNEY	VN133	WA006031A
VANCOUVER PD	VANPD	WA0060300
W		
WAHKIAKUM CO SO	CATSO	WA0350000
WALLA WALLA CO DEPT OF CORRECTIONS	WWJ13	WA036013C
WALLA WALLA CO SO	WWASO	WA0360000
WALLA WALLA CITY ATTORNEYS OFFICE	WW11A	WA036011A
WALLA WALLA CO PROS OFFICE	WW13A	WA036013A
WALLA WALLA COMM CTR	WWACC	WA036013N
WALLA WALLA CO DEPT OF COURT SERVICES	WWC25	WA036025J
WALLA WALLA PD	WWAPD	WA0360100
WAPATO PD	WAPPD	WA0391300
WARDEN PD	EML77	WA0131100
WASHINGTON EMERGENCY MANAGEMENT	OLYEM	WA027CMVS
WASHINGTON INSURANCE COMMISSIONER	INS29	WA034225Y

AGENCY NAME	MNE-MONIC	ORI
WASHINGTON STATE FUSION CENTER	WSFC	WAWSP0022
WASHINGTON STATE PARKS AND RECREATION	PRK01	WA03420000
WASHINGTON STATE UNIVERSITY POLICE	WSUPD	WA0380500
WASHINGTON STATE UNIVERSITY PD VANCOUVER	VANCC	WA0061000
WASHOUGAL PD	WASPD	WA0060400
WENATCHEE PD	WENPD	WA0040400
WEST RICHLAND PD	WRIPD	WA0030500
WESTERN WA UNIVERSITY PD	WWUPD	WA0370800
WESTPORT PD	GH500	WA0140900
WHATCOM CO COMM CENTER	BELCC	WA037013N
WHATCOM CO DISTRICT COURT PROB	WMA14	WA037013G
WHATCOM CO FIRE MARSHALS OFFICE	WCF00	WA0371100
WHATCOM CO JUVENILE COURT	WMJ01	WA037025J
WHATCOM CO PROSECUTOR	BELSO	WA037013A
WHATCOM CO SO	BELSO	WA0370000
WHITMAN CO COMM CENTER	CX20	WA038013N
WHITMAN CO PROSECUTOR	COLSO	WA038013A
WHITMAN CO SO	COLSO	WA0380000
WINLOCK PD	CHECC	WA0211200
WINTHROP PD	OKASO	WA0241000
WOODINVILLE PD	SEASO	WA0174000
WOODLAND PD	KELSO	WA0080500
WOODWAY PD	MLTCC	WA0311600
Y		
YAKIMA CO CORRECTIONS	YAKCJ	WA039013C
YAKIMA CO DISTRICT COURT PROBATION	YSA10	WA039013G
YAKIMA CO JUVENILE COURT	YKJVC	WA039025J
YAKIMA CO PRE-TRIAL SERVICES	YPT01	WA039013B
YAKIMA CO PROSECUTOR	YASO2	WA039013A
YAKIMA CO SO	YAKSO	WA0390000
YAKIMA DISTRICT COURT	YAKSO	WA039033J
YAKIMA PD	YAKPD	WA0390500
YELM PD	OLYCC	WA0340900
Z		
ZILLAH PD	ZILPD	WA0390600