2016-17

WASHINGTON STATE PATROL
ACCESS USER ACKNOWLEDGMENT

I. Introduction

Since its inception, the National Crime Information Center (NCIC) has operated under a shared management concept between the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Division and state users. The NCIC Advisory Policy Board established a single state agency in each state to assume responsibility as the NCIC CJIS Systems Agency (CSA) for all agencies within the state. The CSA is responsible for the planning of necessary hardware, software, funding, security, auditing, and training of all authorized agencies within the state for complete access to FBI CJIS systems data services. The Washington State Patrol (WSP) Criminal Records Division (CRD) Administrator is designated as the NCIC CJIS Systems Officer (CSO). The FBI CJIS Division requires the CSO to manage the following:

1. Operational, technical, and investigative assistance to NCIC users
2. Telecommunications lines to a state interface
3. Legal and legislative review of matters pertaining to NCIC
4. Timely distribution of information related to all aspects of NCIC system usage by means of the ACCESS Operations Manual, NCIC Operating Manual, CJIS Security Policy, Technical and Operational Updates, and related documents
5. Training and training materials to all participating agencies
6. System security to include physical security, personnel, and all technical aspects of security as required in the CJIS Security Policy

The following documents are incorporated by reference and made part of this user acknowledgment:

1. ACCESS Operations Manual
2. CJIS Security Policy
3. U.S. Code of Federal Regulations, Title 28, Part 20
4. Applicable federal and state laws and regulations; ACCESS/WACIC rules, regulations, and policies as recommended by the ACCESS Section

II. Primary Connection and Originating Agency Identifier (ORI) Issuance

All agencies that inquire on or enter data into ACCESS must have a primary connection to ACCESS and a signed WSP ACCESS User Acknowledgment on file prior to adding secondary connections such as regional management systems. Agencies must ensure that all system use through both the primary or secondary connections remain in compliance with ACCESS and FBI CJIS rules.

The CSO will coordinate the assignment of new ORI numbers, the change in ORI location or address, and any other changes, cancellations, or retirements of ORIs accessing WACIC/NCIC. The assignment of an ORI to an agency is not a guarantee of access to the state and federal systems. The CSA makes the final determination of who may access WACIC/NCIC based on the standards provided by the CJIS Security Policy and determination of an agency's administration of criminal justice. Any requests for additional ORIs by an agency will be forwarded to the WSP ACCESS Section Manager, who will

conduct a short audit of the agency to verify compliance standards are being met. See ACCESS Operations Manual Introduction for more information.

III. Indemnification

Each agency(party) shall defend, protect, and hold harmless the other agency(party) from and against all claims, suits and/or actions arising from any negligent or intentional act or omission of that party's employees, agents, and/or authorized subcontractor(s) while performing under this agreement.

IV. Administrative Responsibilities

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

All agencies are required to have formalized written procedures for the following, if applicable: validations, hit confirmation, criminal history use and dissemination, ACCESS misuse, record entry (for all record types entered into WACIC and NCIC), rebackground investigations, password management, disposal of media, physical protection and documenting, updating the system network.

The CSO provides system training to agencies accessing WACIC/NCIC through the state computer system. If employees are using inquiry only functions, they must attend Level 1 certification training. Employees entering information into the WACIC/NCIC system must attend Level 2 certification training. All certifications must be aquired within six months of hire date and renewed biennially. All staff who manage ACCESS users and are not ACCESS certified must view the Upper Management and Administrators Overview Training online and sign the signature log, which must be kept at the agency for review during the triennial ACCESS audit.

Security awareness training is required within six months of initial assignment, and biennially thereafter, for all personnel (who are not ACCESS certified) that have unescorted access to CJI. This includes agency employees, custodial staff, IT staff, upper management, etc. Records of individual basic security awareness training shall be documented, kept current, and maintained by each agency for review during the triennial ACCESS or Technical Security audit.

A Terminal Agency Coordinator (TAC) must be assigned for each terminal agency. This person is the Point Of Contact (POC) for the agency. A TAC must maintain a Level 2 ACCESS certification. The TAC retains the responsibility of ensuring his/her agency is in compliance with state and FBI CJIS Division policies and regulations. A TAC must attend TAC training once during the triennial audit cycle.

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

The CSO provides the criminal justice community with the current ACCESS Operations Manual, NCIC Operating Manual, NCIC Code Manual, and CJIS Security Policy. Manual updates are provided on a quarterly basis. The agency shall incorporate such changes upon receipt. Information is provided via email and can be found on the ACCESS website at the following link:

http://www.wsp.wa.gov/_secured/access/access.htm

V. Criminal History Record Information (CHRI) Responsibilities

Each agency shall conform to system policies, as established by the FBI CJIS Division and ACCESS, before access to CHRI is permitted. This will allow for control over the data and give assurance of system security.

1. The rules and procedures governing terminal access to CHRI shall apply equally to all participants in the system.
2. All criminal justice agencies with ACCESS terminals and access to computerized CHRI data from the system shall permit an FBI CJIS Division and an ACCESS audit team to conduct appropriate audits. Agencies must cooperate with these audits and respond promptly.
3. All terminals interfaced directly with the ACCESS/WACIC/NCIC systems for the exchange of CHRI must be under the management control of a criminal justice agency, as defined by the CJIS Security Policy.
4. All agencies must ensure they provide all required information when running criminal history checks. WSP retains access to all agency criminal history logs through the ACCESS System. Secondary dissemination of criminal history must be logged by the agency.

VI. Record Entry Responsibilities

Record Quality

Criminal justice agencies have a specific duty to maintain records that are accurate, complete, and current. ACCESS recommends agencies conduct self audits as a means of verifying the completeness and accuracy of the information in the system. These self assessments should be on a continual basis to ensure both quality assurance and compliance with standards. Errors discovered in NCIC records are classified as serious errors, form errors, or an error trend.

Serious errors: FBI CJIS will cancel the record and notify the entering agency via administrative message. The message provides the entire canceled record and a detailed explanation of the reason for cancellation.

Form errors or error trends: The CSA notifies the ORI by letter of the corrective action to be taken. No further notification or action will be taken by the CSA, unless the CSA deems it appropriate.

Timeliness

WACIC/NCIC records must be entered promptly to ensure maximum system effectiveness. Records must be entered according to standards defined in the ACCESS Operations Manual.

Accuracy and Completeness

The accuracy of WACIC/NCIC data must be double checked and documented, including the initials and date by a second party. The verification should include assuring the data in the WACIC/NCIC record matches the data in the investigative report and that other checks were made. Agencies lacking support staff for second party checks should require the case officer to check the record.

Complete records of any kind include all information available on the person or property at the time of entry. ACCESS recommends "packing the record" for all entries. Complete inquiries on persons include numbers that could be indexed in the record (i.e. Social Security Number (SSN), Vehicle Identification Number (VIN), Drivers License Number (OLN), etc.). Inquiries should be made on all names/aliases used by the suspect. Complete vehicle inquiries include VIN and license plate numbers.

Record Validations

NCIC/WACIC validation listing are prepared pursuant to a schedule, as published in the ACCESS Operations Manual. These listings are distributed to the originating agency via File Transfer Protocol (FTP).

Validation requires the originating agency to confirm the record is complete, accurate, and active. Validation is accomplished by reviewing the original entry and current supporting documents, and correspondence with any appropriate complainant, victim, prosecutor, court, motor vehicle registry files, or other appropriate source or individual. Validation efforts must be well documented. Validation efforts include what was done to complete the validation of the individual record. Documentation of phone calls, letters, dates and dispositions need to be included with each record that was validated. Many agencies document this information in the case file. In the event the agency is unsuccessful in its attempts to contact the victim, complainant, etc., the entering agency must make a determination based on the best information and knowledge available whether or not to retain the original entry in the file.

The agency must sign the validation certificate and fax, mail, or email a copy to the ACCESS Section each month certifying the records were validated. If the CSA has not received a validation certificate response from an agency within the specified period of time, the CSA will purge all records which are the subject of that agency's validation listings from NCIC and WACIC.

VII. Security Responsibilities

Technical Roles and Responsibilities

All agencies participating in ACCESS must comply with and enforce system security. Each interface agency (city, county, or other agency) having access to a criminal justice network must have someone designated as the technical security POC. A criminal justice network is a telecommunications infrastructure dedicated to the use by criminal justice entities exchanging criminal justice information. The technical security POC's shall be responsible for the following:

1. Identifying the user of the hardware/software and ensuring that no unauthorized users have access to the same
2. Identifying and documenting how the equipment is connected to the state system
3. Ensuring that personnel security screening procedures are being followed as stated in the CJIS Security Policy
4. Ensuring that appropriate hardware security measures are in place
5. Supporting policy compliance and keeping the WSP Information Security Officer (ISO) informed of security incidents

Security Enforcement

Each interface agency is responsible for enforcing system security standards for their agency, in addition to all of the other agencies and entities to which the interface agency provides CJIS and Washington State Department of Licensing (DOL) records information. Authorized users shall access CJIS and DOL systems and disseminate the data only for the purpose for which they are authorized. Each criminal justice and non-criminal justice agency authorized to access FBI CJIS systems and DOL shall have a written policy for the discipline of policy violators.

Physical Security

A physically secure location is a facility or an area, a room, or a group of rooms within a facility with both the physical and personnel security controls sufficient to protect CJI and associated information systems. The physically secure location is subject to criminal justice agency management control.

The perimeter of a physically secure location shall be prominently posted and separated from non-secure locations by physical controls.

All personnel with access to computer centers, terminal areas, and/or areas where CJIS information is housed shall either be escorted by authorized personnel at all times or receive a fingerprint-based background check and view security awareness training.

Personnel Security

To verify identification, a state of residency and national fingerprint-based record checks shall be conducted within 30 days of initial employment or assignment for all personnel who have authorized access to FBI CJIS systems and those who have direct responsibility to configure and maintain computer systems and networks with access to FBI CJIS systems. All requests for system access shall be made as specified by the CSO. The CSO or their official designee is authorized to approve CJIS systems access. All official designees to the CSO shall be from an authorized criminal justice agency.

Support personnel, contractors, and custodial workers who access computer terminal areas shall be subject to a state of residency and national fingerprint-based record check and view the security awareness training, unless these individuals are escorted by authorized personnel at all times. Authorized personnel are those persons who have passed a state and national fingerprint-based record check and have been granted access.

Private Contractors/Vendors

Private contractors shall be permitted access to CJIS record information systems pursuant to an agreement which specifically identifies the contractor's purpose and scope of providing services for the administration of criminal justice. The agreement between the criminal justice government agency and the private contractor shall incorporate the CJIS Security Addendum approved by the Director of the FBI. Private contractors who perform the administration of criminal justice shall meet the same training and certification criteria required by governmental agencies performing a similar function, and shall be subject to the same extent of audit review as are local user agencies.

Hit Confirmation

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.

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.

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.

VIII. Compliance Audits

The FBI CJIS Division requires triennial audits be conducted by the CSA to review CJIS standards of compliance and provide recommendations for best business practices. WSP audit staff provide three types of reviews:

1. **Agency Compliance Review:** WSP Auditors conduct an administrative interview with the TAC. The interview includes questions to determine adherence to WACIC/NCIC policy requirements including:

    a. TAC responsibilities
    b. ACCESS certification, rebackground of ACCESS users and other trainings
    c. System security
    d. Media protection
    e. Criminal history
    f. National Instant Criminal background Check System (NICS)
    g. Random sample of missing persons in WACIC/NCIC
    h. Random sample of warrants in WACIC/NCIC
    i. Random sample of protection orders in WACIC/NCIC
    j. Random sample of stolen vehicles in WACIC/NCIC
    k. Record maintenance
    l. Hit confirmation
    m. ORI usage and administration of criminal justice functions
    n. Written procedures
    o. Validations
    p. Site security visits to ensure terminal locations are secure

2. **Data Quality Review:** WSP Auditors conduct an on-site data quality review. Auditors compare WACIC/NCIC records against agency case files. Auditors check for accuracy, completeness, and verify entry and removal practices. The auditors document records with errors for the agency to update.

3. **Auditor Recommendations for Best Practices:** WSP Auditors provide a compliance report of information received during the interview and data quality review. They provide recommendations for best business practices.

IX. Technical Security Audits

The agency is responsible for compliance to technical standards set forth by ACCESS and the CJIS Security Policy. Technical security audits will follow the WACIC/NCIC triennial audit schedule.

1. **Agency Compliance Review:** The WSP ISO performs security audits addressing the following compliance areas:

   a. Personnel security measures
   b. Security incident response
   c. Configuration management control
   d. Encryption
   e. Media protection (physical and electronic)
   f. Physical protection
   g. Session lock capabilites
   h. System and communications protection and information integrity
   i. Boundary protection
   j. Malicious code protection
   k. Event logging capability
   l. System use notification
   m. Patch management
   n. Identification and authentication
   o. Wireless devices – mobile / bluetooth / cellular
   p. Partitioning and virtualization
   q. Cloud computing

WSP ACCESS USER ACKNOWLEDGMENT

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

I further understand DOL may review activities of any person who receives vehicle, vessel, and firearm record information to ensure compliance with limitations imposed on the use of the information. The DOL shall suspend or revoke for up to five years the privilege of obtaining information of a person found to be in violation of chapter 42.56 RCW, chapter 46.12 RCW, or the user agreement with DOL. I understand misuse of this information is a gross misdemeanor and is punishable by a fine not to exceed $10,000 or by imprisonment in a county jail not to exceed one year, or both such fine and imprisonment for each violation. RCW 46.12.640.

Agency Name:	City of Everett Prosecutor's Office	
ORI:	WA03031A	
Agency Head Name (printed):	James D. Iles	
Agency Head Email:	jiles@everettwa.gov	
Agency Head Telephone Number:	(425) 257-7000	
Agency Head Signature	James D. Iles	Date: 11/3/16

Please return a copy of this signature page to the WSP ACCESS Section.

24x7 Hit Confirmation Agreement
Must be completed by agencies who:

A. **Provide 24/7 teletype printer coverage for another agency.**
B. **Receive 24/7 teletype printer coverage from another agency.**

Every terminal agency that enters records destined for NCIC/WACIC must ensure hit confirmation is available for all records, except III, 24 hours per day either at the agency or through a written agreement with another agency at its location. The terminal agency printer must be monitored 24 hours per day. In the event that 24 hour per day hit confirmation coverage is not available, the terminal agency printer must be capable of being forwarded to a 24 hour a day facility. A 24 hour telephone number of the agency responsible for confirming hits must be placed in the Miscellaneous Field of every entry.

Parties who enter into this agreement must adhere to the response times and regulations set forth in the ACCESS Operations Manual and the CJIS Security Policy. This interagency agreement must be current and approved by the CJIS Systems Agency (CSA), the Washington State Patrol (WSP) before agencies adopt the policies and procedures set forth by the agreement.

Termination of Agreement
This agreement shall remain in effect unless terminated by either agency upon thirty (30) days written notice. The agency terminating the agreement must also formally notify the WSP ACCESS Section within the thirty (30) days. Termination of this agreement requires the agency printer to be forwarded to another 24 hour per day facility.

I hereby acknowledge the responsibility and duty to perform teletype hit confirmation to the terminal agency 24 hours per day within the requirements defined by NCIC/WACIC and the CJIS Security Policy.

Agency Providing 24/7 Coverage:		
ORI:		
Agency Head Name (printed):		
Agency Head Signature:		Date:

Agency Receiving 24/7 Coverage:		
ORI:		
Agency Head Name (printed):		
Agency Head Signature:		Date:

Holder of the Record Agreement

Must be completed by agencies who:

A. Use their ORI to enter another agency's records.
B. Have their records entered under another agency's ORI.

A Holder of the Record Agreement (HORA) is required when an agency uses their ORI to enter another agency's records, thus becoming the holder of the record. The holder of the record is defined as an agency that is using their ORI to enter another agency's records. The owner of a record is defined as the agency where the record originated.

The purpose of this agreement is to establish responsibility for records entered in WACIC/NCIC by the holder of record under its NCIC assigned ORI on behalf of the owner of record. As they relate to records entered for the owner of record, the holder of record assumes the following responsibilities: data entry; documentation; cancellation and modification of entries; timeliness of entries, cancellations and modifications; hit confirmation; second party checks; and validation of entries. The owner of the record is also responsible for providing the HORA with information for entry in a timely manner.

The holder of record must adhere to the regulations set forth in the ACCESS Operations Manual and the CJIS Security Policy. This interagency agreement must be current and approved by the CJIS Systems Agency (CSA), the Washington State Patrol (WSP) before agencies adopt the policies and procedures set forth by the agreement.

Entries provided under the HORA (check all that apply):

☐ All entries	☐ Articles	☐ Boats	☐ Gangs
☐ Guns	☐ Identity Theft	☐ Images	☐ License Plates
☐ Missing Persons	☐ Person of Interest	☐ Protection Orders	☐ Securities
☐ Supervised Persons	☐ Unidentified Persons	☐ Vehicles	☐ Vehicle/Boat Parts
☐ Wanted Persons	☐ Violent Persons		

Termination of Agreement

This agreement shall remain in effect unless terminated by either agency upon thirty (30) days written notice. The agency terminating the agreement must also formally notify the WSP ACCESS Section within the thirty (30) days. Termination of this Agreement shall not negate the obligation of either party to maintain records entered under this agreement to ensure their accuracy and timeliness.

Agency Acting as the Holder of the Record:		
ORI:		
Agency Head Name (printed):		
Agency Head Signature:		Date:

Agency Acting as the Owner of the Record:		
ORI:		
Agency Head Name (printed):		
Agency Head Signature:		Date:

Inter-agency Agreement

Must be completed by agencies who:

A. Provide criminal justice services to another agency.
B. Receive criminal justice services from another agency.

An inter-agency agreement describing the criminal justice services provided and/or received by an agency must be in place.

Agency Providing Service: SNO PAC 9.1.1

Agency Receiving Service: City of Everett Prosecutor's Office

Services Provided (check all that apply):

- [ ] Hit confirmation
- [ ] Dispatch
- [ ] Record entry
- [ ] Record validations
- [ ] Gun transfers/Concealed Pistol Licenses (CPLs)
- [x] Use of regional management system
- [x] Terminal connection to ACCESS
- [x] Other services (describe):

Parties who enter into this agreement must adhere to the regulations set forth in the ACCESS Operations Manual and the CJIS Security Policy. This interagency agreement must be current and approved by the CJIS Systems Agency (CSA), the Washington State Patrol (WSP) before agencies adopt the policies and procedures set forth by the agreement.

Termination of Agreement

This agreement shall remain in effect unless terminated by either agency upon thirty (30) days written notice. The agency terminating the agreement must also formally notify the WSP ACCESS Section within the thirty (30) days.

Agency Providing Criminal Justice Service(s):	SNOPAC 911	
ORI:	WA0310130N	
Agency Head Name (printed):	KURT MILLS	
Agency Head Signature:		Date: 11/9/16

Agency Receiving Criminal Justice Service(s):	City of Everett Prosecutor's Office	
ORI:	WA031031A	
Agency Head Name (printed):	James D. Iles	
Agency Head Signature:		Date: 11/3/16

Management Control Agreement
Must be completed by agencies who:

A. Have a city or county Information Technology (IT) department handling IT services for the criminal justice agency.

Pursuant to the CJIS Security Policy, it is agreed that with respect to administration of that portion of computer systems and network infrastructure interfacing directly or indirectly with A Central Computerized Enforcement Service System (ACCESS) for the interstate exchange of criminal history/criminal justice information, the Criminal Justice Agency shall have the authority, via managed control, to set and enforce:

(1) Priorities.
(2) Standards for the selection, supervision, and elimination of access to personnel who may be tasked with working on or interfacing with any of the telecommunication systems or criminal justice systems/computers enumerated in paragraph three below.
(3) Policy governing operation of justice systems, computers, access devices, circuits, hubs, routers, firewalls, and any other components, including encryption, that comprise and support a telecommunications network and related criminal justice systems to include but not limited to criminal history record/criminal justice information, insofar as the equipment is used to process or transmit criminal justice systems information guaranteeing the priority, integrity, and availability of service needed by the criminal justice community.
(4) Restriction of unauthorized personnel from access or use of equipment accessing the State network.
(5) Compliance with all rules and regulations of the Criminal Justice Agency Policies and CJIS Security Policy in the operation of all information received.

Responsibility for management of security control shall remain with the criminal justice agency, as required by the CJIS Security Policy.

This agreement covers the overall supervision of all Criminal Justice Agency systems, applications, equipment, systems design, programming, and operational procedures associated with the development, implementation, and maintenance of any Criminal Justice Agency system to include NCIC Programs that may be subsequently designed and/or implemented within the Criminal Justice Agency.

Agency Providing IT Service(s):	City of Everett IT Department	
Agency Head Name (printed):	Steven L. Hellyer	
Agency Head Signature:		Date: 11-3-16

Criminal Justice Agency Receiving IT Service(s):	City of Everett Prosecutor's office	
ORI:	WA 031031A	
Agency Head Name (printed):	James D. Iles	
Agency Head Signature:		Date: 11/3/16

Information Exchange Agreement
Must be completed by agencies who:

A. Provide criminal justice information to contracted prosecutors.

An information exchange agreement describing the Criminal Justice Information (CJI) provided and/or received by an agency must be in place between the agency providing the information and the contracted prosecutor receiving the information.

1. Security Control: Each person receiving the information will maintain the information in a physically secure location and only authorized individuals will have access to the CJI. The information will not be left in the open for unauthorized individuals to view.
2. Misuse: Each person receiving the information will use the information for criminal justice purposes only. The information received is *not* to be used in any civil cases or disseminated to non criminal justice personnel.
3. Training: Each person receiving the information will be responsible to view the Basic Security Awareness Training once every two years. The training log will be provided by and maintained at the criminal justice agency providing the CJI for review at the audit.
4. Destruction: CJI shall be securely disposed of when no longer required and destroyed by shredding or incineration.

Services Provided (check all that apply):

☐ Criminal History ☐ Other CJI (describe):

_____

_____

Parties who enter into this agreement must adhere to the regulations set forth in the ACCESS/NCIC Operating Manuals and the CJIS Security Policy. This Information Exchange Agreement must be current and approved by the CJIS Systems Agency (CSA), the Washington State Patrol (WSP) before agencies adopt the policies and procedures set forth by the agreement.

Termination of Agreement
This agreement shall remain in effect unless terminated by either party upon thirty (30) days written notice.

Agency Providing Criminal Justice Information:		
ORI:		
Agency Head Name (printed):		
Agency Head Signature:		Date:

Contracted Prosecutor Receiving Criminal Justice Information:		
Contractor Name (printed):		
Contractor Signature:		Date:

City Named in the Contract		
Authorizing Name (printed):		
Authorizing Signature:		Date:

AGREED:

CITY OF EVERETT, WASHINGTON

By: Ray Stephanson, Mayor

Date: 11-3-2016

ATTEST:

Sharon Fuller, City Clerk

Date: 11-3-2016

APPROVED AS TO FORM:

James D. Iles, City Attorney

Date: 11/3/16

Agreement

EVERETT CITY COUNCIL AGENDA ITEM COVER SHEET

PROJECT TITLE:
Washington State Patrol ACCESS User Acknowledgement

	Briefing	COUNCIL BILL #	
	Proposed Action	Originating Department	Legal
	Consent	Contact Person	Leslie Tidball
11/2/16	Action	Phone Number	425 257 8512
	First Reading	FOR AGENDA OF	
	Second Reading		
	Third Reading		
	Public Hearing		
	Budget Advisory	Initialed by:	
		Department Head	
		CAA	cdp
		Council President	AM

Location	Preceding Action	Attachments	Department(s) Approval
		ACCESS User Agreement	Legal, IT

Amount Budgeted	-0-	
Expenditure Required	-0-	Account Number(s):
Budget Remaining	-0-	
Additional Required	-0-	

DETAILED SUMMARY STATEMENT:
Certified City of Everett Prosecutor employees are required to access Criminal Justice Information Services (CJIS) provided by the Washington State Patrol. The City of Everett Prosecutors Office must abide by certain rules in order to maintain the highest levels of security of this information. The Washington State Patrol requires all agencies with access to CJIS information to sign an ACCESS User Acknowledgement.

RECOMMENDATION (Exact action requested of Council): Authorize the Mayor or his designee to sign the Washington State Patrol ACCESS User Acknowledgement agreement.

Council Approved on 11/2/2016 SZ