Terminal Agency Coordinator Responsibilities

Being the Terminal Agency Coordinator (TAC) for an agency comes with a lot of different tasks.

- Act as the point of contact for your agency
- Maintain Level 2 certification
- Ensure that all assistant TACs are level 2 certified
- Read the **Introduction Chapter** of the ACCESS Operations Manual
- Must attend one New TAC Training session within six months of assignment and TAC Review every three years there after
- Ensure monthly validations are completed (if applicable)
- Advise ACCESS of all users that are new to your agency
- Advise ACCESS of all users that have left your agency
- Ensure all ACCESS users maintain a current certification
- Ensure accuracy of your agency's records (if applicable)
- Perform recommended self-audits
- Complete a **Memo 550** to inform ACCESS of any agency related updates (e.g. TAC change, agency head change, IT point of contact change, email address, phone numbers, agency address change, etc.)
- Maintain current and updated formal written procedures for your agency. Under the ***Forms Tab*** on the **ACCESS webpage** there are templates for both the Criminal Justice Agency (CJA) and Non-Criminal Justice Agency (NCJA) that contain the current required information.

Important links for TACs:

- CJIS Launchpad: CJIS Launch Pad
- nexTEST: nexTEST - CJIS Testing
- CJIS Online: CJIS Online
- CJIS Validations: CJIS Validations
- CJIS Audit: CJIS Audit

If you have any questions, please contact the ACCESS Section
(360) 534-2010
ACCESS@wsp.wa.gov
ACCESS - Washington State Patrol

Audit Process

The National Crime Information Center (NCIC) requires Triennial (every three years) audits conducted by the Criminal Justice Security System Agency (CSA). The Washington State Patrol (WSP) conducts audits to review NCIC standards of compliance and provide recommendations for best business practices.

WSP provides three types of audits:

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

   - TAC responsibilities
   - ACCESS certification
   - Security Awareness Training
   - System Security
   - System Administration
   - Media Protection
   - Criminal History
   - Secondary Dissemination
   - N-DEx inquiries (*if applicable*)
   - National Instant Criminal Background Check System (NICS)
   - Random samples of Missing Persons, Warrants, & Protection Orders in NCIC/WACIC
   - Record maintenance
   - 2nd party checks
   - Hit Confirmation
   - ORI usage and administration of criminal justice functions
   - All applicable agreements
   - Written procedures
   - Validations
   - Site security visits to ensure terminal locations are secure

2. **Data Quality Review**
   WSP auditor's conduct an on-site data quality review for agencies that enter records. Auditors compare NCIC/WACIC 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. Auditors categorize these records are follows:
   - **Invalid:** The record must be removed from NCIC/WACIC.
   - **Inaccurate:** Fields in the NCIC/WACIC entry do not match the case file.
   - **Incomplete:** Missing information in the NCIC/WACIC entry.
   - **Unable to locate:** Case file cannot be found for the NCIC/WACIC entry.

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.

4. **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 being conducted with the agency technical point of contact by the WSP technical security auditors, with guidance from the Information Security Office (ISO).

nexTEST and CJIS Online

Please ensure that you read the TAC nexTEST Guide and the CJIS Online User Guide for additional information. TACs can utilize the ACCESS Webpage for all ACCESS related documents, manuals and self-paced trainings.

nexTEST – All ACCESS Users

- TACs must advise WSP of all new users requiring ACCESS. Please send an email to ACCESS@wsp.wa.gov that includes:
    1. First and last name
    2. SID number
    3. ORI
    4. ACCESS Level
- ACCESS will advise the TAC when the new user(s) has been added and send a follow-up email that will include the user ID's and instructions to complete the certification.
- All new users must log into nexTEST to view the **Security Awareness Training** and pass the **Security Awareness Test**. Once completed, the user is able to take the **ACCESS Certification Training** and **Test**, which is now fully online and self-paced.
    - All ACCESS certified users must recertify **annually** (There are no grace periods or exceptions to this requirement).
    - Users can recertify any time within the annual time frame.
- Users will be able to complete all parts of training themselves online within NexTEST, at their own pace. TAC's no longer need to contact ACCESS if a user expires or fails their test. Any user that fails their test or fails to certify before their expiration date will need to retake the training and then the test will open for them to try again."
    - New, expired, or failed user must complete the **Security Awareness** portion of the training, before they are able to take the **ACCESS certification training and test**.
- TACs must advise ACCESS anytime a user leaves the agency (transfers, quits, retires, etc.)
- By using the *Agency Login, TACs* have the ability to log into nexTEST to track their agency user certification expirations, by clicking the *Reports → Certification Status Report*.
    - TACs will also be notified by email on the 1st of every month for all users who will be expiring within the next 30-60 days.
- All certified users must sign in through the *User Login* button to view the Security Awareness and Recertification trainings and testing.

nexTEST and CJIS Online (Cont.)

CJIS Online – All Non-ACCESS Users

- All non-ACCESS certified users and unescorted personnel with access to Criminal Justice Information (CJI), like custodial or IT staff, must also view **Security Awareness Training** and **Test** annually, through CJIS Online.
- Agencies CJIS Online accounts are managed by the agency TAC
    - TACs are able to add, remove or edit users

Audit Cycle

15th ACCESS WACIC/NCIC Business Audit
6th ACCESS Technical Security Audit
4th ACCESS Non-Criminal Justice Audit

Month/Year	**County**
May 2025	Adams (01), Whitman (38)
June 2025	Chelan (04), Dougals (09), Okanogan (24)
July 2025	Benton (03), Franklin (11), Walla Walla (36)
August 2025	Benton (03), Franklin (11), Walla Walla (36)
September 2025	Snohomish (31)
October 2025	Snohomish (31)
November 2025	Grays Harbor (14)
January 2026	King (17)
February 2026	King (17)
March 2026	King (17)
April 2026	Lewis (21), Pacific (25), Wahkiakum (35)
May 2026	Clallam (05), Jefferson (16)
June 2026	Ferry (10), Pend Orielle (26), Stevens (33)
July 2026	Lincoln (22), Spokane (32)
August 2026	Lincoln (22), Spokane (32)
September 2026	Skagit (29)
October 2026	Island (15), San Juan (28)
November 2026	Cowlitz (08)
January 2027	Pierce (27)
February 2027	Pierce (27)
March 2027	Kitsap (18)
Apr 2027	Whatcom (37)
May 2027	Asotin (02), Columbia (07), Garfield (12)
June 2027	Grant (13)
July 2027	Kittitas (19)
August 2027	Yakima (39)
September 2027	Yakima (39)
October 2027	Clark (06)
November 2027	Mason (23)
January 2028	Thurston (34)
February 2028	Thurston (34)
March 2028	Thurston (34)
April 2028	Klickitat (20), Skamania (30)

The audit schedule is subject to change without advance notice.
If you have any questions, please contact the ACCESS Section at (360) 534-2010

WSP ACCESS USER ACKNOWLEDGMENT

As an agency head/director, I hereby acknowledge the duties and responsibilities as set forth in this WSP 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 Department of Licensing (DOL) may review activities of any person who receives drive, vehicle, vessel and firearm records information to ensure compliance with limitations imposed on the use of the information. The DOL may suspend or revoke, for up to five years, the privilege of obtaining information of a person found to be in violation of Revised Code of Washington (RCW) 42.56, RCW 46.52, RCW 46.22, RCW 46.12, or the user agreement with DOL. I understand that misuse of this information is subject to civil and criminal penalties punishable by fines or imprisonment under the Federal Drive Privacy Protection Act and RCW 46.12, RCW 46.22, RCW 46.52.

Agency Name:	*Starbucks PD*	
ORI:	*WASTESTORI*	
Agency Head Name (printed):	*Chief George Washington*	
Agency Head Email:	*ChiefofPD@StarbuckPD.org*	
Agency Head Telephone Number:	*555-555-1212*	
Agency Head Signature:		Date: 5/1/2023

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

24x7 Hit Confirmation Agreement

24x7 Hit Confirmation Agreements must be completed by agencies who:

A. Provide 24x7 teletype printer coverage for another agency.
B. Receive 24x7 teletype printer coverage from another agency.

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

Parties who enter into the 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 a thirty (30) day 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 authorized criminal justice facility.

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

Agency Providing 24x7 Coverage:	*Fictional Sheriff's Office (agency available 24/7)*	
ORI:	*WAFAKEORI*	
Agency Head Name (printed):	*Sheriff Fred Flintstone*	
Agency Head Signature:		Date: *5/1/2023*

Agency Receiving 24x7 Coverage:	*Starbucks PD (agency needing assistance)*	
ORI:	*WASTESTORI*	
Agency Head Name (printed):	*Chief George Washington*	
Agency Head Signature:		Date: *5/1/2023*

Holder of the Record Agreement

Holder of the Record Agreements must be completed by agencies who:

A. User their ORI to enter another agency's information.
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. The **holder of the record** is defined as the agency that is using their ORI to enter another agency's records. The **owner of the 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 the record under its NCIC assigned ORI on behalf of the owner of the record. As they relate to records entered for the owner of the record, the holder of the record assumes the following responsibilities: data entry; documentation; cancellation and modification of entries; timeliness of entries, clears, cancellation 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 the record must adhere to the regulations set forth in the ACCESS Operations Manual and the CJIS Security Policy. This HORA must be current and approved by the CJIS Systems Agency (CSA), the Washington State Patrol (WSP, before agencies adopt the policies set forth by the agreement.

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

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

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, completeness and timeliness.

Agency Acting as the Holder of the Record:	*Sheriff's Office (agency available 24/7)*	
ORI:	*WAFAKEORI*	
Agency Head Name (printed):	*Sheriff Fred Flintstone*	
Agency Head Signature:		Date: *5/1/2023*

Agency Acting as the Owner of the Record:	*Starbucks PD* (takes report & gives to above agency)	
ORI:	*WASTESTORI*	
Agency Head Name (printed):	*Chief George Washington*	
Agency Head Signature:		Date: *5/1/2023*

Inter-Agency Agreement

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.

Serviced provided (check all that apply):

- ☐ Hit Confirmation
- ☐ Dispatch
- ☐ Record Entry
- ☐ Record Validations
- ☐ Gun Transfers/Concealed Pistol Licenses (CPLs)
- ☐ Use of Regional Management System (RMS)
- ☐ Terminal connection to ACCESS
- ☐ Other services (Describe)

Other Services: _____

_____

Parties who enter into this agreement must adhere to the regulations set forth in the ACCESS Operations Manual and the CJIS Security Policy. This Inter-Agency 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 with the thirty (30) days.

Agency Providing Criminal Justice Service(s):	*911 Communications Center*	
ORI:	*WACOMM101*	
Agency Head Name (printed):	*Director Daisy Duck*	
Agency Head Signature:		Date: *5/1/2023*

Agency Receiving Criminal Justice Service(s):	*Starbucks PD*	
ORI:	*WASTESTORI*	
Agency Head Name (printed):	*Chief George Washington*	
Agency Head Signature:		Date: *5/1/2023*

Management Control Agreement

Must be completed by a criminal justice agency receiving services from a non-criminal justice agency (such as city, county or tribal information technology or record archive facility) and updated whenever either signatory change.

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 criminal history/criminal justice information by 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 (3) below.
3. Policy governing operation f 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 of 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 control of the criminal justice function remains solely 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 associates 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.

Non-Criminal Justice Agency Providing Service(s):	*City/County It*	
Agency Head Name (printed):	*Mickey Mouse*	
Agency Head Signature:		Date: *5/1/2023*

Criminal Justice Agency Receiving Service(s):	*Starbucks PD*	
ORI:	*WASTESTORI*	
Agency Head Name (printed):	*Chief George Washington*	
Agency Head Signature:		Date: *5/1/2023*

Attachment D-2 Management Control Agreement for Combined 911 Centers Only

Management Control Agreement for Personnel Determinations
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 and updated whenever either signatory change.

Agencies issues an ORI ending in 'N' are by NCIC definition, Non-Criminal Justice Agencies (NCJA) providing dispatch functions for a Criminal Justice Agency (CJA).

Therefore, pursuant to the CJIS Security Policy, it is agreed that with respect to personnel determinations for employees/contractors of 911 center interfacing directly or indirectly with A Central Computerized Enforcement Service System (ACCESS) for the interstate exchange of criminal justice/criminal justice information, the CJA shall have the authority, via managed control, to set and enforce:

1. Standards for the selection, supervision and elimination of access to criminal history/criminal justice information by personnel who may be tasked with working on or interfacing with any of the telecommunication systems or criminal justice systems/computers.
2. Restriction of unauthorized personnel from access or use of equipment accessing the State Network.

Responsibility for management control of the criminal justice functions above remain solely with the CJA, as required by the CJIS Security Policy.

This agreement requires personnel determinations be made by the CJA but does not allow the CJA to direct hiring or termination of 911 center personnel: only to approve/reject personnel from working on CJIS systems.

Combined 911 Center ORI:	*911 Communications Center*	
Agency Head Name (printed):	*Director Daisy Duck*	
Agency Head Signature:		Date: *5/1/2023*

Criminal Justice Agency ORI:	*WASTESTORI*	
Agency Head Name (printed):	*Chief George Washington*	
Agency Head Signature:		Date: *5/1/2023*

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 purposed 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 for viewing the Basic Security Awareness Training annually. The training log will be provided 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 Operations Manuals and the CHIS Security Policy. This information Exchange Agreement must be current and approved by the CJIS System 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 noticed.

Agency Providing Criminal Justice Information:	*Starbucks PD*	
ORI:	*WASTESTORI*	
Agency Head Name (printed):	*Chief George Washington*	
Agency Head Signature:		Date: *5/1/2023*

Contracted Prosecutor Receiving Criminal Justice Information:	*ABC Attorneys at Law*	
Contractor Name (printed):	*Walt Disney*	
Contractor Signature:		Date: *5/1/2023*

City Named in the Contract:	*Starbuck*	
Authorizing Name (printed):	*Mayor Oprah Winfrey*	
Authorizing Signature:		Date: *5/1/2023*

Addendum for a Criminal Justice Agency (CJA) using a Non-Criminal Justice Agency (NCJA) ORI must be completed by agencies who:

A. 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.

This addendum is added to the ACCESS User Acknowledgement for a Criminal Justice Agency (CJA) that has statutory Authority under Public Law 952-544 and/or 101-630 to request fingerprint based Criminal History Record Information (CHRI) checks to perform a Non-Criminal Justice (NCJA) function such as licensing, Guardian Ad Litem (GAL), Court Appointed Special Advocate (CASA) and other Non-Criminal Justice employment purposes under the public Laws listed.

Because the CJA must adhere to the CJIS Security Policy, the follow CJA policies and procedures cover the requirements normally provided by an NCJA, and do not need to be duplicated:

- Management Control Agreement and/or CJIS Security Addendums for contract personnel
- Physical protection
- Password management
- Disposal of media
- Data breach reporting

The CJA is still required to create, maintain and provide the following NCJA specific policies and procedures:

- NCJA Misuse
- Fingerprint Process

All fingerprint-based applicant submissions must include in the 'Reason Fingerprinted' field an accurate representation of the purpose and/o authority for which the CHRI is to be used.

The CJA must notify the applicant fingerprinted that the fingerprints will be used to check the criminal history records of the FBI. The agency making the determination of suitability for licensing or Non-Criminal Justice employment shall:

- Provide the applicants the opportunity to complete or challenged the accuracy of the information contained in the FBI identification record.
- Advise the applicants that procedures for obtaining a change, correction or updating of an FBI identification record are set forth in Title 28, C.F.R.16.34.

The agency should not deny the license or Non-Criminal Justice employment-based information in the record until the applicant has been afforded a reasonable time to correct or complete the record or has declined to do so.

Statutory Authority (check all that apply):

☐ PL 92-544 ☐ PL 101-630

Description of what fingerprint submissions are used for (CASA/GAL, City Ordinance #, non-criminal justice employment, etc.):

_____
_____

Criminal Justice Agency and ORI		
NCJA ORI:		
Agency Head Name (printed):		
Agency Head Signature:		Date:

ACCESS Pre-Audit Questionnaire:
National Instant Criminal Background Check System (NICS)

If your agency uses NICS, please have your NICS contributor complete the following information:

Agency Name:
ORI:
TAC:
NICS Contributor:

1. Does your agency process Concealed Pistol Licenses (CPL)?	YES	NO
a. Are you using NICS for these transactions? (PUR/14 and PUR/34)		
b. Confirm how you are advising the applicant that the fingerprints will be used to check criminal history, and they have the capability to review, update, correct, and challenge through the FBI? (NON-CRIMINAL JUSTICE APPLICANT'S PRIVACY RIGHTS) Please advise how this information is given to the applicant.		

2. Are you sending your Disposition of Firearms (DOF) (release of firearms from evidence) to WSP Firearms Background Division (FBD)?	YES	NO
a. Are you maintaining the NICS case number for a minimum of three years for audit purposes? (This is NOT done by FBD)		
b. Are you aware that the DOF function should not be used for any additional transactions (CPLS)?		

3. Are you performing Disposition of Firearms (DOF) (release of firearms from evidence)?	YES	NO
a. Are you using NICS for these transactions? (PUR/22, PUR/23, and PUR/24)		
b. Are you maintaining the NICS Transaction Number (NTN) and case number for a minimum of three years for audit purposes?		

4. Did you answer yes to any of the NICS questions above? If so, please answer the following questions:	YES	NO
a. Does your agency use the delay (NLN), denial (NDN), overturn (NDO), and proceed (NPN) message keys?		

b. If your agency denied on a prohibitor not found on your QNP/QNR response, are you entering the subject into the NICS Indices using the full first, middle, and last name?		
c. Does the agency maintain case files for all NICS denials?		
d. Is all documentation for denials that are overturned, destroyed within 24 hours?		

5. Does your agency enter into the NICS Indices? If so, please answer the following questions:	YES	NO
a. Are second party checks being conducted on all entries?		
b. Are all NICS Indices entries being entered complete and accurate?		
c. When NICS Indices entries are cancelled (automatically or manually), is the reason why it is or eventually will be cancelled being documented?		

6. Does your agency respond to U21 unsolicited message requests within 3 days?	YES	NO

NONCRIMINAL JUSTICE APPLICANT'S PRIVACY RIGHTS

As an applicant who is the subject of a national fingerprint-based criminal history record check for a noncriminal justice purpose (such as an application for employment or a license, an immigration or naturalization matter, security clearance, or adoption), you have certain rights which are discussed below. All notices must be provided to you in writing.[1] These obligations are pursuant to the Privacy Act of 1974, Title 5, United States Code (U.S.C.) Section 552a, and Title 28 Code of Federal Regulations (CFR), 50.12, among other authorities.

- **You must be provided an adequate written FBI Privacy Act Statement (dated 2013 or later) when you submit your fingerprints and associated personal information. This Privacy Act Statement must explain the authority for collecting your fingerprints and associated information and whether your fingerprints and associated information will be searched, shared, or retained.[2]**
- **You must be advised in writing of the procedures for obtaining a change, correction, or update of your FBI criminal history record as set forth at 28 CFR 16.34.**
- **You must be provided the opportunity to complete or challenge the accuracy of the information in your FBI criminal history record (if you have such a record).**
- **If you have a criminal history record, you should be afforded a reasonable amount of time to correct or complete the record (or decline to do so) before the officials deny you the employment, license, or other benefit based on information in the FBI criminal history record.**
- **If agency policy permits, the officials may provide you with a copy of your FBI criminal history record for review and possible challenge. If agency policy does not permit it to provide you a copy of the record, you may obtain a copy of the record by submitting fingerprints and a fee to the FBI. Information regarding this process may be obtained at https://www.fbi.gov/services/cjis/identity-history-summary-checks and https://www.edo.cjis.gov.**
- **If you decide to challenge the accuracy or completeness of your FBI criminal history record, you should send your challenge to the agency that contributed the questioned information to the FBI. Alternatively, you may send your challenge directly to the FBI by submitting a request via https://www.edo.cjis.gov. The FBI will then forward your challenge to the agency that contributed the questioned information and request the agency to verify or correct the challenged entry. Upon receipt of an official communication from that agency, the FBI will make any necessary changes/corrections to your record in accordance with the information supplied by that agency. (See 28 CFR 16.30 through 16.34.)**
- **You have the right to expect that officials receiving the results of the criminal history record check will use it only for authorized purposes and will not retain or disseminate it in violation of federal statute, regulation or executive order, or rule, procedure or standard established by the National Crime Prevention and Privacy Compact Council.[3]**

---

[1] Written notification includes electronic notification, but excludes oral notification.

[2] https://www.fbi.gov/services/cjis/compact-council/privacy-act-statement

[3] See 5 U.S.C. 552a(b); 28 U.S.C. 534(b); 34 U.S.C. § 40316 (formerly cited as 42 U.S.C. § 14616), Article IV(c); 28 CFR 20.21(c), 20.33(d) and 906.2(d).

Privacy Act Statement

This privacy act statement is located on the back of the FD-258 fingerprint card.

Authority: The FBI's acquisition, preservation, and exchange of fingerprints and associated information is generally authorized under 28 U.S.C. 534. Depending on the nature of your application, supplemental authorities include Federal statutes, State statutes pursuant to Pub. L. 92-544, Presidential Executive Orders, and federal regulations. Providing your fingerprints and associated information is voluntary; however, failure to do so may affect completion or approval of your application.

Principal Purpose: Certain determinations, such as employment, licensing, and security clearances, may be predicated on fingerprint-based background checks. Your fingerprints and associated information/biometrics may be provided to the employing, investigating, or otherwise responsible agency, and/or the FBI for the purpose of comparing your fingerprints to other fingerprints in the FBI's Next Generation Identification (NGI) system or its successor systems (including civil, criminal, and latent fingerprint repositories) or other available records of the employing, investigating, or otherwise responsible agency. The FBI may retain your fingerprints and associated information/biometrics in NGI after the completion of this application and, while retained, your fingerprints may continue to be compared against other fingerprints submitted to or retained by NGI.

Routine Uses: During the processing of this application and for as long thereafter as your fingerprints and associated information/biometrics are retained in NGI, your information may be disclosed pursuant to your consent, and may be disclosed without your consent as permitted by the Privacy Act of 1974 and all applicable Routine Uses as may be published at any time in the Federal Register, including the Routine Uses for the NGI system and the FBI's Blanket Routine Uses. Routine uses include, but are not limited to, disclosures to: employing, governmental or authorized non-governmental agencies responsible for employment, contracting, licensing, security clearances, and other suitability determinations; local, state, tribal, or federal law enforcement agencies; criminal justice agencies; and agencies responsible for national security or public safety.

As of 03/30/2018

See Page 2 for Spanish translation.

DERECHOS DE PRIVACIDAD DE SOLICITANTES - JUSTICIA, NO CRIMINAL

Como solicitante sujeto a una indagación nacional de antecedentes criminales basado en huellas dactilares, para un propósito no criminal (tal como una solicitud para empleo o una licencia, un propósito de inmigración o naturalización, autorización de seguridad, o adopción), usted tiene ciertos derechos que se entablan a continuación. Toda notificación se le debe proveer por escrito.[1] Estas obligaciones son de acuerdo al Privacy Act of 1974, Title 5, United States Code (U.S.C.) Section 552a, y Title 28 Code of Federal Regulations (CFR), 50.12, entre otras autorizaciones.

- **Se le debe proveer una Declaración de la Ley de Privacidad del FBI (con fecha de 2013 o más reciente) por escrito cuando presente sus huellas digitales e información personal relacionada. La Declaración de la Ley de Privacidad debe explicar la autorización para tomar sus huellas digitales e información relacionada y si se investigarán, compartirán, o retendrán sus huellas digitales e información relacionada.[2]**
- **Se le debe notificar por escrito el proceso para obtener un cambio, corrección, o actualización de su historial criminal del FBI según delineado en el 28 CFR 16.34.**
- **Se le tiene que proveer una oportunidad de completar o disputar la exactitud de la información contenida en su historial criminal del FBI (si tiene dicho historial).**
- **Si tiene un historial criminal, se le debe dar un tiempo razonable para corregir o completar el historial (o para rechazar hacerlo) antes de que los funcionarios le nieguen el empleo, licencia, u otro beneficio basado en la información contenida en su historial criminal del FBI.**
- **Si lo permite la política de la agencia, el funcionario le podría otorgar una copia de su historial criminal del FBI para repasarlo y posiblemente cuestionarlo. Si la política de la agencia no permite que se le provea una copia del historial, usted puede obtener una copia del historial presentando sus huellas digitales y una tarifa al FBI. Puede obtener información referente a este proceso en https://www.fbi.gov/services/cjis/identity-history-summary-checks y https://www.edo.cjis.gov.**
- **Si decide cuestionar la veracidad o totalidad de su historial criminal del FBI, deberá presentar sus preguntas a la agencia que contribuyó la información cuestionada al FBI. Alternativamente, puede enviar sus preguntas directamente al FBI presentando un petición por medio de .https://www.edo.cjis.gov. El FBI luego enviará su petición a la agencia que contribuyó la información cuestionada, y solicitará que la agencia verifique o corrija la información cuestionada. Al recibir un comunicado oficial de esa agencia, el FBI hará cualquier cambio/corrección necesaria a su historial de acuerdo con la información proveída por la agencia. (Vea 28 CFR 16.30 al 16.34.)**
- **Usted tiene el derecho de esperar que los funcionarios que reciban los resultados de la investigación de su historial criminal lo usarán para los propósitos autorizados y que no los retendrán o diseminarán en violación a los estatutos, normas u órdenes ejecutivos federales, o reglas, procedimientos o normas establecidas por el National Crime Prevention and Privacy Compact Council.[3]**

---

1 La notificación por escrito incluye la notificación electrónica, pero excluye la notificación verbal.

2 https://www.fbi.gov/services/cjis/compact-council/privacy-act-statement

3 Vea 5 U.S.C. 552a(b); 28 U.S.C. 534(b); 34 U.S.C. § 40316 (anteriormente citada como 42 U.S.C. § 14616), Article IV(c); 28 CFR 20.21(c), 20.33(d) y 906.2(d).

Declaración de la Ley de Privacidad

Esta declaración de la ley de privacidad se encuentra al dorso del FD-258 tarjeta de huellas digitales.

Autoridad: La adquisición, preservación, e intercambio de huellas digitales e información relevante por el FBI es autorizada en general bajo la 28 U.S.C. 534. Dependiendo de la naturaleza de su solicitud, la autoridad incluye estatutos federales, estatutos estatales de acuerdo con la Pub. L. 92-544, Órdenes Ejecutivas Presidenciales, y reglamentos federales. El proveer sus huellas digitales e información relevante es voluntario; sin embargo, la falta de hacerlo podría afectar la terminación o aprobación de su solicitud.

Propósito Principal: Ciertas determinaciones, tal como empleo, licencias, y autorizaciones de seguridad, podrían depender de las investigaciones de antecedentes basados en huellas digitales. Se les podría proveer sus huellas digitales e información relevante/ biométrica a la agencia empleadora, investigadora, o responsable de alguna manera, y/o al FBI con el propósito de comparar sus huellas digitales con otras huellas digitales encontradas en el sistema Next Generation Identification (NGI) del FBI, o su sistema sucesor (incluyendo los depósitos de huellas digitales latentes, criminales, y civiles) u otros registros disponibles de la agencia empleadora, investigadora, o responsable de alguna manera. El FBI podría retener sus huellas digitales e información relevante/biométrica en el NGI después de terminar esta solicitud y, mientras las mantengan, sus huellas digitales podrían continuar siendo comparadas con otras huellas digitales presentadas a o mantenidas por el NGI.

Usos Rutinarios: Durante el procesamiento de esta solicitud y mientras que sus huellas digitales e información relevante/biométrica permanezcan en el NGI, se podría divulgar su información de acuerdo a su consentimiento, y se podría divulgar sin su consentimiento de acuerdo a lo permitido por la Ley de Privacidad de 1974 y todos los Usos Rutinarios aplicables según puedan ser publicados en el Registro Federal, incluyendo los Usos Rutinarios para el sistema NGI y los Usos Rutinarios Generales del FBI. Los usos rutinarios incluyen, pero no se limitan a divulgación a: agencias empleadoras gubernamentales y no gubernamentales autorizadas responsables por emplear, contratar, licenciar, autorizaciones de seguridad, y otras determinaciones de aptitud; agencias de la ley locales, estatales, tribales, o federales; agencies de justicia penal; y agencias responsables por la seguridad nacional o seguridad pública.

A partir de 30/03/2018

PROTECTION ORDERS AND FEDERAL FIREARMS PROHIBITIONS

Persons subject to a qualifying protection order under federal law are generally prohibited from possessing any firearm or ammunition in or affecting commerce (or shipping or transporting any firearm or ammunition in interstate or foreign commerce, or receiving any such firearm or ammunition). Violation of this prohibition while the order remains in effect is a federal offense punishable by up to ten years imprisonment. Title 18 U.S.C. §§ 922(g)(8), 924(a)(2).

A qualifying court order may be issued by a criminal court or a civil court, such as divorce court, family court, magistrate or general jurisdicition court. The following list enumerates the elements that define a qualifying protection order under the Federal firearms prohibition. ***Generally, a defendant/respondent subject to a protection order that includes one element (indicated by a diamond) from each section listed below is covered by the Federal firearms prohibition.***

I. HEARING

- ❖ Defendant/Respondent received **actual notice** and had an **opportunity to participate**.

II. INTIMATE PARTNER

Plaintiff/Petitioner is an **intimate partner** of the Defendant/Respondent, (18 U.S.C. § 921(a)(32)). **An intimate partner may include**:

- ❖ A **spouse** or **former spouse** of the Defendant/Respondent;
- ❖ A person who **cohabitates or who has cohabitated** with the Defendant/Respondent (i.e., who resides/resided together in sexual/romantic relationship); or
- ❖ A person with whom the Defendant/Respondent **has or had a child in common** (regardless of whether they ever married or cohabitated).

III. RESTRAINS FUTURE CONDUCT

- ❖ The order **restrains** Defendant/Respondent from **harassing, stalking,** or **threatening** the intimate partner, child of the Defendant/Respondent, or child of the Defendant/Respondent's intimate partner; ***or***
- ❖ The order **restrains** Defendant/Respondent from engaging in other conduct that would place the intimate partner in **reasonable fear of bodily injury** to the partner or child.

IV. CREDIBLE THREAT OR PHYSICAL FORCE

- ❖ The order includes a finding that Defendant/Respondent is a **credible threat** to the physical safety of the intimate partner or child; ***or***
- ❖ The order, by its terms, explicitly prohibits the use, attempted use, or threatened use of **physical force** against the intimate partner or child that would reasonably be expected to cause bodily injury.

FOR FURTHER INFORMATION ABOUT SECTION **922(g)(8)** OR FEDERAL FIREARMS PROHIBITIONS GENERALLY, CONTACT YOUR LOCAL FIELD DIVISION OF THE BUREAU OF ALCOHOL, TOBACCO, FIREARMS AND EXPLOSIVES BY CALLING **1-800-800-3855,** OR VISIT WWW.ATF.GOV/FIELD/. FOR FURTHER INFORMATION ABOUT DOMESTIC VIOLENCE, PLEASE CONTACT THE NATIONAL CENTER ON PROTECTION ORDERS AND FULL FAITH AND CREDIT AT **1-800-903-0111,** PROMPT **2,** OR VISIT THEIR WEB SITE AT WWW.BWJP.ORG.

ATF Information 3310.2
Revised September 2011

PROTECTION ORDERS AND FEDERAL FIREARM PROHIBITIONS
QUALIFYING RELATIONSHIPS UNDER 18 UNITED STATES CODE (U.S.C.) SECTION 922 (g)(8)
and
SETTING THE BRADY INDICATOR (BRD) IN THE NATIONAL CRIME INFORMATION CENTER (NCIC) DATABASE

The NCIC Brady Indicator provides three choices: "Y" indicates the respondent is prohibited under federal law from possessing firearms, i.e., the order meets the criteria of 18 U.S.C. 922 (g)(8); "N" indicates the respondent is not prohibited under federal law from possessing firearms, i.e., the order does not meet the Title 18 Section 922 (g)(8) criteria; and "U" which indicates that it cannot be determined whether the respondent is federally prohibited from possessing firearms, i.e., it can't be determined if the order meets the federal criteria.

The "Protection Order" Prohibition in the Gun Control Act sets out specific relationships between the SUBJECT of a protection order and the PROTECTED PERSON. The federal firearm prohibition does not apply UNLESS the relationship falls within one of these categories. 18 U.S.C. 922 (g)(8) applies to a subject who is restrained from harming "an intimate partner of such person or child of such intimate partner or person."

Intimate Partner – With respect to a person, the spouse of the person, a former spouse of the person, an individual who is a parent of a child of the person, and an individual who cohabits or has cohabited with the person. ATF Regulations: 27 C.F.R. 178.11, *NCIC 2000 Manual Protection Order File, Section* 2.5 (3).

Cohabitation – Requires a live-in relationship (or former live-in relationship) between two (2) individuals (can be same sex) which, in essence, is a sexual/romantic one, ***NOT*** *merely a roommate*.

The chart below contains relationships frequently encountered on protection orders and the appropriate determination for NCIC entry. Research should be conducted on all protection orders entered with a BRD of U (Unknown) to determine if clarifying information is available from the court, e.g., the petition may contain relationship details which don't appear in the order itself.

PROTECTED PERSON	SUBJECT	BRD		PROTECTED PERSON	SUBJECT	BRD
Spouse	Spouse	Y		Grandchild	Grandparent	N
Former-Spouse	Former-Spouse	Y		Grandparent	Grandchild	N
Unmarried Child in Common	Unmarried Child in Common	Y		Brother/Sister	Brother/Sister	N
Unmarried Currently or formerly living together unless documentation of cohabitation exists	Unmarried Currently or formerly living together unless documentation of cohabitation exists	U		Cousins	Cousins	N
Child	Parent	Y		Roommates	Roommates	N
Step-Child	Step-Parent	Y		Neighbors	Neighbors	N
Currently or formerly cohabiting	Currently or formerly cohabiting	Y		Step-Parent	Step-Child	N
Parent	Child	N		Boyfriend/Girlfriend Unless cohabitation exists	Boyfriend/Girlfriend Unless cohabitation exists	N
Nephew/Niece	Uncle/Aunt	N		Same sex cohabiting, intimate relationship	Same sex, cohabiting, intimate relationship	Y
Uncle/Aunt	Nephew/Niece	N		Stranger	Stranger	N

RCW 7.105.325: NICS Indices Entry for Protection Orders

This e-mail is to notify your agency of the addition of a new SPC code for the National Instant Criminal Background Check System (NICS) Indices. As of July 1, 2022, based on RCW 7.105.325, law enforcement agencies (LEA) in Washington State are required to enter protection orders with firearm restrictions into the NICS Indices, in addition to the Washington Crime Information Center (WACIC)/National Crime Information Center (NCIC).

Legislation in 2022 resulted in significant updates to protection orders in Washington State. Some of these changes include:

- A new chapter, RCW 7.105, for protection orders
- Protection orders were combined into a single form
- Law enforcement agencies are now required to enter protection orders with firearm restrictions into the NICS Indices

The intent of the NICS Indices is to capture records that are not entered into NCIC, WACIC and a person's criminal history. These entries can be automatically denying for firearm purposes. Due to the change within Engrossed Second Substitute House Bill 1320, RCW 7.105.325 now includes verbiage that requires Washington LEAs to enter protection orders from the court with firearm restrictions into the NICS Indices for the length of the protection order, even if they have already been entered into WACIC/NCIC. Based on this RCW, **protection orders not issued under RCW chapter 7.105 do not require entry into the NICS Indices.** This means your agency does not need to add to the NICS Indices protection orders issued prior to July 1st, 2022, because RCW chapter 7.105 was not yet in effect.

RCW 7.105.325

Entry of protection order data—Other than for extreme risk protection orders.

(1) The clerk of the court shall enter any protection order, including temporary protection orders, issued under this chapter into a statewide judicial information system on the same day such order is issued, if possible, but no later than the next judicial day.

(2) A copy of a protection order granted under this chapter, including temporary protection orders, must be forwarded immediately by the clerk of the court, by electronic means if possible, to the law enforcement agency specified in the order. Upon receipt of the order, the law enforcement agency shall immediately enter the order into any computer-based criminal intelligence information system available in this state used by law enforcement agencies to list outstanding warrants. The order must remain in the computer until the expiration date specified on the order. If the court has entered an order that prohibits the respondent from possessing or purchasing a firearm, the law enforcement agency shall also enter the order into the national instant criminal background check system and any other federal or state computer-based systems used by law enforcement or others to identify prohibited purchasers of firearms. The order must remain in each system for the period stated in the order, and the law enforcement agency shall only expunge orders from the systems that have expired or terminated. Entry into the computer-based criminal intelligence information system constitutes notice to all law enforcement agencies of the existence of the order. The order is fully enforceable in any county in thestate.

(3) The information entered into the computer-based criminal intelligence information system must include notice to law enforcement on whether the order was personally served, served by electronic means, served by publication, or served by mail.

(4) If a law enforcement agency receives a protection order for entry or service, but the order falls outside the agency's jurisdiction, the agency may enter and serve the order or may immediately forward it to the appropriate law enforcement agency for entry and service, and shall provide documentation back to the court verifying which law enforcement agency has entered and will serve the order.

RCW 7.105.350

Reporting of orders—Extreme risk protection orders.

(1) The clerk of the court shall enter any extreme risk protection order, including temporary extreme risk protection orders, issued under this chapter into a statewide judicial information system on the same day such order is issued, if possible, but no later than the next judicial day.

(2) A copy of an extreme risk protection order granted under this chapter, including temporary extreme risk protection orders, must be forwarded immediately b the clerk of the court, by electronic means if possible, to the law enforcement agency specified in the order. Upon receipt of the order, the law enforcement agency shall immediately enter the order into the national instant criminal background check system, any other federal or state computer-based systems used by law enforcement or others to identify prohibited purchasers of firearms, and any computer-based criminal intelligence information system available in this state used by law enforcement agencies to list outstanding warrants. The order must remain in each system for the period stated in the order, and the law enforcement agency shall only expunge orders from the systems that have expired or terminated. Entry into the computer-based criminal intelligence information system constitutes notice to all law enforcement agencies of the existence of the order. The order is fully enforceable in any county in the state.

(3) The information entered into the computer-based criminal intelligence information system must include notice to law enforcement whether the order was personally served, served by electronic means, served by publication, or served by mail.

(4) If a law enforcement agency receives a protection order for entry or service, but the order falls outside the agency's jurisdiction, the agency may enter and serve the order or may immediately forward it to the appropriate law enforcement agency for entry and service, and shall provide documentation back to the court verifying which law enforcement agency has entered and will serve the order.

(5) The issuing court shall, within three judicial days after the issuance of any extreme risk protection order, including a temporary extreme risk protection order, forward a copy of the respondent's driver's license or identicard, or comparable information, along with the date of order issuance, to the department of licensing. Upon receipt of the information, the department of licensing shall determine if the respondent has a concealed pistol license. If the respondent does have a concealed pistol license, the department of licensing shall immediately notify a law enforcement agency that the court has directed the revocation of the license. The law enforcement agency, upon receipt of such notification, shall immediately revoke the license.

(6) If an extreme risk protection order is terminated before its expiration date, the clerk of the court shall forward on the same day a copy of the termination order to the department of licensing and the law enforcement agency specified in the termination order. Upon receipt of the order, the law enforcement agency shall promptly remove the order from any computer-based system in which it was entered pursuant to subsection (2) of this section.

Entry into the NICS Indices

When entering into the NICS Indices your agency will use PCA H when the Brady criteria qualifies on a protection order. If the PCA code is anything other than J, these will be visible to all states regardless of state of purchase or state of residence as they are federally prohibiting.

If the order does not qualify for Brady but does qualify for PCO/07, you will use PCA code J. When PCA code J is entered, then the SPC code field is required. There are three different SPC codes that can be used when PCO/07 applies: WA0007, WACR01, and the newest SPC Code, CRTORD.

- **WA0007 – 9.41.040(2)(a)(iv)**
  - This is used when the court order qualifies for PCO/07 based on RCW9.41.040(2)(a)(iv).
  - If you are entering under WA0007, full faith and credit will not apply.
  - In addition, records entered under WA0007 will only be visible to an out of state LEA (including FBI NICS) when the state of purchase or state of residence is Washington.
- **WACR01 – WA Court-ordered restriction**:
  - This is used when the court ordered firearm restrictions. This is solely based on statute and is not just limited to protection orders, this can be any court order with a firearm restriction.
  - If you are entering under WACR01, full faith and credit will not apply.
  - In addition, records entered under WACR01 will only be visible to an out of state LEA (including FBI NICS) when the state of purchase or state of residence is Washington.
- **CRTORD – Court Order Active and Valid**:
  - This is used when the court order itself prohibits firearms (see below for examples):

Firearms, Weapons, and Concealed Pistol License; Defendant:
[ ] do not, own, possess, or control a firearm. (RCW 9.41.040.)
[ ] do not access, obtain, or possess a firearm, other dangerous weapon, or concealed pistol license. (RCW 9.41.800.)
[ ] shall **immediately surrender** all firearms and other dangerous weapons within the defendant's possession or control and any concealed pistol license. Comply with the ***Order to Surrender and Prohibit Weapons*** filed separately. (RCW 9.41.800.)

[ ] For crimes not defined as a serious offense, the court makes the following mandatory findings pursuant to RCW 9.41.800(1) and (2): [ ] The defendant used, displayed, or threatened to use a firearm or other dangerous weapon in a felony; or [ ] The defendant is ineligible to possess a firearm pursuant to RCW 9.41.040; or [ ] Possession of a firearm or other dangerous weapon by the defendant presents a serious and imminent threat to public health or safety, or to the health or safety of any individual. (*If any of these boxes are checked, the court is required to order a weapons surrender under 9.41.800.*)

  - Enter with PCA/J, SPC/CRTORD to ensure full faith and credit is applied. This is a "universal" code and will be visible in every state, the District of Columbia and five US Territories.

CRTORD – Court Ordered Restriction has been added (to Omnixx) to the Enter NICS Indices Record (EDP) and Modify NICS Indices Record (MDP) forms.

SPC	DESCRIPTION
WA0007	RCW 9.41.040(2)(a)(iv)
WACR01	WA Court-ordered restriction
CRTORD	Court order active and valid

If your agency does not use Omnixx, you may need to speak with your regional management system (RMS) administrator to have this new SPC code added. The technical specs are attached.

For additional information, please refer to the ACCESS Operations Manual. If you have further questions, you may submit a work order to ITDHelp@wsp.wa.gov or email ACCESS@wsp.wa.gov.

We are continuing to gather information regarding legislative updates that affect NICS and will provide an e-mail with further SPC code and RCW updates shortly.

Brady – Federal Firearm Prohibitor

1. Hearing
   - Defendant received actual notice and had the opportunity to be heard
     - Was the order signed?
     - Was there a Proof of Service?
2. Intimate Partner
   - Federal qualifying relationships
   - Was relationship defined on the order?
3. Restrict Future Conduct
   - Does the order restrain from harassing, stalking, or threatening
     - Most orders meet this criteria (PCO/1)
4. Credible Threat **OR** Physical Force
   - Common words used are must not attack, assault, molest -anything physical

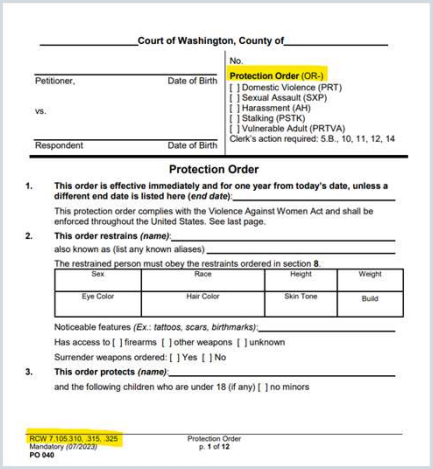
If all criteria are met: Brady = Yes

24

HB 1562 Updates as of 7/23/2023

RCW 9.41.040.2(a)(iv) has been updated to **9.41.040.2(a)(ii)**

- PCO/07 can only apply if it is a protection order, no contact order, or restraining order
- Orders can now be issued under RCWs **9A.40, 9A.44, 9A.88**



Court of Washington, County of

Petitioner, Date of Birth

vs.

Respondent Date of Birth

No.

Protection Order (OR-)

[ ] Domestic Violence (PRT)
[ ] Sexual Assault (SXP)
[ ] Harassment (AH)
[ ] Stalking (PSTK)
[ ] Vulnerable Adult (PRTVA)
Clerk's action required: 5.B., 10, 11, 12, 14

Protection Order

1. **This order is effective immediately and for one year from today's date, unless a different end date is listed here (*end date*):**
   This protection order complies with the Violence Against Women Act and shall be enforced throughout the United States. See last page.
2. **This order restrains (*name*):**
   also known as (list any known aliases)
   The restrained person must obey the restraints ordered in section 8.

Sex	Race	Height	Weight
Eye Color	Hair Color	Skin Tone	Build

Noticeable features *(Ex.: tattoos, scars, birthmarks)*:
Has access to [ ] firearms [ ] other weapons [ ] unknown
Surrender weapons ordered: [ ] Yes [ ] No

3. **This order protects (*name*):**
   and the following children who are under 18 (if any) [ ] no minors

RCW 7.105.310, .315, .325
Mandatory (07/2023)
PO 040

Protection Order
p. 1 of 12

25

PCO/07 – State Firearm Prohibitor

PCO/07 applies if:

A. **the subject is restricted under RCW 9.41.040.2(a)(ii):**
- Defendant received actual notice and had the opportunity to be heard
- Restrains future conduct to a **protected person** – no limitation to who protected person is
- Credible threat **OR** physical force
- It is **a protection order, no contact order, or restraining order issued under** RCW 7.105, 9A.46, **9A.40, 9A.44, 9A.88**, 10.99, 26.09, 26.26A, or 26.26B RCW or any of the former chapters 7.90, 7.92, 10.14, and 26.50

26

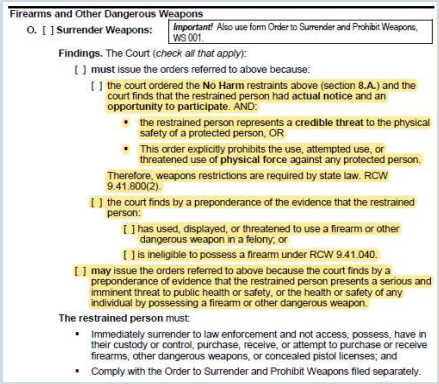
PCO/07 – State Firearm Prohibitor cont.

PCO/07 applies if:

B. There are any findings on the order stating that the individual cannot own, possess, or control a firearm

C. Order to Surrender form is included- RCW 9.41.800

Extreme Risk Protection Order
- Automatically restricts the subject's firearms rights
- Protection Order Condition (PCO) code entry is not required



Firearms and Other Dangerous Weapons

O. [ ] **Surrender Weapons:** **Important!** Also use form Order to Surrender and Prohibit Weapons, WS 001.

Findings. The Court (*check all that apply*):

[ ] **must** issue the orders referred to above because:

[ ] the court ordered the **No Harm** restraints above (section **8.A.**) and the court finds that the restrained person had **actual notice** and an **opportunity to participate**. AND:

- the restrained person represents a **credible threat** to the physical safety of a protected person, OR
- This order explicitly prohibits the use, attempted use, or threatened use of **physical force** against any protected person.

Therefore, weapons restrictions are required by state law. RCW 9.41.800(2).

[ ] the court finds by a preponderance of the evidence that the restrained person:

[ ] has used, displayed, or threatened to use a firearm or other dangerous weapon in a felony; or

[ ] is ineligible to possess a firearm under RCW 9.41.040.

[ ] **may** issue the orders referred to above because the court finds by a preponderance of evidence that the restrained person presents a serious and imminent threat to public health or safety, or the health or safety of any individual by possessing a firearm or other dangerous weapon.

The restrained person must:

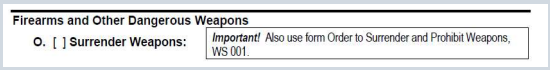
- Immediately surrender to law enforcement and not access, possess, have in their custody or control, purchase, receive, or attempt to purchase or receive firearms, other dangerous weapons, or concealed pistol licenses; and
- Comply with the Order to Surrender and Prohibit Weapons filed separately.

27

Order to Surrender (OTS) Proof of Surrender (POS)

OTS and POS field requirements:

- Did the court mark on the Protection Order "order to surrender weapons"?
  - Yes, then OTS = N
  - Unmarked, then OTS = N
- Is there a completed OTS form attached to the protection order?
  - Yes, then OTS = Y
  - No, then OTS = N
- Did your agency receive a completed POS form?
  - Yes, then POS = Y
  - No **and** no Declaration of Non-Surrender form, then POS = N
- Did your agency receive a completed Declaration of Non-Surrender form?
  - Yes, POS = Y
  - No **and** no POS form, then POS = N


Firearms and Other Dangerous Weapons

O. [ ] Surrender Weapons: *Important!* Also use form Order to Surrender and Prohibit Weapons, WS 001.

28

RCW 7.105.325: NICS Indices Entry for Protection Orders

Per ***RCW 7.105.325(2)*** "the law enforcement agency shall also enter the order into the national instant criminal background check system (NICS)"

If you have a protection order that qualifies for Brady and/or PCO/07, you must enter that order into WACIC/NCIC as usual <u>AND</u> also into the NICS Indices.

- Yes, this is repetitive
- Yes, you must re-enter into the NICS Indices if the order is extended and expires in NICS Indices
- Yes, you receive notice that the order will expire in the NICS Indices
- Yes, you must 2nd party check NICS Indices entries
- Yes, this does include ERPO (per RCW 7.105.350)
- No, NICS does not require validations
- No, will not be reviewing NICS Indices entries during your ACCESS Audit

For guidance for entries into the NICS Indices contact Firearms@wsp.wa.gov

29

RCW 7.105.325: NICS Indices Entries

Per ***RCW 7.105.325(2)*** "the law enforcement agency shall also enter the order into the national instant criminal background check system (NICS)"

If your agency is entering into the NICS Indices, there are a few items that will now be included during your triennial audit:

- Second Party checks must be conducted against all entries
  - All entries must be entered accurately, completely, timely, and exist
- When NICS Indices entries are cancelled (automatically or manually), the reason why it is or eventually will be cancelled needs to be documented
  - The WSP FBD has sent out a tool to track this if your agency would like
- Your agency must respond to U21 unsolicited message requests within 3 days

For guidance for entries into the NICS Indices contact Firearms@wsp.wa.gov

30