F.29.	7/6/2021

Subject:
Request Board Delegation: Memorandum of Understanding with the Department of Highway Safety Motor Vehicle Data and the Office of the State Courts Administrator.

Fiscal Impact:
none

Dept/Office:
Public Safety Group: Community Corrections

Requested Action:
It is requested the Brevard County Board of County Commissioners authorize the County Manager or his designee to sign the OSCA JIS-DHSMV Access Annual Certification Statement and the JIS Inter-Agency Agreement on behalf of Brevard County.

Summary Explanation and Background:
Brevard County Community Corrections (BCCC) oversees Pretrial Release (PTR) Services at the Brevard County Jail. Both PTR and BCCC employees require State certification for Limited Access to view criminal history information for the purpose of effectively conducting necessary job duties. This Certification and Limited Access is provided by the Office of the State Courts Administrator's Judicial Inquiry System (JIS).

The Judicial Inquiry System recently updated the web service connection to the Department of Highway Safety Motor Vehicle (DHSMV) DAVID data. Part of the process in making the connection required the Office of the State Courts Administrator (OSCA) to enter into a new Memorandum of Understanding (MOU) with DHSMV. To meet the requirements of the new MOU, each agency accessing DHSMV DAVID data through JIS will need to submit the OSCA JIS-DHSMV Access Annual Certification Statement within 15 days of signing the JIS Inter-Agency Agreement.

JIS management and general counsel require the signer of these documents be able to legally bind the user agency with his or her signature. Therefore, it is requested Brevard County Board of County Commissioners authorize the County Manager or his designee to sign said documents, annually. This request and supporting documents have been reviewed and coordinated with the County Attorney's office.

Clerk to the Board Instructions:
Submit to the Chair of the Brevard County Board of County Commissioners for signature.

BREVARD County

BOARD OF COUNTY COMMISSIONERS

FLORIDA'S SPACE COAST

Kimberly Powell, Clerk to the Board, 400 South Street ● P.O. Box 999, Titusville, Florida 32781-0999

Telephone: (321) 637-2001
Fax: (321) 264-6972
Kimberly.Powell@brevardclerk.us

July 7, 2021

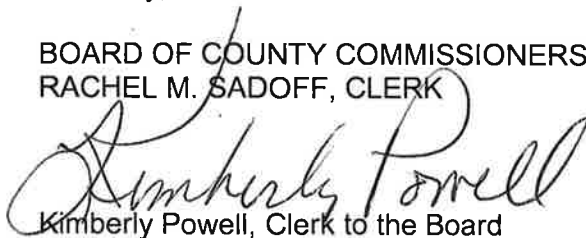M E M O R A N D U M

TO: Matthew Wallace, Public Safety Director

RE: Item F.29., Request for Memorandum of Understanding with the Department of Highway Safety Motor Vehicle (DHSMV) Data and the Office of the State Courts Administration (OSCA)

The Board of County Commissioners, in regular session on July 6, 2021, authorized the County Manager, or his designee, to execute the OSCA Judicial Inquiry System (JIS)-DHSMV Access Annual Certification Statement and the JIS Inter-Agency Agreement on behalf of Brevard County.

Your continued cooperation is always appreciated.

Sincerely,

BOARD OF COUNTY COMMISSIONERS
RACHEL M. SADOFF, CLERK

Kimberly Powell, Clerk to the Board

cc: County Manager

JUDICIAL INQUIRY SYSTEM (JIS) INTER-AGENCY AGREEMENT

This Agreement between the Office of the State Courts Administrator (OSCA) and

Agency Name

Agency Address

is for access to criminal history and other criminal justice-related information through the Judicial Inquiry System (JIS).

OSCA and the (Agency) agree as follows:

I. OSCA Obligations

A. OSCA, as administrator of the Judicial Inquiry System (JIS), will provide the Agency with access to data sources for official business purposes.

B. OSCA will provide access to the JIS at no cost to the Agency.

C. OSCA reserves the right to approve or deny all requests for access to JIS.

II. Agency Obligations

A. The Agency agrees to:

1. Abide by all terms and conditions stated in the User Agreement between the following:

   - Federal Bureau of Investigations (FBI) CJIS Security Policy
   - OSCA and Appriss Data User Agreement
   - OSCA and Department of Highway Safety and Motor Vehicle (DHSMV) Memorandum of Understanding
   - OSCA and Department of Juvenile Justice (DJJ) Memorandum of Understanding
   - OSCA and Florida Association of Court Clerks (FACC) Memorandum of Understanding
   - OSCA and Florida Department of Law Enforcement (FDLE) User Agreement

2. Access JIS for official business purposes only.

3. Abide by all local, state, and federal laws, policies, procedures, and regulations relating to access to and use of criminal justice information.

4. Establish internal policies and procedures to ensure that all users comply with agreements listed above.

5. Restrict use and dissemination of information obtained from JIS to performance of official business only in accordance with all applicable federal laws, state laws, court rules, and agreements listed above.

6. Maintain any information obtained from JIS in a location that will prohibit unauthorized access and destroy records containing such information in compliance with all applicable federal laws, state laws, court rules, and agreements listed above.

7. Allow only approved personnel to access to JIS.

8. Identify an FCIC Agency Coordinator (FAC), if applicable, and a Point of Contact (POC) who will approve user access to JIS.

   The POC/FAC's responsibilities include, but not limited to, the following:
   - Review and approve requests for JIS access based on users' job responsibilities.
   - Notify JIS Administrators immediately to inactivate user access following separation from the Agency, user reassignment that no longer requires access, negligent, improper, or unauthorized use or dissemination of any information.
   - Provide JIS Administrators with updated JIS Inter-Agency Agreement within thirty (30) days of change to the agency head, POC, and/or FAC. New accounts will not be set up until an updated agreement is fully executed
   - Monitor JIS user activity on an ongoing basis.
   - Ensure the Agency's JIS users comply with polices and requirements within this agreement.
   - Ensure the Agency's JIS users comply with internal agency policies that apply to JIS usage.
   - FAC must authorize each user's access to data sources that require CJIS certification or security awareness training.

9. Take steps to prevent a security breach caused by access and use of the site under this Agreement. If the Agency believes that there has been a breach of security the POC or FAC shall immediately notify OSCA JIS Administrators.

10. Maintain security updates to computers or systems that access JIS. Take precautions against viruses, worms or any other cyber security threats that may impact JIS.

11. Ensure data extracted from JIS that is stored or transmitted that is of confidential, private, or sensitive nature shall meet the Federal Bureau of Investigations (FBI) CJIS Security Policy encryption requirements. data source encryption requirements.

B. The Agency understands that violation of these terms and/or the below cited laws may result in immediate revocation of JIS access, possible civil and criminal prosecution, and/or further disciplinary procedures.

C. The Agency's failure to comply with laws, rules, and the user agreement shall constitute grounds for immediate termination of access. Access will remain revoked until the Agency complies with all rules and requirements.

D. Access and use of JIS is governed by all applicable state and federal law, including but not limited to, the confidentiality requirements contained in chapter 119, Florida Statutes, sections 119.10, 39.0132, 501.171, 815, 839.26, 943.053, 984.06, 985.04, and the Federal Driver's Privacy Protection Act.

E. The Agency must complete an DHSMV Annual Certification Statement to ensure proper and authorized use and dissemination of information and provide it to OSCA annually.

> **DHSMV Annual Certification Statement -** The Agency Party shall submit to the OSCA an annual statement indicating that the Agency has evaluated and certifies that it has adequate controls in place to protect the personal data from unauthorized access, distribution, use, modification, or disclosure, and is in full compliance with the requirements of this agreement and applicable laws. The Agency shall submit this statement annually, within fifteen (15) business days after the anniversary of the execution date of this agreement. Failure to timely submit the certification statement may result in an immediate termination of this agreement.

III. Other Terms and Conditions

A. OSCA is not responsible for the content of any linked site or any updates to links provided on JIS. Links on JIS will enable the Agency to leave JIS and are provided as a convenience for the individual user. The inclusion of links does not imply any endorsement by OSCA.

B. Either party may terminate this agreement upon thirty (30) days written notice to the other party. OSCA may terminate this agreement without notice if the Agency fails to comply with the terms of this agreement.

C. This agreement constitutes the entire agreement of the parties and may not be modified without written agreement executed by both parties.

D. This agreement is valid for three (3) years after the date of OSCA execution.

E. Failure to submit a newly signed agreement upon request from JIS Administrators shall result in revocation of access until such time that a signed agreement is received.

F. The Agency and OSCA agree that this Agreement is subject to the provisions of section 768.28, Florida Statutes.

JIS Point of Contact (POC):

POC Name		POC Phone:
POC E-mail Address		
POC Signature		Date:

Additional POC Name (optional)		POC Phone:
POC E-mail Address		
POC Signature		Date:

Additional POC Name (optional)		POC Phone:
POC E-mail Address		
POC Signature		Date:

Additional POC Name (optional)		POC Phone:
POC E-mail Address		
POC Signature		Date:

Additional POC Name (optional)		POC Phone:
POC E-mail Address		
POC Signature		Date:

FDLE FCIC Agency Coordinator (FAC):
(Required for authorizing access to data sources which require FDLE training/certification)

FAC Name		FAC Phone:
FAC E-mail Address		
FAC Signature		Date:

Agency Head Approval:

Agency Head Name	
Agency Head Title	
Agency Head Signature		Date:

OSCA Approval:

OSCA Address	500 South Duval Street, Tallahassee, Florida 32399-1900
OSCA Official's Name	Roosevelt Sawyer, Jr.
OSCA Official's Title	State Courts Technology Officer
OSCA Official Signature		Date:

OSCA JUDICIAL INQUIRY SYSTEM (JIS) USER ACCESS APPLICATION

Clear Form

Name: asfasfds sfsfdsf	Job Title: sfsdfsfsd ssdfsdf
Agency E-mail: ssdsfsdfdsf	Business Phone: (555) 555-5555
Agency Name/Division: dgdgddfg dgdfgdsg dgdfg	Primary County: (select one)
User role: (select one) Other:	Check if role is Sworn but not listed in dropdown ☐	SSN for FCIC/NCIC: 123-45-6789

MUST BE APPROVED BY LOCAL AGENCY JIS POINT OF CONTACT (POC) OR FCIC AGENCY COORDINATOR (FAC)

The agency FAC confirms the user's certification status below <u>and</u> approves access to data sources which require such FDLE training/certification:

☑ CJIS Online Security Awareness training **(Level 2 or higher)**   ☑ CJIS Limited Access <u>or</u> Full Access certification

Permit access to the following data sources through JIS as needed based on the user's job duties:

☐ APPRISS	*Requires Security Awareness training, Limited Access, or Full Access cert.*
☐ CCIS	*Requires user's agency to provide the user with a copy of Florida Statute 815 "Computer-Related Crimes Act" for review prior to access.*
DAVID ○ <u>N</u>o Photo/Sig. ○ <u>Wi</u>th Photo/Sig. [Reset]	*Agency must review Florida Statute 322.142(4) to determine access. If DAVID access is required, please select only one option.*
☐ DJJ	*Requires Security Awareness training, Limited Access, or Full Access cert. Agency must review Florida Statute 985.04 to determine access.*
☐ DOC	*Requires Security Awareness training, Limited Access, or Full Access cert.*
☐ FCIC	*Requires Limited Access or Full Access cert. Includes FCIC Rap Sheet, FCIC/NCIC Hot Files, and FCIC/NCIC Protection Orders as applicable.*
☐ FCIC Florida Summary Rap Sheet	*Requires Limited Access or Full Access cert.*
☐ Florida Concealed Weapons Check	*Requires Limited Access or Full Access cert. Access restricted to Law Enforcement Agencies & State Attorney Offices.*
☐ NCIC	*Requires Limited Access or Full Access cert. Includes NCIC Rap Sheet and Out-of-State Driver License.*
SSN displayed in CCIS and DAVID responses ○ Full SSN ○ Last 4 digits [Reset]	*Agency must review Florida Statute 119.071(5) to determine access. If left unchecked, user will only see the last 4 digits in CCIS and DAVID responses.*
Active Warrant Alert Calendar System ○ Primary County view ○ Primary County Admin ○ Circuit view [Reset] ○ Circuit Admin	***LIMITED AGENCIES - CURRENTLY COLLIER AND LEE COUNTY ONLY*** *Requires Limited Access or Full Access cert.* *Admin access includes calendar modification capabilities* *Circuit access allows access to all counties in your judicial circuit*
VFOSC and HRSO e-mail notifications ○ Primary county ○ All counties within circuit [Reset] ○ Specific counties within circuit:	***OPTIONAL TO RECEIVE - LIMITED ACCESS BASED ON JOB DUTIES*** *Requires Security Awareness training Level 2 or higher.* *Violent Felony Offenders of Special Concern and High-Risk Sex Offenders*

FIRST APPEARANCE CALENDAR ACCESS

- Access to the First Appearance Calendar must be granted based on the user's job duties <u>and</u> that the user possesses the required FDLE CJIS Limited Access or Full Access certification.
- **All Criminal Justice agency calendar users will automatically have access to the following data sources:** CCIS, DAVID, DJJ, DOC, FCIC/NCIC Hot Files, FCIC Rap Sheet, FCIC Summary Rap Sheet, and NCIC Rap Sheet (and Out-of-State DL, if searches initiated by local agency calendar administrators).
- <u>NOTE: If calendar access is checked below, please ensure that the appropriate data sources listed above are selected on page 1.</u>

   ○ Primary County access

   ○ Primary County access with Administrative features (add, delete, modify)   [**Reset**]

   ○ Circuit access with Admin. features (display, add, delete, modify all counties in circuit).

TERMS OF USAGE

By signing below, I understand:

1. access to JIS is restricted to official business purposes.
2. personal use of JIS is prohibited.
3. it is my responsibility to safeguard my access to JIS, to encrypt my password if stored, to not allow other individuals access to my JIS logon credentials and allowing other users to use my computer while logged on is strictly prohibited.
4. I must log off the system after each use.
5. I must ensure unauthorized users do not have the ability to view my computer monitor
6. selling information obtained from JIS to any person, entity or governmental agency is prohibited
7. it is recommended that computing devices shall not be left unattended without enabling a password-protected screensaver that is activated after fifteen minutes of inactivity or logging off the device.
8. the confidential nature of the information received through JIS and will abide in accordance with the JIS Inter-Agency Agreement as updated.
9. access to JIS is subject to deactivation due to an extended period of inactivity. Reactivation of the account will require the submission of a new JIS user access application.
10. access to JIS is allowed only via an agency-issued device with a fully functioning operating system that meets FBI Criminal Justice Information Services (CJIS) Security Policy and FDLE CJIS Agency User Agreement as updated.
11. information obtained through the JIS shall not be made available for unauthorized public inspection.
12. I may be held responsible for inappropriate dissemination of any information obtained from JIS.
13. violation of these terms and/or the below cited laws may result in immediate revocation of my JIS access, termination of my employment, possible civil and criminal prosecution
14. access and use of JIS is governed by all applicable state and federal law, including but not limited to, the confidentiality requirements contained in chapter 119, Florida Statutes, sections 119.10, 39.0132, 501.171, 815, 839.26, 943.053, 984.06, 985.04, and the Federal Driver's Privacy Protection Act.
15. I shall not utilize an auto logon, application remembering, script or hard-coded password when logging into JIS.

I hereby acknowledge that any violation of these provisions or misuse of the system may result in civil and/or criminal prosecution pursuant to sections 775.082, 775.083, 775.084, Florida Statutes, Title 18 U.S.C. §§ 2723, 2724, Title 28 CFR § 20.25, and as otherwise provided for by law. I consent to monitoring, recording, and auditing of my usage of JIS that may occur without my knowledge or prior notice.

User Printed Name	**User Signature**	**Date**

By signing below, I authorize the user to utilize JIS and have confirmed with our FCIC Agency Coordinator (when applicable) that the user possesses the appropriate CJIS training/certification.

POC/FAC Printed Name	**POC/FAC Signature**	**Date**

Submit application to jis_support@flcourts.org. Digital signatures are acceptable. Please allow 10 business days upon receipt by JIS staff for processing.

"Clear Form" button	Located in the upper right corner of the form, click this button is you wish to clear all fields.
Name	**Required field.** Name of individual applying for access.
Job Title	**Required field.** User's agency job title.
Agency E-Mail	**Required field.** User's work email address.
Business Phone	**Required field.** User's work phone number. Enter using the following format: *555-555-5555*.
Agency Name/Division	**Required field.** User's agency and division, if applicable.
Primary County	**Required field.** The location of the office where the user works. If user works in multiple offices, please list the primary office.
User Role	**Required field.** Click to the drop-down list to select the role that best describes the user's position. Please review the entire list before selecting "Other." It is not necessary to enter any information in the free-text field to the right if you have selected the appropriate role from the drop-down list. Contact jis_support@flcourts.org if you are unsure which role to select. Only if a relevant role is NOT found, select "Other" and type a brief role description in the text field below the User role.
Check if role is Sworn but not listed in dropdown	If the applicant is working in a sworn capacity <u>and</u> we do not offer a corresponding "sworn" role in the drop-down list, please use this checkbox to indicate as such (sworn officers such as law enforcement, corrections, correctional probation, auxiliary law enforcement. Sworn officers have different levels of CCIS and DMV access versus support staff. http://www.fdle.state.fl.us/CJSTC/Officer-Requirements/How-to-Become-an-Officer.aspx
SSN for FCIC/NCIC	Required field only **if** the user's job duties require them to conduct FCIC/NCIC transactions. FDLE utilizes the SSN as the User Code to validate CJIS certification. Enter using the following format: *123-45-6789*

"Must be approved by local agency JIS Point of Contact (POC) or FCIC Agency Coordinator (FAC)" section:

The agency FAC confirms the user's certification status below <u>and</u> approves access to data sources which require such FDLE training/certification:	Select the level(s) of FDLE training/certification that the user possesses. This is used to determine their level of access to the system. Please note that certain data sources require minimum training/certification (see below). **Level 1** Security Awareness training is **insufficient** for utilizing JIS.
Permit access to the following data sources through JIS as needed based on the user's job duties	Place a check by each the data source the user will need to access through JIS in order to perform their job duties as determined by the agency.

➢ APPRISS	**Must possess the FDLE CJIS Security Awareness training, FDLE CJIS Limited Access certification, or FDLE CJIS Full Access certification to access this data source due to CJI data requirements.**
	
	NOT PERMITTED ACCESS:
	    ➢ Any agency that is restricted from receiving NCIC data (examples below):
	          o Attorney General Bureau of Victim Compensation
	          o Department of Children and Families Adult Protective Investigators
	          o Department of Children and Families Human Services
	          o Office of Criminal Conflict and Civil Regional Counsel
	          o Public Defenders
	
	This data source compiles information entered into jail booking applications throughout the country providing up-to-date arrest information as well as current booking images where available.

➢ CCIS	CCIS policy requires user's agency to provide the user a copy of Florida Statute 815 "Computer-Related Crimes Act" for review prior to access. This data source from the Florida Association of Court Clerks and Comptrollers provides current information on court cases for all 67 counties in Florida. In most cases a local clerk detail link is available on an individual case enabling users to go directly to the Clerk's website to view the progress docket; otherwise, the docket is available directly through the CCIS user interface in JIS.
➢ DAVID	Florida DHSMV policy requires POC or FAC to review Florida Statute 322.142(4) to determine if the user meets the qualifications to receive DHSMV photo/signature. Per DHSMV, non-criminal justice users are not permitted access to photos, signatures, and insurance policy numbers. To reset the selection, click on the RESET button. NOTE: User's driver license number is no longer required for DAVID access through JIS. This data source provides Florida driver history, vehicle, and vessel information as well as images. <u>Image and signature access are determined by statute and the user's agency.</u>
➢ DJJ	**Must possess the FDLE CJIS Security Awareness training, FDLE CJIS Limited Access certification, or FDLE CJIS Full Access certification to access this data source due to CJI data requirements.** DJJ policy allows access as outlined in Florida Statute 985.04. This data source provides information on Florida juvenile arrest, probation, commitments, dispositions, and juvenile booking photos on subjects under 24 years of age.
➢ DOC	**Must possess the FDLE CJIS Security Awareness training, FDLE CJIS Limited Access certification, or FDLE CJIS Full Access certification to access this data source due to CJI data requirements.** This data source provides information regarding the status of individuals who have been placed under the active supervision of the Florida Department of Corrections. It will also provide detailed information regarding arrest date, underlying offense and dates of supervision, and whether the individual is currently an absconder, active inmate, or released inmate.

➢ FCIC	**Requires FDLE CJIS Limited Access certification or FDLE CJIS Full Access certification.**
	Provides access to the FCIC Rap Sheet, FCIC/NCIC Hot Files, and FCIC/NCIC Protection Orders.
	
	NOT PERMITTED ACCESS TO THE NCIC PORTION OF THE HOT FILES AND PROTECTION ORDERS (examples below):
	    ➢ Any agency that is restricted from receiving NCIC data
	    ➢ Attorney General Bureau of Victim Compensation
	    ➢ Office of Criminal Conflict and Civil Regional Counsel
	
	FCIC – Rap Sheet: This data source provides the information regarding arrest history and disposition stored by the Florida Department of Law Enforcement. This is the traditional rap sheet providing detailed arrest information in order of oldest arrest first and most recent arrest last.
	
	FCIC – Hot Files: This data source provides information from the Florida Department of Law Enforcement regarding outstanding warrants, active-only protection orders, probationary statuses, as well as risk identifications such as, but not limited to, Violent Felony Offender of Special Concern (VFOSC), High Risk Sexual Offender (HRSO), Sexual Offender or Sexual Predator, and Habitual or Career Offender.
	
	NCIC – Hot Files: This data source provides information from the National Crime Information Center and the Interstate Identification Index regarding national warrants, active-only protection orders, sexual offender registrations, immigration violations, gang member alerts, terrorist alerts, and National Instant Criminal Background Check System (NICS) Denied Transaction File Notifications. Access to this information is not permitted by public defender staff or for civil-related functions not authorized by law.
	
	FCIC – Protection Orders (QPO): This data source provides information from the Florida Department of Law Enforcement and National Crime Information Center regarding Florida expired and cleared Protection Orders in addition to active Protection Orders. Access to the NCIC portion of this information is not permitted by public defender staff or for civil-related functions not authorized by law.
	
	NCIC – Protection Orders (QPO): This data source provides information from the National Crime Information Center regarding expired and cleared Protection Orders in addition to active Protection Orders from outside of Florida. Access to the NCIC portion of this information is not permitted by public defender staff or for civil-related functions not authorized by law.

➢ FCIC FL Summary Rap Sheet	**Requires FDLE CJIS Limited Access certification or FDLE CJIS Full Access certification.** Provides access to summarized Florida Rap Sheet. This data source provides information regarding arrest history and disposition stored by the Florida Department of Law Enforcement. This is a summarized format of the FCIC Rap Sheet that quantifies the arrest history listing total number of felony charges and convictions, total number of misdemeanor charges and convictions, total number of incarcerations, etc. The most recent arrest appears first, with the oldest arrest appearing last.
➢ FL Concealed Weapons Check	**Requires FDLE CJIS Limited Access certification or FDLE CJIS Full Access certification.** Provides access to Florida Concealed Weapons License information. RESTRICTION: Only local, state, and federal law enforcement and State Attorney offices are permitted access. This data source provides information on Florida concealed weapon license holders. Access to this information is allowed for the performance of lawful duties by law enforcement and state attorney staff only.

➤ NCIC	**Requires FDLE CJIS Limited Access certification or FDLE CJIS Full Access certification.**
	Provides access to the NCIC Rap Sheet and Out-of-State Driver License data.
	
	NOT PERMITTED ACCESS:
	    ➤ Any agency that is restricted from receiving NCIC data (examples below):
	        ○ Attorney General Bureau of Victim Compensation
	        ○ Department of Children and Families Adult Protective Investigators
	        ○ Department of Children and Families Human Services
	        ○ Office of Criminal Conflict and Civil Regional Counsel
	
	This data source provides information regarding all out-of-state and federal criminal history. Access to this information is not permitted by public defender staff or for civil-related functions not authorized by law.

SSN displayed in CCIS and DAVID responses	Used to determine if the user's job duties require access to view the full SSN or if they are limited to just the last 4 digits of the SSN in returned records specifically from CCIS and DAVID. If left unchecked, the user will only receive the last 4 of the SSN. To reset the selection, click on the RESET button.
Active Warrant Alert Calendar System (AWACS)	***LIMITED AGENCIES – CURRENTLY COLLIER AND LEE COUNTY ONLY*** Access to AWACS should be restricted to those individuals who are required by their agency to review criminal history information on individuals attending the related hearings. Reviewing this information must not be for curiosity, but with specific, justifiable purposes. Access to AWACS must be granted based on the user's job duties and that the user possesses required FDLE CJIS Limited Access certification or Full Access certification. To reset the selection, click on the RESET button. AWACS, a component of the Judicial Inquiry System (JIS), was implemented as a result of the Andrew Widman Act. It provides an automated link between JIS, the Clerks of Court Comprehensive Case Information System (CCIS), the FCIC/NCIC warrant information systems, the Appriss booking system, and law enforcement agencies charged with execution of warrants. AWACS performs automated searches on individuals scheduled to appear at court events subsequent to First Appearance and provides a merged criminal history record and automatic notification to criminal justice personnel of outstanding warrants, current incarcerations, and FCIC/NCIC status alerts (High Risk Sex Offender Alerts, Violent Felony Offender of Special Concern Alerts, Absconder Alerts, Immigration Violator Alerts, etc.).

Primary County view	Ability to view subjects scheduled for court for their primary county for dockets and judges identified to JIS Administrators.
Primary County Admin	Administrative access permits users to add subjects to their primary county's AWACS calendar and initiate a re-running of a docket.
Circuit view	Ability to view subjects scheduled for court for their circuit for dockets and judges identified to JIS Administrators.
Circuit Admin	Administrative access permits users to add subjects to any AWACS calendars within their circuit and initiate a re-running of a docket

VFOSC & HRSO email notifications	*OPTIONAL TO RECEIVE - LIMITED ACCESS BASED ON JOB DUTIES*
	Requires Security Awareness training Level 2 or higher.
	The JIS First Appearance calendar offers the option for CJIS-trained/certified (Level 2 or higher) users to receive email notifications when subjects who are flagged by FDLE or FDOC in FCIC as a Violent Felony Offender of Special Concern (VFOSC) and/ or High-Risk Sex Offender (HRSO) are fingerprinted. Emails should be restricted to personnel who must have access to this information as part of their job responsibilities.
	POCs and FACs are to inform JIS Support via email at jis_support@flcourts.org to have the user removed from notifications (e.g., job responsibilities changed, user separated from the agency).
	For more information of VFOSC and HRSO emails, please refer to the "JIS First Appearance Calendar User Manual."
	To reset the selection, click on the RESET button.

Primary County	JIS will only send email notifications originating from the user's primary county which should be identified at the top of page 1 of the application.
All counties within circuit	JIS will only send email notifications originating from all counties within the user's circuit.
Specific counties within circuit	JIS can send email notifications to the user from certain counties within their circuit as specified in this section of the application.

"First Appearance Calendar Access" section:

Access to the First Appearance Calendar must be restricted to those individuals who are required by their agency to review criminal history information on individuals attending First Appearance hearings. Reviewing this information must not be conducted for curiosity, but with specific, justifiable purposes.

Access to the First Appearance Calendar must be granted based on the user's job duties <u>and</u> that the user possesses required FDLE CJIS Limited Access certification or Full Access certification:

- **All Criminal Justice agency calendar users will <u>automatically</u> have access to the following data sources:**

  - CCIS
  - DAVID
  - DJJ
  - DOC
  - FCIC/NCIC Hot Files

  - FCIC Rap sheet
  - FCIC Summary Rap Sheet
  - NCIC Rap Sheet
  - Out-of-State DL (if searches are initiated by local agency calendar administrators)

Since access is automatically given to the data sources listed above, <u>please ensure that they are selected on page 1</u>.

Primary County access	Allows user to see first appearance data only for their county. Allows user to perform a re-query on the first appearance data only for their county.
Primary County access with Administrative features (add, delete, modify)	Allows user to see first appearance data only for their county. Allows user to perform a re-query on the first appearance data only for their county. Allows user to perform specific administrative functions only for their county such as adding and deleting subjects, modifying calendar cutoff times, and searching booking events (see JLA User Manual for details). Access to these features should limited to staff who manage their county's JIS calendar for First Appearance as changes made by the users will be seen by others who have access to that county's calendar.
Circuit access with Administrative features (displays all counties within circuit)	Allows user to see the first appearance data for all counties in their judicial circuit and perform re-queries on the first appearance data for all counties in their judicial circuit. All circuit wide access automatically includes administrative access. Allows user to perform specific administrative functions only for their county such as adding and deleting subjects, modifying calendar cutoff times, and searching booking events (see JLA User Manual for details). Access to these features should limited to staff who manage their circuit's JIS calendar for First Appearance as changes made by the users will be seen by others who have access to that circuit's calendars. Agencies authorizing circuit wide access may be asked to further justify the request due to the possibility of access crossing outside the user's jurisdiction.

User Acknowledgement section:

Terms of Usage ("By signing below, I understand...")	This section informs users of their responsibilities to safeguard information accessed from JIS and applicable penalties for violating terms of usage.
User Printed Name / User Signature / Date	**Required fields.** Each user must acknowledge by signature that they have read and understand the requirements and rules outlined in the Terms of Usage. Although we accept either electronic or digital signatures, we encourage the use of digital signatures as a more secure method since they require a password. **For more information or assistance on applying electronic and digital signatures, please contact your agency's IT department.** Enter date using the following format: *MM/DD/YYYY*.

640

POC/FAC authorization:

| POC/FAC Printed Name / Signature / Date | **Required Fields**
Either the user's agency POC or FAC may sign the form approving access to the system and confirming all selections made on the form.

By signing the application, the POC or FAC is:

1. Authorizing the user to utilize JIS.
2. Confirming that the user possesses the appropriate CJIS training/certification to access the APPRISS, DJJ, DOC, FCIC, and NCIC data sources as well as the JIS First Appearance Calendar.

NOTE: Points of Contact that do not serve as FCIC Agency Coordinators must communicate with their FAC (when applicable) to confirm the user's training/certification status.

For more information or assistance on applying electronic and digital signatures, please contact your agency's IT department.

NOTE: We also strongly encourage that the POC or FAC lock the document upon electronically/digitally signing the document PRIOR to submitting to JIS Support to prevent any unauthorized changes.

To lock the document, check the following setting presented by Adobe (see below screenshot): |
| | |

Sign Document   ✕

Sign As: 2025.03.20   ⌄   ⑦

Password:

Certificate Issuer: Info...

Appearance: Standard Text ⌄

⑦

☐ Lock Document After Signing   ⬅   ⑦

ⓘ   Click Review to see if document content may affect signing   Review...

Sign   Cancel

Enter date using the following format: *MM/DD/YYYY.*

Submission instructions	Submit application to jis_support@flcourts.org. They may be sent to JIS administrators' CJNet email addresses for purposes of encryption if the agency wishes; however, it must be sent from a CJNet account as well in order to maintain encryption. Although we accept either electronic or digital signatures, we encourage the use of digital signatures as a more secure method since they can require a password to apply a signature. Please allow 10 business days upon receipt of JIS administrators for processing.

Office of the State Courts Administrator

JUDICIAL INQUIRY SYSTEM (JIS) DEPARTMENT OF HIGHWAY SAFETY
AND MOTOR VEHICLE (DHSMV) ACCESS CERTIFICATION STATEMENT

Under penalty of perjury I have read the requirements contained in the
Memorandum of Understanding, Florida Administrative Code, Rule Chapter
60GG-2 (Formerly 74-2, FAC), and the Department of Highway
Safety and Motor Vehicles Vendor IT Security Policy and declare that the
following is true:

The Requesting Party,

(*Agency Name*)

hereby certifies that the Requesting Party has appropriate internal controls in
place to ensure that the data is protected from unauthorized access,
distribution, use, modification, or disclosure. This includes
policies/procedures in place for both personnel to follow and data security
procedures/policies to protect personal data. The data security
procedures/policies have been approved by a Risk Management IT Security
Professional or internal auditor.

Agency Head Signature

Printed Name

Title

Agency Name

Date