



CJIS-CT User Access and Authorization Instructions

Criminal Justice Information System
55 Farmington Avenue, Hartford, CT 06105
Telephone (860) 622-2000
CJIS.HelpDesk@ct.gov

Type of Access Requested

The CJIS-CT User Access and Authorization form is needed to request access and authorization for CISS, MVP, Judicial Online Communication Exchange (JOCE) and CR-39 Application. Check the corresponding box that matches the request for a user's Type of Access (new, modify, terminate).

Modify or Terminate: If you choose Modify or Terminate, provide the current User ID.

Modifying: If modifying a previous access/claims request in section 2 and 3, select all access/claims that apply, not just new requests. Un-selected access/claims will be removed from user's account, ie CISS Search, MVP, CR-39 and JOCE.

Judicial Applications: If you are requesting access for JOCE/CR-39 only, the form should be sent helpdesk@jud.ct.gov or your known judicial contact. Judicial will send the validated and completed form to cjis.helpdesk@ct.gov

Section 1 – CJIS-CT User Identification

- Enter the user's name, email address, phone, and FAX number.
- Enter the CJIS-CISS Identity Provider User Account Name – For Administrator Use Only
- Enter the Federated Identity Provider User Account Name – For Administrator Use Only
- Enter the user's Employer (Agency) or Police Department Name as noted below:

Agency	Employer Name	Employer Sub Unit Name
Board of Pardons and Paroles	BOPP	N/A
Court Support Services Division	CSSD	Family Services Unit
Court Support Services Division	CSSD	PROB
Department of Correction	DOC	N/A
Department of Emergency Services and Public Protection	DESPP	N/A
Department of Motor Vehicles	DMV	N/A
Department of Motor Vehicles Administrative Per Se Unit	DMV	PERSE
Department of Motor Vehicles Passenger Endorsement Review Unit	DMV	PERU
Department of Motor Vehicles Commercial Vehicle Safety Division	DMV	CVSD
Division of Criminal Justice	DCJ	N/A
Division of Public Defender Services	DPDS	N/A
Judicial	JUD	N/A
Local Law Enforcement	<PD Name>	N/A
Office of Policy and Management	OPM	N/A
Office of the Victim Advocate	OVA	N/A
Superior Court Operations	SCO	N/A

Agency	Employer Name	Employer Sub Unit Name
Sponsored by Department of Emergency Services and Public Protection	DESPP-Sponsor	Federal Agency requesting CISS access

- Enter the user's Employer Subunit Name (currently for DMV only) **OR** Assignment as appropriate (Dispatcher, Detective, Officer, Records, Clerk, etc.).
- Enter the user's Department Address.
- Enter the user's COLLECT User ID (if applicable).
- Enter the Primary and Secondary phone numbers used for Multi-Factor Authentication (MFA). Please indicate phone type (work, mobile, home).
- User signature is required (electronically or physically – refer to Electronic Signature section for details).

Section 2 - CISS Search Account Access

- For POST Certification Credit Training, indicate training dates. POST Certification Training Dates listed at <http://www.ct.gov/cjis> (follow link for Training).
- Authorization for CISS Search access from Internet.
- Declaration of usage of Mobile Device Management solution for managing Mobile devices accessing CISS Search.
- Agency should disable the user access within 30 Mins of the User being no longer with the Agency. Agencies are trained to disable the User access or can reach out to CJIS-CT Helpdesk for disabling the user access.
- Refer to pages 3 through 8 for GFIPM Claim Definitions.
- Refer to page 9 for a guide to assigning CISS Administrative Responsibility, if appropriate.

Section 3 – MVP, Judicial Online Communication Exchange(JOCE) and CR-39 Access

- If you are requesting access to the CISS Message Viewer Portal, check the "Request MVP Access" box. This access is only available to the agencies listed.
- If you are requesting access for JOCE and/or CR-39, please check the appropriate box.
- Check your appropriate Agency selection.
- **Please select SLEO claim for CISS Search if you are requesting JOCE/CR-39 application access. ??**

Section 4 – TAC Officer Approval

- A TAC Officer within the user's agency must complete this section. A TAC Officer must be in accordance with the CT CJIS Security Policy.
- Approvers sign electronically or physically, refer to Electronic Signature section for details.

Section 5 – Agency Approval/Designee Approval

- A CJIS Authorizing Designee within the user's agency must complete this section.
- See the CJIS Authorizing Designees listed on pages 10 and 11.
- For Local Police Departments check with your local contact to determine who are the Agency Approver(s).
- Agency Approver, sign electronically or physically, refer to Electronic Signature section for details.
- For DESPP sponsored Users, DESPP will assume all responsibilities for the requesting Federal agency having access to CISS Search.
- For DESPP sponsored Users, DESPP will ensure compliance for Federal agencies using CISS Search to the CJIS Security Policy.

CISS Confidentiality Acknowledgement

- Complete the user information section.
- Refer to the hyperlinks for details on Criminal Statutes related to computer and information security.
- Read and place a check on all the points on the user agreement.

- Sign the form electronically and or physically.
- Refer to Electronic Signature section for details.

Completed Form

CISS Community Agency Administrator must email completed form (sections 1 – 5) and the CISS Confidentiality Acknowledgement to CJIS Operations for processing: CJIS.HelpDesk@ct.gov. Retain the original document within your agency.

If you have questions or need clarification, contact the CJIS Help Desk at (860) 622-2000.

GFIPM Claim Definitions

Claim Definition	Data Classification
<p>Public Data The user has permission to search for public data and documents within the user's home system, network or agency.</p>	<p>Public Data is defined by GFIPM as any information that is permitted to be released to the public and not subject to controlled unclassified information (CUI) access restrictions. This claim indicates that the user is authorized to see this type of information. Note that this does not imply that the data will be made available to the public through CISS. The scope of CISS users is generally defined as any agency or branch that is represented on the CJIS Governing Board.</p> <p>CISS Data Sources:</p> <ul style="list-style-type: none"> • PRAWN – Active Warrants • OBIS – Inmate Records • (SOR) Sex Offender Registry • CRMVS • CIB • POR • MNI-CCH
<p>Government Data The user has permission to search for government data and documents within the user's home system, network or agency.</p>	<p>Government Data is defined by GFIPM as any data obtained by a government agency pursuant to an administrative, legal or investigative function in furtherance of the official duties or functions of the agency.</p> <p>CISS Data Sources:</p> <ul style="list-style-type: none"> • DMV – Vehicle/Boat Registration data, • Driver's License data

Claim Definition	Data Classification
<p>Criminal Justice Data The user has permission to search for criminal justice data and documents within the user's home system, network or agency.</p>	<p>Criminal Justice Data is defined by GFIPM as data from law enforcement agencies, administrative agencies, courts, and corrections agencies regarding arrest, investigation, conviction, and sentencing for violation of a federal, state, tribal or territorial criminal law, including post-conviction correctional supervision during incarceration, supervision after release from incarceration, and performance of restitution." This claim indicates that the user is authorized to see this type of information.</p> <p>CISS Data Sources:</p> <ul style="list-style-type: none"> • CIB • CRMVS • DOC/BOPP Case Notes • DESPP - Sex Offender Registry • Local Agency Record Management System (RMS) • OBIS - Inmate Records • PRAWN – Active Warrants • CMIS Probation Data • MNI-CCH

Claim Definition	Data Classification
<p>Criminal History Data The user has permission to search for criminal history data and documents within the user's home system, network or agency.</p>	<p>Criminal History Data is defined by GFIPM as any information collected by criminal justice agencies on individuals that consists of identifiable descriptions and notations of arrests, detention, indictments, information notes or other formal criminal charges, and any disposition arising from them, including sentencing, correctional supervision, and /or release. The term does not include identification information, such as fingerprint records, to the extent that such information does not indicate involvement of the individual in the criminal justice system.</p> <p>CISS Data Sources:</p> <ul style="list-style-type: none"> • DESPP • POR

Claim Definition	Data Classification
<p>Criminal Investigative Data The user has permission to search for criminal investigative data and documents within the user's home system, network or agency.</p>	<p>Criminal Investigative Data is defined by GFIPM as information obtained from a variety of sources (public, government, confidential, etc.) The information may be utilized to further an investigation or could be derived from an investigation.</p> <p>CISS Data Sources:</p> <ul style="list-style-type: none"> • Criminal Law Enforcement Record Management System (RMS)
<p>Criminal Intelligence Data The user has permission to search for criminal intelligence data and documents within the user's home system, network, or agency.</p>	<p>Criminal Intelligence Data is defined by GFIPM as data which has been evaluated to determine that it: (i) is relevant to the identification of and the criminal activity engaged in by an individual who or organization which is reasonably suspected of involvement in criminal activity, and (ii) meets criminal intelligence system submission criteria.</p> <p>CISS Data Sources:</p> <ul style="list-style-type: none"> • Criminal Law Enforcement Record Management System (RMS) • Regional Information Sharing Systems • Joint Regional Information Exchange System • Law Enforcement Intelligence Units
<p>Sworn Law Enforcement Officer The GFIPM standard defines a "sworn law enforcement officer" as a user that is: A full time employee of a state-recognized law enforcement agency. Authorized (has the authority) to make an arrest. Certified by a State Certifying Authority, i.e., Police</p>	<p>Note that these criteria are not absolute rules and may be tailored to accommodate other definitions based on community consensus. Users who are "law enforcement officers" under some community definition are given this claim.</p> <p>CGS Chapter 950-Penal Code: General Provisions Sec. 53a-3</p>

Claim Definition	Data Classification
<p>Officer Standards and Training (POST), or equivalent. Additionally states that a user can be consider a SLEO if they are “a full time employee of a state-recognized law enforcement agency, acting on behalf of a SLEO, in performance of the user's assigned duties.”</p>	<p>(9) “Peace officer” means a member of the Division of State Police within the Department of Emergency Services and Public Protection or an organized local police department, a chief inspector or inspector in the Division of Criminal Justice, a state marshal while exercising authority granted under any provision of the general statutes, a judicial marshal in the performance of the duties of a judicial marshal, a conservation officer or special conservation officer, as defined in section 26-5, a constable who performs criminal law enforcement duties, a special policeman appointed under section 29-18, 29-18a or 29-19, an adult probation officer, an official of the Department of Correction authorized by the Commissioner of Correction to make arrests in a correctional institution or facility, any investigator in the investigations unit of the office of the State Treasurer, any special agent of the federal government authorized to enforce the provisions of Title 21 of the United States Code, or a member of a law enforcement unit of the Mashantucket Pequot Tribe or the Mohegan Tribe of Indians of Connecticut created and governed by a memorandum of agreement under section 47-65c who is certified as a police officer by the Police Officer Standards and Training Council pursuant to sections 7-294a to 7-294e, inclusive;</p> <p>CISS Data Sources:</p> <ul style="list-style-type: none"> • DOC/BOPP Case Notes • CMIS Probation Data • DMV (Driver) – Photos • MNI-CCH • OBIS – Inmate Records • PRAWN – Active Warrants • WEAPONS* (must also meet DESPP WEAPONS data claim definition)
<p>*Youthful Offender Data</p> <p>The GFIPM specification does not provide a standard mechanism to indicate that information pertains specifically to youthful offenders or to indicate that a user is authorized to view youthful offender information. To support the CISS security model, CJIS will implement a custom “Youthful Offender Data Search Home Privilege Indicator.”</p>	<p>For the purposes of CISS, <u>Youthful Offender Data</u> is information pertaining to an individual with youthful offender status as defined in Section 54-76b of the Connecticut General Statutes. This claim indicates that the user is authorized to see this type of information. Generally, this claim is used in conjunction with a more specific claim. For instance, information could be labeled such that the user must have both the “criminal justice data” indicator and the “youthful offender data” indicator to see criminal justice data related to youthful offenders.</p> <p>CISS Data Sources:</p> <ul style="list-style-type: none"> • OBIS – Inmate Records • PRAWN – Active Warrants • CRMVS – Limited Information

Claim Definition	Data Classification
	<ul style="list-style-type: none"> • DOC/BOPP Case Notes • MNI-CCH
<p>*COLLECT Certification Indicator Active, Connecticut On-Line Law Enforcement Communications system (COLLECT) certified users.</p>	<p>CISS Data Sources:</p> <ul style="list-style-type: none"> • MNI/CCH • Wanted File (CT WANTED AND NCIC) • WEAPONS
<p>*Weapons Data Access to CT WANTED, NCIC, WEAPONS (name and address) shall be given to active, Connecticut On-Line Law Enforcement Communications system (COLLECT) certified users who are also Connecticut sworn law enforcement officers, dispatchers, investigators, inspectors, or record keepers defined as:</p> <ol style="list-style-type: none"> 1. <u>Connecticut sworn law enforcement officer</u> is defined as an active, COLLECT certified user who is also a sworn law enforcement member of the Division of State Police within the Connecticut Department of Emergency Services and Public Protection or an organized local police department within the state of Connecticut, a prosecutor, chief inspector or inspector in the Connecticut Division of Criminal Justice, a Connecticut constable who performs criminal law enforcement duties, a Connecticut adult probation officer, an official of the Connecticut Department of Correction authorized by the Commissioner of Correction to make arrests in a correctional institution or facility, a member of a law enforcement unit of the Mashantucket Pequot Tribe or the Mohegan Tribe of Indians of Connecticut created and governed by a memorandum of agreement under section 47-65c who is certified as a police officer by the Police Officer Standards and Training Council pursuant to Connecticut general statutes, sections 7-294a to 7-294e, inclusive. 2. <u>Dispatchers</u> are defined as COLLECT certified users who are also dispatchers within the Connecticut Department of Correction, Connecticut Department of Motor Vehicles, Connecticut Department of Emergency Services and Public Protection, Division of State Police and the local police departments within Connecticut, including the Mashantucket 	<p>CISS Data Sources:</p> <ul style="list-style-type: none"> • DESPP – WEAPONS

Claim Definition	Data Classification
<p>Pequot Tribe or the Mohegan Tribe of Indians of Connecticut.</p> <p>3. <u>Investigators</u> are defined as COLLECT certified users who are also investigators within the Connecticut Division of Criminal Justice.</p> <p>4. <u>Inspectors</u> are defined as COLLECT certified users who are also inspectors within the Connecticut Department of Motor Vehicles.</p> <p>5. <u>Record keepers</u> are defined as COLLECT certified users who are also record keepers within the Court Support Services Division within the Connecticut Judicial Department and within the Department of Emergency Services and Public Protection and record specialists within the Connecticut Department of Correction.</p>	
<p>*WANTED File Data Access to CT WANTED, NCIC, WEAPONS (name and address) shall be given to active, Connecticut On-Line Law Enforcement Communications system (COLLECT) certified users who are also Connecticut sworn law enforcement officers, dispatchers, investigators, inspectors, or record keepers defined as:</p> <p>1. <u>Connecticut sworn law enforcement officer</u> is defined as an active, COLLECT certified user who is also a sworn law enforcement member of the Division of State Police within the Connecticut Department of Emergency Services and Public Protection or an organized local police department within the state of Connecticut, a prosecutor, chief inspector or inspector in the Connecticut Division of Criminal Justice, a Connecticut constable who performs criminal law enforcement duties, a Connecticut adult probation officer, an official of the Connecticut Department of Correction authorized by the Commissioner of Correction to make arrests in a correctional institution or facility, a member of a law enforcement unit of the Mashantucket Pequot Tribe or the Mohegan Tribe of Indians of Connecticut</p>	<p>CISS Data Sources:</p> <ul style="list-style-type: none"> • DESPP – WANTED File

Claim Definition	Data Classification
<p>created and governed by a memorandum of agreement under section 47-65c who is certified as a police officer by the Police Officer Standards and Training Council pursuant to Connecticut general statutes, sections 7-294a to 7-294e, inclusive.</p> <p>2. <u>Dispatchers</u> are defined as COLLECT certified users who are also dispatchers within the Connecticut Department of Correction, Connecticut Department of Motor Vehicles, Connecticut Department of Emergency Services and Public Protection, Division of State Police and the local police departments within Connecticut, including the Mashantucket Pequot Tribe or the Mohegan Tribe of Indians of Connecticut.</p> <p>3. <u>Investigators</u> are defined as COLLECT certified users who are also investigators within the Connecticut Division of Criminal Justice.</p> <p>4. <u>Inspectors</u> are defined as COLLECT certified users who are also inspectors within the Connecticut Department of Motor Vehicles.</p> <p>5. <u>Record keepers</u> are defined as COLLECT certified users who are also record keepers within the Court Support Services Division within the Connecticut Judicial Department and within the Department of Emergency Services and Public Protection and record specialists within the Connecticut Department of Correction.</p>	
<p>Criminal Justice Data Agency Edit Privilege Indicator The user has permission to edit, on behalf of the user's home agency, criminal justice data and documents within the user's home system, network, or agency. User eligibility requirements may include access to Law Enforcement criminal justice data in home agency.</p>	<p>CISS Data Sources:</p> <ul style="list-style-type: none"> CISS Electronic Content Management System (Document Repository) – Content Stewards – Users responsible for annotating, redacting, and releasing documents.

**There is no standard GFIPM metadata property to represent this security claim and, as such, a custom Connecticut-only claim is for CISS purposes.*

***Local Agency Security Officer (LASO) – Per the CT CJIS Security Policy**

Each Local Agency Security Officer (LASO) shall:

- Identify who is using the CJIS Governing Board approved hardware, software, and firmware and ensure no unauthorized individuals or processes have access to the same.
- Identify and document how the equipment is connected to the CT CJIS system.
- Ensure that personnel security screening procedures are being followed as stated in this Policy.
- Ensure the approved and appropriate security measures are in place and working as expected.
- Support policy compliance and ensure the CJIS Governing Board ISO is promptly informed of security incidents

**The LASO is the only authorized CISS user to access the CISS Audit Logs for their respective agency.*

CISS Community Agency Administrator – Per the CT CJIS Security Policy

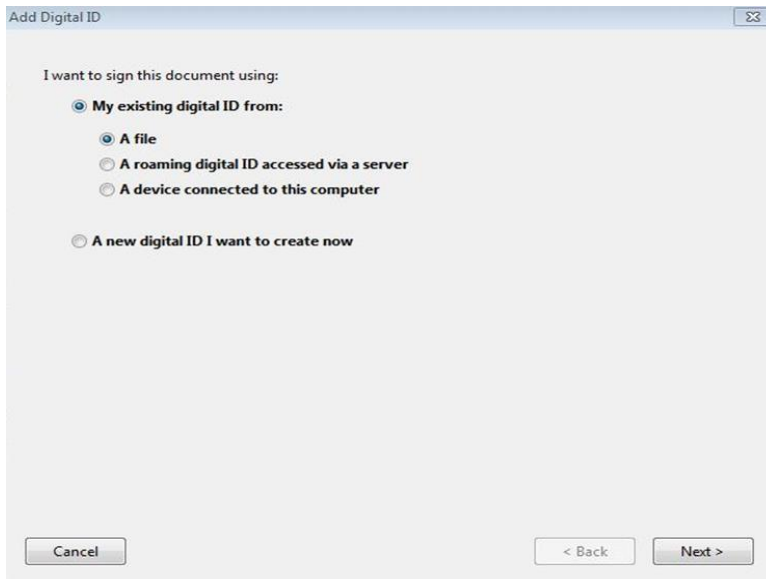
The CISS Community Agency Administrator is employed by a specific agency to perform the administration of CISS. In general, the CISS Community Agency Administrator will have the ability to perform functions for users in their agency only. However, they may be designated by other agencies to perform their duties as well (Example: Department of Correction (DOC) and Board of Pardons and Parole (BOPP)). The functions they will be able to perform include the following:

- Administer agencies, roles, groups, groups of agencies, users and expired passwords
- Save queries and reports to the Public Query Library

CT Terminal Agency Coordinator (TAC) - Per the CT CJIS Security Policy

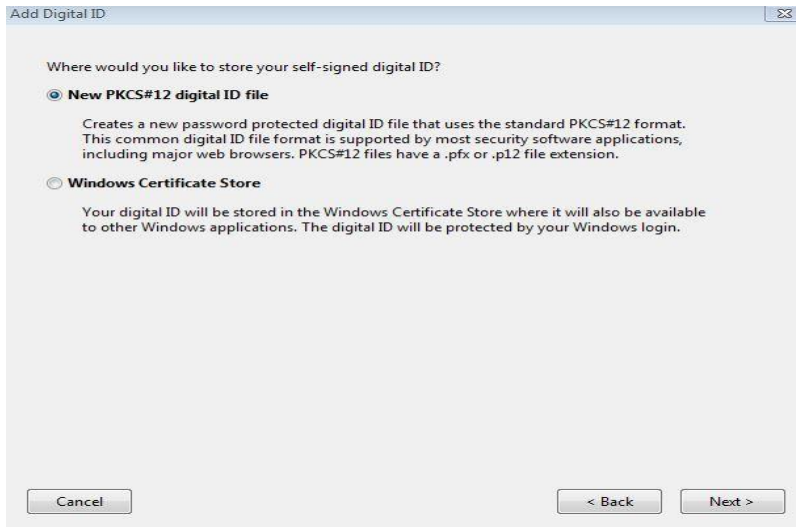
The Terminal Agency Coordinator (TAC) serves as the point-of-contact at the agency for matters relating to CT CJIS information access. The TAC administers CT CJIS systems programs within the agency and oversees the agency's compliance with CT CJIS systems policies.

- 1) The User for whom access is requested fills out the CUAR form, when user clicks the field that has signature; the user is directed to an *Add Digital ID* window as shown below, with following options.

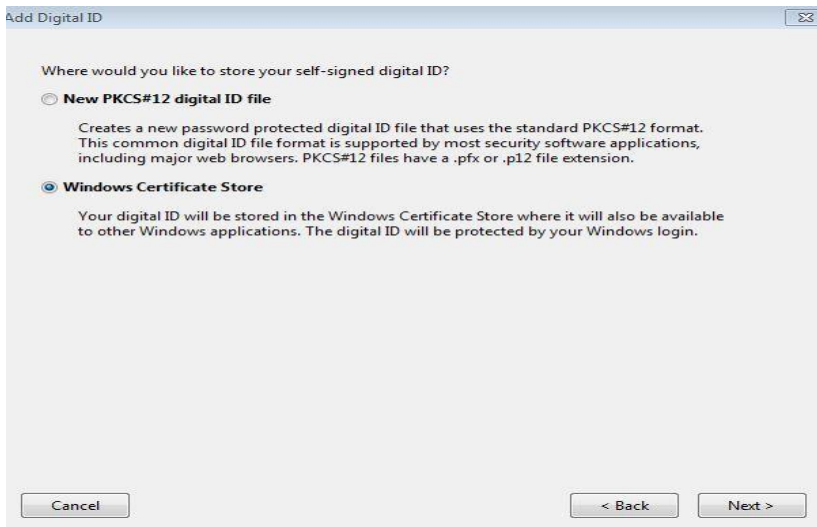


- 2) For the first time use to set up the signature, 'A new digital ID I want to create now' option is selected.
- 3) This leads to the page that has options on where the signatures should be saved and used in future. There are two options to save e-signatures,
 - a) New PKCS#12 digital ID file - password is required every time the user attaches the signature to any e-form.
 - b) Windows Certificate Store - password is not required; user just needs to click on sign.

Using the 1st method (a),



Using the 2nd method (b),



- 4) Once either of two options are selected, then the user's detail page is displayed where the user's name, Organization name, unit, email address details are provided.

Add Digital ID

Enter your identity information to be used when generating the self-signed certificate.

Name (e.g. John Smith):

Organizational Unit:

Organization Name:

Email Address:

Country/Region:

Key Algorithm:

Use digital ID for:

Cancel < Back Next >

- 5) Generally there are three options to select under *Use digital ID for*, either one is selected depending on user's security level.
- 6) The file name and the path to store the e-signature is provided with the password, by clicking on sign button the user is set up to attach his\her e-signature on the form by confirming the password when New PKCS#12 digital ID file is selected.
 - a) Using New PKCS#12 digital ID - user has to provide the password to attach signature.

Sign Document

Sign As:

Password:

Certificate Issuer: bhamini thanushetty Info...

Appearance:

bhamini thanushetty Digitally signed by bhamini thanushetty
 DN: cn=bhamini thanushetty, o=State of CT CJIS, ou=CJIS/CISS, email=bhamini.thanushetty@ct.gov, c=US
 Date: 2015.12.17 10:22:26 -05'00'

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

Sign Cancel

- b) Using Windows certificate store, user could directly attach the signature.



- 7) Every time the user has to attach signature to the form, user must click the *form field by* and password depending on the method user chooses digital ID.
- 8) The user could send the e-signed copies to CJIS for further action and also print the e-signed form and maintain the records at agency level.
- 9) The users could also sign the form manually, scan it and e-mail it to CJIS-CISS for further action.