MID ATLANTIC REGIONAL JUSTICE SHARING FEDERATION
PARTICIPATION AND PORTAL ACCESS AGREEMENT

This multi-party agreement (Agreement) is entered into by and between the organizations as shown on Attachment 2, hereinafter collectively referred to as the "Parties" or "Members," or "Federation Members."

PREAMBLE

WHEREAS, several states and the District of Columbia have a need to share criminal justice information about their shared offenders;

WHEREAS, the Parties have formed a federation called the "Mid-Atlantic Regional Information Sharing ("MARIS") Federation ("MARIS Federation," or "Federation");

WHEREAS, the intent of the Federation is to improve public safety and the functioning of the criminal justice system through greater information sharing across the Federation, while allowing each Party to establish and enforce its own policies for providing access to and use of its information;

WHEREAS, this Agreement is a pre-condition for membership in the MARIS Federation;

WHEREAS, this Agreement sets forth the responsibilities and obligations of a Party wishing to share certain criminal justice information portal access with other entities who have similarly subscribed to these responsibilities and obligations,

WHEREAS, Authorized Users of a Party are defined as those organizations and persons vetted in accordance with the Party's own policies , who are permitted to seek or provide data through the Party's criminal justice information portal, and who are obligated to follow the Party's rules for data receipt, disclosure, and use (i.e.; the Federation Members whose authenticated information is shared securely by an Identity Provider [as defined below] to access a Service Provider's [as defined below] protected resource).

NOW, THEREFORE, intending to be legally bound, the Parties agree as follows:

1. INTEGRATION AND CONSIDERATION

The Preamble of this Agreement is hereby integrated into this Agreement as an operative and binding section of the Agreement.

This Agreement is based upon good and valuable non-monetary consideration as described herein, and shall not fail for want of consideration.

This Agreement constitutes the entire agreement between the Parties regarding the subject of Federation membership and direct mutual criminal justice information portal access. This Agreement supersedes all prior and all contemporaneous agreements, understandings and communications, whether written or oral, regarding these subjects.

2. OBJECTIVE

To allow mutual criminal justice information portal access between and among the Parties and their Authorized Users for the purpose of promoting stronger public safety outcomes in the Parties'

respective jurisdictions. This Agreement establishes a governing body among the Parties which will provide for a viable mechanism to oversee the electronic data sharing of criminal justice information between the Federation Members consistent with the terms of this Agreement, and establish a mechanism to amicably resolve disputes among Federation Members, and promote the enhancement and expansion of the Federation.

3. MODIFICATION

No amendments or changes shall be made to the terms and conditions of this Agreement without the re-execution of this Agreement.

4. TERMINATION / SUSPENSION

Any Federation member may terminate its participation in the Federation at any time, upon written notice to the Federation Members, in which, the termination shall be effective on any future date as specified by the Party or, if no future date is specified, upon the following normal business day after the date of the notice. Termination of Federation membership constitutes termination of this Agreement as to the terminating Party.

A Party may suspend data flow and/or portal access in whole or in part to any other Party/Authorized User or combination of Parties/Authorized Users, whenever a reasonable determination has been made that any term of this Agreement or related law, rule, procedure, or policy has been or will be violated, and for any other extenuating circumstances. The Parties shall make a good faith effort to resolve any issues that may prevent resumption of data flow and/or portal access.

5. OTHER PROVISIONS

The Parties shall at all times be subject to all applicable federal and state laws and regulations in the performance of their duties under this Agreement. Nothing in this Agreement is intended to conflict with federal or state law or regulation, or a policy or directive of any Party. Each Party is responsible for its own conduct under this Agreement, and retains all defenses, including immunities available under applicable state and federal law. Nothing in this Agreement shall be construed to limit or waive the sovereign immunity of any Party or Authorized User. No Party agrees to insure, defend, or indemnify a Party or the Federation

If a term or condition of this Agreement conflicts with a state or federal law or regulation, the term or condition shall be invalid, but the remaining terms and conditions of this Agreement shall, to the extent possible, remain in full force and effect. If a term or condition of this Agreement is inconsistent with a directive or policy of any Party, the term or condition shall be invalid after the Party provides notice of the conflict to all other Parties. The remaining terms and conditions of this Agreement shall, to the extent possible, remain in full force and effect.

6. PARTY AND AUTHORIZED USER CHARACTERISTICS / NOTICE AND CHANGES

The Parties agree a Party must be a criminal justice agency as defined in 28 C.F.R. § 20.3 (g) (2011) to be a Federation Member.

Attachment 1- Authorized Users, is hereby incorporated by reference and is a part of this Agreement. Authorized Users may be added to this Agreement, and are hereby incorporated into this Agreement. upon receipt of the revised Attachment 1 by the MARIS Federation Governing Board. Any new

Attachments must be created substantially in the form of Attachment 1. New additions to Authorized Users to this Agreement must adhere to the Party-specific approval process regarding Party/Authorized User portal access and participation.

All Parties must ensure that all Authorized Users are required to adhere to the terms of this Agreement and to the terms of every Service Provider Policy Document governing data to which the Authorized User requests and accepts access

7. AUTHORITY TO PARTICIPATE IN THE FEDERATION

The Party warrants and represents that it is the authorized representative of the State, Territorial, or Tribal governmental jurisdiction seeking to join the MARIS Federation, and that the Party has the appropriate rights and permissions to transmit and receive all data shared under this Agreement. Each Party shall retain the rights to the data it shares pursuant to this Agreement.

8. SECURITY CONTROLS

Further, each Party warrants and represents that it has an existing process to ensure and/or enforce compliance with its own data and information security system safeguards, rules, controls and privacy requirements. Each Party agrees that it will make a good faith effort to implement and comply with the data and information security system safeguards, rules, controls and privacy requirements of the other Parties in a timely manner. The Parties further agree to assist with a thorough investigation of any reported allegation of a violation of this Agreement by an Authorized User, and to take appropriate corrective action in accordance with its existing process.

9. GOVERNANCE OF THE FEDERATION

The Parties hereby create and empower the MARIS Federation Governing Board ("Governing Board") to create Bylaws for the operation and governance of the MARIS Federation, and to suggest changes to this Agreement for Party consideration. Each State, Territorial, or Tribal Governmental jurisdiction shall have one representative on the Governing Board.

Each Party agrees to participate in the governance of the Federation in a meaningful manner which shall include, but not be limited to: the designation of an appropriate representative as a member of the Governing Board, regular participation in Governing Board meeting, and a good faith commitment to seek resolution of any disagreement or grievance arising from participation in the Federation through the prescribed governance process.

10. PARTICIPATION AS AN IDENTITY PROVIDER ORGANIZATION

An identity provider (IdP) is responsible for authenticating the credentials of their designated Authorized Users. Each Party must share information (claims) about the authentication of their designated Authorized Users with Service Providers (SPs) when those users attempt to access the SP's protected resource. Generally, an IdP maintains or leverages a directory of Authorized User accounts to support authentication as well as maintenance of attributes about Authorized Users (such as job title or function, agency or unit, email address, trainings and certifications, etc.) The IdP shares user authentication and attribute information with an SP by forming standards-based "assertions" (messages containing Authorized User authentication and attribute information) and including those assertions electronically with each request for access.

A Federation Member that operates one or more IdP(s) is called an Identity Provider Organization. Any Party may participate in the Federation as an Identity Provider Organization. Such participation is subject to the consent of the Governing Board, in accordance with the provisions of the Federation's Bylaws or other Federation policies.

When participating as an IdP, each Party agrees as follows:

A. Party will ensure that the Authorized User assertions formed by the IdP conform to the assertion requirements established in the *MARIS Architecture* Document, and that they accurately reflect the Authorized User's information at all times. Each Party agrees that Authorized User assertions will reflect changes in Authorized User status within eight hours of the Party being notified of the status change.

B. Party will produce the Authorized User assertions that contain the minimum Authorized User attributes as determined by the Governing Board, and documented in the *MARIS Architecture* Document. Party will ensure that attribute values in Authorized User assertions are set in accordance with the attribute definitions established in the *MARIS Architecture* Document. The *MARIS Architecture* document is hereby incorporated by reference into this Agreement. New versions of the *MARIS Architecture* Document are likewise incorporated by reference as of the date they are sent by the Federation Governing Board to the Parties.

C. Party will audit IdP operations in conformance with Federation policy at a minimum, and at a frequency determined by the Federation. Scope of audit will be limited to the provisions of this section and any Federation policies related to IdP operation. Party agrees to share the material results of audits with other Federation members upon request.

D. Party, upon learning of unauthorized access, will take reasonable precautions to prevent unauthorized access to systems that maintain Authorized User information and form assertions, and, should such unauthorized access occur, will notify the other members within eight hours of the unauthorized access.

E. Party will take reasonable precautions to prevent compromise of private cryptographic keys, to effect immediate revocation of any certificates for which the private keys have been compromised, and to notify all of the other members within eight hours of learning about any such compromise.

F. Party will ensure that Authorized Users whose identities are asserted through the IdP are informed, through training, notices, policies, and other generally accepted security practices, of the importance of safeguarding authentication credentials and other security practices to include the policies published by the service provider organizations in their service provider policy documents.

G. Party will develop and adopt policies, operational standards, and technical standards established by, or as otherwise approved as acceptable by, the Federation.

H. Party will cooperate with reasonable and legitimate requests from other Federation members for assistance in Federation operations, including but not limited to investigations of Authorized User misconduct or unauthorized access and troubleshooting technical or operational issues.

10. PARTICIPATION AS A SERVICE PROVIDER ORGANIZATION

A service provider (SP) is a technology mechanism that allows a Federation Member to provide other Federation Members with secure access to a protected resource (such as an application or dataset). The SP receives, with each request for access, information about the authenticity of the end user, which allows the SP to decide whether to grant the requested access.

A Federation Member that operates one or more SP(s) to protect its resources is called a Service Provider Organization.

Any Party may participate in the Federation as a service provider organization. Such participation is subject to the consent of the Federation Governing Board, in accordance with the provisions of this Agreement, the Federation's Bylaws, or other Federation policies.

When participating as a service provider organization, each Party agrees as follows:

A. Party will trust Authorized User authentication statements provided by identity providers in the Federation and will accept those authentication statements as a valid means of authenticating Authorized Users for accessing services (subject to access control restrictions).

B. Party will publish, in a manner acceptable to the Federation, a Service Provider Policy document for each service provider and protected resource. This document must address, at a minimum:

   1. Designate a technical and data quality point of contact to coordinate with Authorized Users on matters involving implementation of Service Provider access and data quality.
   2. A description of the resource, sufficient to inform a potential end-user of the data, content, or functionality available.
   3. Identify who is authorized to access the resource and under what conditions or circumstances.
   4. Any obligations that end users must accept as a condition of accessing the information.
   5. Describe how the service provider utilizes and protects personally identifiable information (PII) of end users, including but not limited to retention, auditing, destruction of data.

C. Party will provide written notification to all Federation Members as soon as reasonably possible of any change to a published Service Provider Policy document and will require timely compliance and conformance with these changes.

D. Party will take reasonable precautions to prevent compromise of private cryptographic keys, to effect immediate revocation of any certificates for which the private keys have been compromised, and to notify all members within eight hours of learning of any such compromise.

E. Party will develop and adopt all policies, operational standards, information security safeguards and controls, and technical standards required by law or as otherwise approved as acceptable by, the Federation.

F. Party will cooperate with reasonable and legitimate requests from all Federation Members for assistance in Federation operations, including but not limited to investigations of Authorized User or end user misconduct or unauthorized access and troubleshooting technical or operational issues.

G. Party agrees to log all user activity and all user access and share material portions of those logs with any Federation Members upon request using a standards-based format.

As a Service Provider Organization in the Federation, Party retains full control at all times over which Authorized Users are able to access its data and protected resources. Nothing in this agreement obligates or requires a participant to share any data or resources with any other Party, Authorized User, or individual.

11. FEDERATION MANAGEMENT RESPONSIBILITIES

A. Designation of a Member to Maintain the Federation Registry. The Federation Governing Board will designate one of the Federation members to maintain the Federation's Cryptographic Trust Document. That member agrees to maintain accurate, current entries in the Federation's Cryptographic Trust Document (the formal participant registry) for all members' IdPs and SPs.

B. Designation of a Member to Maintain a "Where Are You From" (WAYF) Service. The Federation Governing Board will designate one of the Federation members to stand up and maintain a WAYF service. Such member agrees that the WAYF service will be available with minimal downtime and will provide access to all IdPs in the Federation's Cryptographic Trust Document.

12. ASSUMPTION OF COST

The signatory acknowledges that any costs associated with participation in the Federation that is not covered by federal funding or other external resources, will be the Party's responsibility and cost of each participating jurisdiction. Nothing contained in this Agreement shall be construed to obligate any expenditure or reservation of funds in excess or advance of appropriations, or to obligate any expenditure which is not in accordance with applicable state and federal regulations and laws.

13. NO THIRD PARTY BENEFICIARY

This document shall not and is not intended to benefit or to grant any right or remedy to any person or entity that is not a party to this document.

14. NOTICES

All notices, certificates, acknowledgments, or other written communications shall be sent by the most expeditious means available. The notice shall be in writing and be deemed received and properly delivered, if duly mailed by certified or registered mail to each member at the address provided in Attachment 2, or to such other address, by written notice, designated by a member of the Federation.

15. RESPONSIBILITIES

Parties agree to adhere to the following terms and limitations on the use of the shared data:

A. The Parties shall use such information only for the purposes defined in this Agreement and permitted by state and federal law.

B. The Parties shall not further disseminate such information to any third parties, unless such dissemination is done in compliance with applicable federal and state law and for a purpose defined in this Agreement.

C. The Parties shall not disseminate any data to unauthorized users without the express written consent from the Service Provider or Identity Provider.

D. The Parties shall not disseminate any PII or other data about Authorized Users unless otherwise necessary for a purpose permitted by this Agreement without the express written consent from the Identity Provider.

E. The obligations under Section 15 shall survive the termination of this Agreement.

F. Except as otherwise prescribed by law, no Party has any responsibility or accountability for the use or disclosure of data made available by or to another Party after that data has been accessed or disclosed in accordance with this Agreement.

G. Each Party shall make reasonable efforts to ensure that the data it shares it was accessed and provided and is maintained in compliance with all applicable state and federal laws, regulations, and agency policies and procedures. No other promises are offered as to the quality or accuracy of the data.

H. ALL DATA AND DATA ACCESS IS PROVIDED "AS IS" AND WITHOUT ANY WARRANTY OF ANY KIND TO THE PARTIES, WHETHER EXPRESS, IMPLIED OR STATUTORY. NO PARTY WARRANTS THAT THE DATA WILL BE ERROR-FREE, OR THAT THE ELECTRONIC NETWORK WILL BE ERROR FREE OR UNINTERRUPTED, OR THAT ERRORS WILL BE CORRECTED. ALL PARTIES HEREBY DISCLAIM ALL IMPLIED AND EXPRESS WARRANTIES, CONDITIONS AND OTHER TERMS, WHETHER STATUTORY, ARISING FROM THE COURSE OF DEALING, OR OTHERWISE, INCLUDING WITHOUT LIMITATION TERMS AS TO QUALITY, MERCHANTABILITY, FITNESS FOR PURPOSE AND NONINFRINGEMENT.

19. POINTS OF CONTACT.

Attachment 2 -- Contacts, is hereby incorporated into and made a part of this Agreement. Contacts may be added to this Agreement, and are hereby incorporated into this Agreement and made fully a part of this Agreement upon receipt of the revised Attachment 2 by the Parties from the MARIS Board. Any future Contacts submitted to the Federation must be presented substantially in the form of Attachment 2.

20. DISPUTE RESOLUTION AND GOVERNING LAW

The Parties shall attempt in good faith to resolve any dispute arising out of or relating to this Agreement promptly by negotiations between representatives who have authority to settle the controversy. The Parties intend that all disputes arising under this Agreement be resolved expeditiously. Disputes under this Agreement shall be initially submitted to the Governing Board for informal resolution, failing which mediation shall be undertaken, in accordance with Governing Board policies and procedures. If, at any point during the Dispute Resolution Process, all of the Parties to the dispute accept a proposed resolution to resolve the dispute, the Parties agree to implement the terms of the resolution within the agreed upon timeframe.

Notwithstanding the foregoing, a Party may be relieved of its obligation to participate in the Dispute Resolution Process if such Party (i) believes that the other Party's acts or omissions create an immediate threat to the confidentiality, privacy or security of data or will cause irreparable harm to the Party or any third party, and (ii) pursues immediate relief against such other Party in a court of competent jurisdiction. The Party pursuing immediate relief must notify the Parties' governing body of such action within twenty-four hours of filing for the relief and of the result of the action within twenty-four hours of learning of same.

If the relief sought is not granted and the Party seeking such relief chooses to pursue the dispute, the Parties must then submit to the Dispute Resolution Process described herein.

21. PUBLICITY

Parties agree to provide notice in advance, and to receive the approval of the Governing Board, of any publicity releases in connection with the activities under this Agreement. A publicity release is defined as an act or device designed to attract public interest, specifically information with news value issued as a means of gaining public attention or support.

22. LIMITATION OF RIGHTS

The Parties represent and warrant that this Agreement, when duly executed and delivered, will constitute the legal, valid, and binding obligation of each Party, enforceable by each Party against the other,and subject to all provisions of law. Except as specifically stated herein, this document does not,and shall not be construed to create any other rights, substantive or procedural, enforceable at law by any person in any matter, civil or criminal

23. SIGNATURES

This Agreement may be executed in any number of counterparts, and by different parties in separate counterparts. The signed copies will together form a single Agreement. Additional Parties may be added by their full execution of a counterpart to the Agreement. The effective date of this Agreement as to any Party is the date of affixation of the final required signatory for that Party. All then-existing Parties must be notified of the pendency of additional Party counterparts prior to the additional Party's effective date by virtue of an updated version of Attachment #2 and an executed counterpart of this Agreement. Delivery by electronic transmission of an executed counterpart of this Agreement is as effective as delivery of an original executed counterpart of this Agreement.

Signatures affixed must be sufficient to legally bind the Parties. All parties, and their respective signatories on their behalf, represent that they and their signatories have full authority to enter into this Agreement.

24. JOINTLY DRAFTED

This MOU shall be deemed to have been drafted by the Parties and, in the event of a dispute, shall not be construed against any Party.

END OF NUMBERED TERMS

IN WITNESS WHEREOF the parties hereto have executed this MOU, effective as to each party as of the last date affixed by each party:

MARYLAND DEPARTMENT OF PUBLIC SAFETY AND CORRECTIONAL SERVICES

This agreement has been approved for form and legal sufficiency.

Stuart M. Nathan
Principal Counsel
Maryland Department of Public Safety
And Correctional Services

Dec. 26, 2014
Date

Kevin Combs,
Chief Information Officer
Maryland Department of Public Safety
And Correctional Services

1/6/15
Date

~~Gregg Hershberger~~ Carroll A. Parrish
Secretary (Acting)
Maryland Department of Public Safety
And Correctional Services

1-11-15
Date

DISTRICT OF COLUMBIA CRIMINAL JUSTICE COORDINATING COUNCIL

Signature

12.31.14
Date

Mannone A. Butler, Executive Director

DELAWARE CRIMINAL JUSTICE INFORMATION SYSTEMS (DELJIS)

Signature

11/25/15
Date

Peggy Bell, Executive Director

DELAWARE CRIMINAL JUSTICE COUNCIL

Signature

11/16/15
Date

Christian Kervick, Executive Director

PENNSYLVANIA GOVERNOR'S OFFICE OF ADMINISTRATION (OA)

Signature

12/24/2014
Date

Signature

Date

Review for form and legality:

Signature
OA Office of Chief Counsel 12/23/2014

Date

Signature
Office of General Counsel

Date

Signature
Office of Attorney General

1/29/15
Date

Attachment 1: Authorized Users

The Authorized Users permitted access by each Party shall be law enforcement entities, or other entities, defined as follows by each Party:

1.Party	2. Authorized Users
MD	

1.Party	2. Authorized Users
DE	

v. 1.0 December 10, 2014
Attachment 1c, DE, page 1 of 1

1.Party	2. Authorized Users
PA	

v. 1.0 December 10, 2014
Attachment 1d, PA, page 1 of 1

Attachment 2: Contacts

Maryland Department of Public Safety and Correctional Services (DPSCS)
Kevin Combs Chief Information Officer 6776 Reisterstown Road Ste. 209 Baltimore, MD 21215 (410) 585-3812 (Office) (410) 318-6004 (Fax) kcombs@dpscs.state.md.us
District of Columbia Criminal Justice Coordinating Council (CJCC)
Imran Chaudhry Chief Information Officer 441 4th Street, NW Washington, DC 20001 202.727.7862 (Office) 202.724.3691 (Fax) imran.chaudhry@dc.gov
Delaware Criminal Justice Information Systems (DELJIS)
Peggy A. Bell Executive Director 802 Silver Lake Blvd – Suite 101 Dover DE 19904 SLC – D530A (302) 739-4856 (302) 739-6285(fax) (302) 270-4442 (cell) Peggy.Bell@state.de.us
Pennsylvania Commission on Crime and Delinquency (PCCD)
Robert K. Merwine Director - Office of Criminal Justice System Improvements 3101 North Front Street Harrisburg, PA 17108 (work) 717-265-8542 (fax) 717-772-0550 rmerwine@pa.gov