PRIVACY ACT STATEMENT

AUTHORITY: 5 U.S.C. Section 301, Departmental Regulations; 6 U.S.C. Section 101, et seq., the Homeland Security Act; 10 U.S.C. Section 113, Secretary of Defense; 10 U.S.C. Section 5013, Secretary of the Navy; 10 U.S.C. Section 3013, Secretary of the Army; 10 U.S.C. Section 8013, Secretary of the Air Force; 42 U.S.C. Sections 2451, et seq., the National Aeronautics and Space Act; DoD 5200.08-R, DoD Physical Security Program; DoD Instruction 5200.08, Security of DoD Installations and Resources; DoD Instruction 2000.16, DoD Antiterrorism Standards; DoD Directive 2000.12, DoD Antiterrorism Program; DoD Directive 8521.01E, Department of Defense Biometrics; DoD Directive 8500.1, Information Assurance; UFC 40010-01, Unified Facilities Criteria, DoD Minimum Antiterrorism Standards for Buildings; Army Regulation 190-13, The Army Physical Security Program; OPNAVINST 5530.14E, Navy Physical Security and Law Enforcement Program; Marine Corps Order P5530.14; Marine Corps Physical Security Program Manual; Federal Property Management Regulations, Part 102-81 (Security); and E.O. 9397 (SSN).

PRINCIPAL PURPOSES: Management of physical and/or logical access, performing enrollments, background screening/vetting, identity verification, suitability determination, and credentialing and management of access and adjudication information.

ROUTINE USES: In addition to those disclosures generally permitted under 5 U.S.C. Section 552a(b) of the Privacy Act, these records or information contained therein may specifically be disclosed outside the particular Government agency responsible for collection for routine uses pursuant to 5 U.S.C. 552a(b)(3) and Government agency "blanket routine uses."

DISCLOSURE: Voluntary. However, failure to provide the requested information may delay, prevent, or otherwise affect entry to secured Government-controlled facilities, locations, or systems, and/or result in further inspection of person or property.

Please carefully read this Agreement. This Agreement sets forth the terms and conditions of your participation in one or more RAPIDGate® programs and affects your legal rights. The RAPIDGate programs are the RAPIDGate® Program, the RAPIDGate-Premier™ Program, and the RAPID-IAC™ Program. They are referred to collectively in this Agreement as the "***Programs***" and individually as a "***Program***." You are entering into this Agreement with SureID, Inc. (formerly named Eid Passport, Inc.), the service provider of the Programs. SureID, Inc. is referred to in this Agreement as the "***Service Provider***."

By selecting the "I ACCEPT" box below, you accept all terms and conditions of this Agreement, as it may be updated by the Service Provider from time to time, and you agree to be bound by this Agreement.

IF YOU DO NOT AGREE TO BE BOUND BY THIS AGREEMENT, SELECT THE "I DO NOT ACCEPT" BOX BELOW AND "QUIT" THE REGISTRATION PROCESS.

1. Introduction

1.1. The Programs combine identity authentication, vetting, access management, and credentialing to help make Government facilities, networks, and people safer and more secure. At the same time, the Programs help to make access easier and faster for vetted and credentialed personnel.

1.2. You may register if you or your company are sponsored by a participating Government agency and, where applicable, your company has enrolled in the Program. You must complete the registration process and comply with all Program terms and conditions. This Agreement sets forth those terms and conditions.

1.3. Your Program registration is valid for the period of time you or your company selected at the time of enrollment or renewal. The period typically is either one year or 90 days.

1.4. Your Program point of contact will be the individual designated by your company as the RAPIDGate Company Administrator or the individual designated by your Government sponsor as the RAPID-IAC Administrator (collectively referred to in this Agreement as the "***RCA***").

1.5. If we need to communicate with you, usually we will do so through your RCA. The RCA is responsible for promptly forwarding our communications to you. However, sometimes we or our third-party providers may communicate with you directly. Direct communications will be mailed to you to the U.S. mailing address you provide at Program registration. Sensitive information may be included. As the most common example, if you "fail" a Program background screening, a copy of your background screening report will be mailed to you at your provided mailing address.

1.6. You should download and retain for your records a copy of this Agreement at http://www.rapidgate.com. The Service Provider may, from time to time, update this Agreement. The Service Provider will post the updated Agreement to the above website and will notify you, through your RCA, of updates. You are encouraged to regularly check the above website or call 1-877-727-4342 to obtain a current copy of the Agreement.

The updated Agreement will become binding on you 30 days after it is posted on the Service Provider's website. Your continued participation in a Program after that date will constitute your acceptance of the terms of the updated Agreement. If you do not wish to be bound by the updated Agreement, you must provide written notice to the Service Provider at info@rapidgate.com or at the following mailing address:

SureID, Inc.
5800 NW Pinefarm Place
Hillsboro, OR 97124

Following receipt of such notice, the Service Provider will terminate you from the Program, deactivate the Program credential issued to you (including any digital certificates contained in the credential), and notify your RCA.

PLEASE NOTE:

(This section does not apply if you are registering for a Program not requiring screenings.)

If you register for a Program, you will be subject to Government database checks and/or commercial background screenings (collectively "***Program Screenings***") to determine your eligibility to participate in the Program. Records checked may include criminal and other records that date back more than 10 years. If you are accepted into the Program, screenings will be conducted on an ongoing basis while you are a Program participant.

Program Screenings are conducted for the purpose of supporting physical and/or logical access control and identity management at secure Government facilities. Program Screenings are not conducted for employment purposes. Your company must agree, as a condition of participating in a Program, that it will not take adverse employment action against you based upon the results of Program Screenings, use the Program as an employment screening service, or otherwise use the Program for employment purposes. If you have any questions or concerns, please speak with your company's RCA or Human Resources Department.

2. Information Being Collected From You

2.1. The information you are required to provide during the registration process consists of any or all of the following:

- Full legal name
- Current residence address
- Date of birth
- Height
- Weight
- Gender
- Citizenship status
- Individual business email address (failing to provide your individual business email address may affect your ability to use the full capabilities of the Program credential)
- Digital photograph of face
- Digital fingerprint images
- Social Security Number (providing the Social Security Number is voluntary, but failure to do so will preclude your participation in the Programs)
- Billing credit card number and expiration date (if applicable)
- Billing address (if applicable)
- Identification document(s) listed on Form I-9

You must promptly notify the Service Provider of any changes to your information by telephone or in writing using the contact information provided in section 1.6.

2.2. The Service Provider and/or the Government may use the information collected from you for purposes including but not limited to:

- Verifying your Program sponsorship
- Processing Government database checks on you
- Conducting commercial background screenings on you
- Verifying your claimed identity
- Manufacturing and issuing a Credential
- Managing the lifecycle of a Credential
- Managing the Programs
- Issuing and managing digital certificates on a Credential
- Preparing reports for the Government

- Performing law enforcement, national security, anti-terrorism or other investigative functions
- Any "routine use" under 5 U.S.C. Section 552a(b)(3) or any Government agency "blanket routine use"

2.3. The Government may have access, ownership, and control rights over the information collected on you through the Programs. The Government considers this information to be part of a Government "system of records" subject to the Privacy Act of 1974 (see Privacy Act Statement on page 1 of this Agreement).

2.4. The Service Provider may engage one or more third parties to support Program functions. The Service Provider, its third-party providers, and the Government all have responsibility for safeguarding the security, confidentiality and integrity of your personally identifiable information ("***PII***") collected and/or stored through the Programs. The Service Provider and its third-party providers are committed to maintaining this data in strict confidence. They employ physical, technical, and administrative safeguards per the applicable legal requirements and Government policy. For further information regarding Governmental privacy, please see the Privacy Act Statement on page 1 of this Agreement.

2.5. By clicking the "I ACCEPT" button below, you authorize the Service Provider and its third-party providers to collect and use your PII for the purposes set forth in this Agreement, and to retain your PII and any updates to your PII for a commercially reasonable period of time.

3. Government Database Checks

3.1. The Government may require that you be checked against databases maintained by one or more Government agencies, as a condition of your Program eligibility.

3.2. One example of a Government database you may be checked against is the National Crime Information Center ("***NCIC***"). The NCIC is an electronic clearinghouse of crime records maintained by the Federal Bureau of Investigations ("***FBI***"). The records are entered by criminal justice agencies. These agencies are responsible for maintaining the accuracy and integrity of the data they enter into the NCIC.

3.3. Records in the NCIC and other Government databases may include criminal records that date back more than 10 years.

3.4. Government database checks may be processed on you at any time while you are a Program participant, including but not limited to:

- When you register for a Program
- Periodically while you are a Program participant
- At Program registration renewal
- At any time upon request by the Government for Program purposes
- At any time at the sole discretion of the Service Provider for Program purposes

3.5. The Service Provider may use third-party providers to process Government database checks. The Service Provider will receive notification of Government database "hits" indicating the presence of disqualifying records. Erroneous hits from the Government databases can occur for reasons outside the control of the Service Provider or its third-party providers. Reasons could

include the presence of out-of-date Government records or multiple persons with the same name in a Government database. If a Government database check on you results in a hit, the Service Provider will attempt to independently confirm the disqualifying records, for example by performing a commercial background screening on you (described in more detail below). However, independent confirmation may not always be available.

3.6. A Government database hit (unless the Service Provider determines it is erroneous) will disqualify you from participating in a Program. The Service Provider will so notify you, through your RCA. You will receive instructions on how you may ask the relevant Government agency for a copy of its records on you, in case you wish to dispute the Government database hit or if you wish to dispute the completeness or accuracy of the Government's records on you. In addition, the Service Provider will inform you or your company's RCA if you are eligible to request a waiver from the Government to allow you to participate in a Program.

3.7. The Service Provider will inform your sponsoring Government agency of any hits from Government database checks on you. If the Service Provider or its third-party provider has underlying record information from the Government database check, the database check information may be shared with the Government.

3.8. If you are registered through your company, the Service Provider will notify your company's RCA of any hits from Government database checks on you. Your company is prohibited, under the terms and conditions of its Program enrollment, from taking adverse employment action against you based on the results of Program Screenings or using the Program as an employment screening service.

3.9. By clicking the "I ACCEPT" button below, you hereby consent and authorize the Service Provider and/or its third-party providers to perform Government database checks, including but not limited to NCIC checks, on you as described in this Agreement.

4. Commercial Background Screenings

4.1. The Government may require that you pass commercial background screenings as a condition of your Program eligibility.

4.2. Commercial background screenings may be conducted on you at any time while you are a Program participant, including but not limited to:

- When you register for a Program
- Periodically while you are a Program participant
- At Program registration renewal
- At any time upon request by the Government for Program purposes
- At any time at the sole discretion of the Service Provider for Program purposes

4.3. The Service Provider may engage one or more third parties to conduct the commercial background screenings.

4.4. Commercial background screenings are based upon searches of public records and may include any or all of the following:

- Validation of your Social Security Number and address history
- National criminal database search
- Federal criminal records search (Public Access to Court Electronic Records)
- Sex offender registry search
- County criminal records search
- Open criminal warrants search
- Office of Foreign Assets Control Specially Designated Nationals list search
- Other Government watch list searches
- Validation of your citizenship status and/or right to work in the United States

4.5. Records searched through the commercial background screenings may include criminal records that date back more than 10 years.

4.6. An "adjudication" process is available to you if you "fail" a commercial background screening and disagree with the result. In such event, the Service Provider or its third-party provider will notify you in writing of a commercial background screening "fail" result and provide you with a copy of your background screening report and instructions on how to seek redress. You will have an opportunity to dispute the information in the report and to request a re-investigation of the information. You will be provided with a written report of the results of the re-investigation and a copy of the amended commercial background screening report if the re-investigation results in any change.

4.7. If you do not timely dispute the commercial background screening results or if you do so but are unsuccessful in changing the results, you will not qualify to participate in the Programs. If you already are a Program participant, your participation will be immediately terminated. The Service Provider will inform you or your company's RCA if you are eligible to request a waiver from the Government to allow you to participate in the Program.

4.8. The Service Provider will inform the Government of the "pass" or "fail" results of the commercial background screening on you. The Service Provider also may inform the Government of the reason for a "fail" result and may provide the Government with a copy of the background screening report on you.

4.9. If you are registered through your company, the Service Provider will notify your company's RCA of the "pass" or "fail" results of the Program background screening on you. However, the Service Provider will not inform your company of the reasons for a "fail" result and will not provide your company with a copy of the background screening report on you. Your company is prohibited, under the terms and conditions of its Program enrollment, from taking adverse employment action against you based on the results of Program Screenings or from using the Program as an employment screening service.

4.10. By clicking the "I ACCEPT" button below, you hereby consent and authorize the Service Provider and/or its third-party providers to perform Program commercial background screenings on you as described in this Agreement.

5. Program Credential

5.1. If you pass the applicable Program Screenings following registration, the Service Provider will manufacture a Program credential that displays your name, photo, and other pertinent

information. The credential may be issued to you by a Government representative at the facility for which you are authorized, by your Program sponsoring entity, or by the Service Provider. The credential will be either a standard Program credential or a Personal Identity Verification-Interoperable ("***PIV-I***") credential.

5.2. To receive a Program credential, you must present at least two Government-issued identity verification documents, one of which contains your photograph. If you are issued a PIV-I credential, you should expect to undergo this identity proofing process during both the registration process and the credential issuance process.

5.3. Once you are issued a Program credential, you will be provided instructions on how to activate it. Following activation, when you arrive at a facility or location that participates in the Program and that has authorized your access, security personnel will scan your credential to verify your identity and your Program authorization status. In addition, security personnel may scan your fingerprint for secondary identity verification purposes. You should wear and display the Program credential at all times while at the facility.

5.4. You are responsible for protecting the Program credential issued to you. You must immediately notify the Service Provider and your company's RCA if your Program credential is lost, stolen, or damaged or if you suspect that someone other than yourself has used the credential. You may not tamper with, disable, deface or otherwise deliberately damage the Program credential. You may not give or share the Program credential with anyone else, copy or otherwise duplicate the credential.

5.5. If the Program credential issued to you is lost, stolen, or damaged, you must immediately notify your company's RCA. The RCA is required to immediately notify the Service Provider at (877) 727-4342. You will be charged a fee to replace a lost, stolen, or damaged Program credential.

5.6. If you stop working for your company, lose your Program sponsorship, or stop participating in a Program, you must immediately return your Program credential to your company's RCA. If you are participating in the RAPID-IAC Program or if you are your company's RCA and there is no RCA replacement for you, you must immediately arrange to securely return the Program credential at your own expense to the Service Provider by contacting customer service at (877) 727-4342.

6. Additional Terms for PIV-I Program Credentials

6.1. For purposes of this Agreement, the following definitions apply:

- "Certificate" means a digital representation of information in a PIV-I Credential which at least (1) identifies the certification authority issuing it, (2) names or identifies the participant, (3) contains the participant's public key, (4) identifies its operational period, and (5) is digitally signed by the certification authority issuing it.

- "Digital Signature" means the result of a transformation of a message by means of a cryptographic system using keys such that a Relying Party can determine: (1) whether the transformation was created using the private key that corresponds to the public key in the signer's digital Certificate; and (2) whether the message has been altered since the transformation was made.

- "PIV-I Credential" means a Personal Identity Verification ("PIV") interoperable card issued by SureID (or its authorized agents) that meets certain technical specifications to work with federal PIV infrastructure elements such as card readers, is issued in a manner that allows Relying Parties to trust the card, and contains participant's Certificates.

- "Private Key" means (1) the key of a signature pair key used to create a digital signature or (2) the key of an encryption key pair that is used to decrypt confidential information. In both cases, this key must be kept secret.

- "Public Key" means (1) the key of a signature key pair used to validate a digital signature or (2) the key of an encryption key pair that is used to encrypt confidential information. In both cases, this key is made publicly available normally in the form of a digital certificate.

- "Public Key Infrastructure (PKI)" means a set of policies, processes, server platforms, software and workstations used for the purpose of administering Certificates and public-private key pairs, including the ability to issue, maintain, and revoke Public Key Certificates.

6.2. Your Obligations, Representations, and Warranties

You hereby agree, represent, and warrant that:

- You shall immediately notify SureID upon loss or suspicion of loss or compromise (including but not limited to suspected or known unauthorized use, theft or misplacement) of your PIV-I Credential, Certificates, or Private Key(s).

- You shall protect your PIV-I Credential and Private Key(s) from access by any other party.

- You shall use the PIV-I Credential and the Private Key(s) solely for authorized and permissible legal business purposes.

- SureID retains the right to revoke your PIV-I Credential, Certificates, and/or Private Key(s) if SureID suspects or has knowledge that you have used them for an unauthorized purpose, that you have provided inaccurate information to SureID or the PKI authorities, or that the your PIV-I Credential, Certificates, or Private Key(s) were obtained through fraudulent means.

- You shall immediately discontinue use of your PIV-I Credential, Certificates, and Private Key(s), and shall immediately return the PIV-I Credential to your employer organization, when you leave your employer's employ.

- You understand that the combination of your PIN and Private Key constitutes a Digital Signature and agree to be legally bound by any document digitally executed via your Private Key and PIN.

- You shall accurately represent yourself in all communications with SureID and with the PKI authorities.

- All information you have provided and in the future will provide in connection with your application for and use of the PIV-I Credential is true, complete, and correct;

- You shall be the only individual able to use your PIV-I Credential and to access your PIN and Private Key(s).

- You shall protect your Private Key(s) at all times in accordance with the relevant SureID PIV-I documents including, without limitation, such SureID Certificate Policy as may be posted online at www.sureid.com.
- You shall abide by all the terms, conditions, and restrictions placed on the use of your Private Key(s) and Certificates.
- You shall create a strong PIN, memorize the PIN and not write it down or reveal it to anyone, and at all times protect the PIN.
- You shall not leave your PIV-I Credential unattended while activated with your PIN.

7. Fees and Registration Renewal

7.1. The Service Provider will process your Program registration after your Program fee is paid. Registration and renewal fees are not refundable. For example, no refund is available if you "fail" a Program Screening, if you end your Program participation early, or if the Government changes or discontinues the Program. Fees are subject to change by the Service Provider at its discretion.

7.2. Prior to the end of your Program term, subject to the approval of your sponsoring Government agency or other sponsoring organization, your company's RCA may renew your registration for another term following payment of the renewal fee to the Service Provider. Your renewal is contingent upon your passing the applicable Program Screenings and in all other respects meeting the Program eligibility criteria.

7.3. If you do not want your registration to be renewed, you must notify your company's RCA at least 60 days before the anniversary of your current registration term to avoid being charged the renewal fee.

8. Grounds for Terminating Your Program Registration and Deactivating Your Credential

Grounds for terminating your Program registration and deactivating your Program credential (and, in the case of a PIV-I credential, revoking any digital certificates) include but are not limited to the following:

- You stop working for the company through which you registered with the Program
- You "fail" a Program Screening
- You no longer have a business need to visit a facility participating in the Program
- Your company directs the Service Provider to remove you from the Program
- Your company no longer is eligible or ends its participation in the Program
- You use a Program credential for unauthorized, improper or impermissible purposes
- The Government facility for which you registered no longer participates in the Program
- The Government directs the Service Provider to remove you from the Program
- The Government removes your company from the Program
- The Government sponsoring entity no longer approves your participation in the Program
- You violate any term or condition of this Agreement

9. General Restrictions

9.1. Program registration does not by itself make you eligible to participate in a Program. Your eligibility to participate in a Program is subject to your passing the applicable Program Screenings and meeting all Program terms and conditions set forth in this Agreement.

9.2. Program participation does not guarantee you access to Government facilities or networks. Facility security personnel maintain the right to deny you access, change the facility's access procedures, and enforce any and all security protocols it deems necessary, including but not limited to inspecting your person as well as your vehicle and its contents, and contacting law enforcement.

10. Waiver and Release

10.1 Program Participation. Program participation is subject to termination for reasons outside the control of the Service Provider. For example, the Government's sponsoring entity may revoke its sponsorship of your company's or your participation in a Program at any time for any reason; your company may choose to stop participating in a Program; the Government's sponsoring entity may modify or discontinue its participation in a Program; the Government or your company may direct the Service Provider to terminate your participation in a Program at any time and for any reason; the Government may choose to discontinue the Program; or you may violate the terms of this Agreement or otherwise become ineligible to participate in the Program. If any of these events occurs, the Service Provider will terminate your Program registration.

Waiver and release: You agree that, if any of the above-described events occur, you have no financial, legal or other remedies, and will not initiate or join any legal action, against the Programs or the Service Provider including without limitation the Service Provider's officers, directors, employees, agents, contractors, assigns, successors, predecessors, representatives, subsidiaries, parents and affiliates (referred to collectively in this Agreement as "***the Service Provider Parties***"), and you hereby fully waive, release and discharge the Service Provider Parties from any and all claims, demands, and causes of action, damages, losses, liabilities, taxes, assessments, fines, penalties, judgments, awards, costs and expenses, including but not limited to reasonable attorneys' fees (collectively "***Claims***") relating to such events.

10.2 Use of Program Screenings. Your company is prohibited, under the terms of the Programs, from using the Programs, including the Program Screenings, for employment purposes including taking adverse employment action against you based on the results of Program Screenings or from using the Program as an employment screening service.

Waiver and release: You agree that you have no financial, legal or other remedies, and will not initiate or join any legal action, against the Service Provider Parties for any adverse pre-employment or employment action taken against or for any other employment decision affecting you relating in any way to your registration with, or participation in, a Program including but not limited to Program Screenings, and you hereby fully waive, release and discharge the Service Provider Parties from any and all Claims relating to such events.

10.3 Program Screenings Based upon Government and other Public Records. The Program Screenings are conducted through searches of Government databases and other public records. Neither the Service Provider nor its third-party providers can guarantee the completeness or accuracy of the data obtained and they may not be able to independently verify hits from

Government database checks. Program screenings may sometimes result in erroneous hits resulting in a background screening "fail."

Waiver and release: You agree that you have no financial, legal or other remedies, and will not initiate or join any legal action, against the Service Provider Parties relating in any way to the accuracy or completeness of data, information or records checked or derived from a Program Screening, or relating in any way to your not passing a Program Screening, and you hereby fully waive, release and discharge the Service Provider Parties from any and all Claims relating to such events.

10.4 Criminal History Information. Program Screenings may include checks of criminal history records or other information that date back more than 10 years. You may be subject to disqualification from the Program if a Program Screening reveals such information.

Waiver and release: You agree that you have no financial, legal or other remedies, and will not initiate or join any legal action, against the Service Provider Parties relating in any way to the age or date of criminal history or other information that is searched or used by the Service Provider Parties, and you hereby fully waive, release and discharge the Service Provider Parties from any and all Claims relating to such events.

10.5 Collection, Use, Storage, Retention, and Protection of PII. The Service Provider stores on its computer servers certain biographic and biometric information it collects from individuals at Program registration, as well as updates to that information, Program participation information, and the results of Program Screenings. Some or all of this information constitutes PII. The Service Provider is committed to maintaining strict procedural, administrative, and technical controls to protect the privacy of all PII that it holds. The Service Provider is subject to rigorous Government oversight and audits of its information assurance practices. The Service Provider does not store on its servers or files Government database check records or commercial background screening reports on Program participants. Commercial background screening reports are stored with the Service Provider's third-party providers. The Service Provider requires its third-party providers to conform to high standards of care to protect PII.

Waiver and release: You agree that you have no financial, legal or other remedies, and will not initiate or join any legal action, against the Service Provider Parties relating in any way to your PII or other data on you that is not stored on the Service Provider's own servers or files, including but not limited to PII or other data on you that is stored by the Government or by the Service Provider's third-party providers, and you hereby fully waive, release and discharge the Service Provider Parties from any and all Claims relating to such PII or other data.

11. Limitation of Liability, Indemnification, Disclaimer of Warranties

11.1 Limitation of Liability. IN NO EVENT SHALL THE SERVICE PROVIDER PARTIES BE LIABLE FOR ANY DIRECT, INCIDENTAL OR CONSEQUENTIAL DAMAGES, PUNITIVE DAMAGES, OR LOST PROFITS, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS, RELATING IN ANY WAY TO THE PROGRAMS OR RELATING IN ANY WAY TO THIS AGREEMENT. Notwithstanding anything to the contrary in this Agreement, the maximum combined aggregate liability of the Service Provider Parties relating in any way to the Programs or relating in any way to this Agreement, is an amount equal to your registration fee for the applicable term.

11.2 Indemnification. The Service Provider is not responsible for your use of a Program, including but not limited to any misuse of a Program credential by you. You hereby agree to defend, indemnify and hold harmless the Service Provider Parties of and from any and all Claims relating in any way to your participation in the Programs, including but not limited to Claims relating to your use of your Program credential to gain access to, or to obtain privileges at, any Government or other facility or location.

11.3 Disclaimer of Warranties. THE SERVICE PROVIDER DISCLAIMS AND MAKES NO WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, TITLE, SECURITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, ACCURACY OF INFORMATION, PROGRAM CONTINUATION, OR INDIVIDUAL PARTICIPATION IN A PROGRAM. THE ENTIRE RISK OF THE USE OF ANY PROGRAM INCLUDING BUT NOT LIMITED TO ANY PROGRAM CREDENTIAL, CERTIFICATES, PRIVATE KEYS, ANY PIV-I SERVICES, OR THE VALIDATION OF ANY DIGITAL SIGNATURES, LIES WITH THE PARTICIPANT, RELYING PARTY, OR YOUR COMPANY.

12. Governing Law, Binding Arbitration and Class-Action Waiver

12.1 Governing Law and Binding Arbitration and Class-Action Waiver. PLEASE READ THIS SECTION CAREFULLY. IT AFFECTS YOUR LEGAL RIGHTS CONCERNING ANY DISPUTES, CLAIMS OR CONTROVERSIES (COLLECTIVELY "DISPUTES") BETWEEN YOU AND THE SERVICE PROVIDER PARTIES. YOU UNDERSTAND AND ACKNOWLEDGE THAT, BY AGREEING BELOW TO BINDING ARBITRATION, YOU ARE GIVING UP THE RIGHT TO LITIGATE (PARTICIPATE IN A LAWSUIT AS A PARTY OR CLASS MEMBER) ALL DISPUTES IN COURT BEFORE A JUDGE OR JURY. INSTEAD, YOU UNDERSTAND AND AGREE THAT ALL DISPUTES WILL BE RESOLVED BEFORE A SINGLE ARBITRATOR, WHOSE AWARD (DECISION) WILL BE BINDING AND FINAL, EXCEPT FOR A LIMITED RIGHT OF APPEAL UNDER THE FEDERAL ARBITRATION ACT. ANY COURT WITH JURISDICTION OVER THE PARTIES MAY ENFORCE THE ARBITRATOR'S AWARD.

12.2 Binding Arbitration. In the event any Dispute arises between you and the Service Provider Parties from or relating to the Programs or this Agreement that you and the Service Provider Parties are unable to resolve informally, you agree that the sole legal remedy shall be to refer such Dispute to binding arbitration before a single arbitrator pursuant to the rules of the American Arbitration Association or such other arbitration rules as you and the Service Provider Parties mutually agree to in writing. The arbitrator, and not any federal, state, or local court or agency, shall have exclusive authority to resolve any dispute relating to the interpretation, applicability, enforceability or formation of this Agreement including, but not limited to, any claim that all or any part of this Agreement is void or voidable. Unless otherwise required by applicable law, each party shall bear its own attorneys' fees without regard to which party is deemed to be the prevailing party in the arbitration proceeding. The arbitrator shall otherwise be authorized to award either party any remedy permitted by applicable law.

12.3 Time to Notify the Service Provider of Dispute. You agree that, if you have a Dispute with any Service Provider Party arising from or relating to the Programs or this Agreement, you must notify the Service Provider in writing within six (6) months of the event, act or omission giving

rise to the Dispute. You agree that you will be barred from initiating or maintaining any arbitration or legal proceeding against any of the Service Provider Parties if this notification requirement is not met.

12.4 Class Action Waiver. ANY DISPUTE RESOLUTION PROCEEDINGS, WHETHER IN ARBITRATION OR COURT, WILL BE CONDUCTED ONLY ON AN INDIVIDUAL BASIS AND NOT IN A CLASS OR REPRESENTATIVE ACTION OR AS A NAMED OR UNNAMED MEMBER IN A CLASS, CONSOLIDATED, REPRESENTATIVE OR PRIVATE ATTORNEY GENERAL ACTION, UNLESS BOTH YOU AND THE SERVICE PROVIDER SPECIFICALLY AGREE IN WRITING TO DO SO FOLLOWING INITIATION OF THE ARBITRATION.

12.5 Choice of Forum. All arbitration or other proceedings arising from or relating to the Programs or this Agreement, and any judicial actions brought to enforce an arbitrator's award or otherwise arising from or relating to the Programs or this Agreement, must be brought and maintained in Washington County or Multnomah County, Oregon.

12.6 Governing Law. This Agreement will be interpreted, construed, and enforced in accordance with the laws of the State of Oregon, without regard to its conflicts of law provisions.

13. Miscellaneous

13.1 Assignment. The Service Provider has the right to assign this Agreement, or any portion of this Agreement, to third parties including but not limited to any successors-in-interest of the Service Provider. You may not assign your rights and obligations under this Agreement unless you first obtain the written consent of the Service Provider.

13.2 Severability. If any provision of this Agreement is found by a proper legal authority to be unenforceable, that provision shall be severed and the remainder of this Agreement shall continue in full force and effect.

13.3 Entire Agreement. This Agreement constitutes the entire agreement between you and the Service Provider with respect to the Programs. This Agreement supersedes any proposal or any prior or contemporaneous writings or other agreements, oral or written, and any other communications or representations relating to the Programs.

13.4 Participant Changes to the Agreement. You may not make any changes to this Agreement unless an authorized representative of the Service Provider agrees in advance to the change in a signed written document.

13.5 Survival of Provisions. The provisions of Sections 2.5, 3.9, 4.10, 10, 11, 12, and 13 will survive the expiration or termination of this Agreement.

CHECK ONE BOX ONLY:

☐ **I DO NOT ACCEPT THE TERMS AND CONDITIONS OF THIS AGREEMENT (You will automatically quit registration)**

☐ **I ACCEPT THE TERMS AND CONDITIONS OF THIS AGREEMENT (You may proceed with registration)**