

National Automotive Service Task Force

Vehicle Security Team

VSP Registry & Secure Data Release Model Terms and Conditions of Use

1. Preamble, Purpose & Definitions.....	2
2. Policy	3
3. Procedures	7

Appendices:

Appendix A - CONTACT INFORMATION

Appendix B - REGISTRY DENIAL AND DISPUTE RESOLUTION APPEAL PROCESS

Appendix C - SECRETARY OF STATE PROOF OF GOOD STANDING

Appendix D - POSITIVE IDENTIFICATION/PROOF OF AUTHORITY

Appendix E - LOCKSMITH LICENSE REQUIREMENTS

1. Preamble, Purpose & Definitions

- 1.1. The work and intent of the National Automotive Service Task Force, hereafter referred to as “NASTF”, and the Vehicle Security Team, hereafter referred to as “VST”, is to provide secure access to security related service information, including key codes, immobilizer reset information, security Personal Identification Numbers (PINs) and other information necessary to successfully enter, start and operate automobiles and light trucks at the request of retail consumers and commercial entities or municipalities that can demonstrate ownership of the vehicle.
- 1.2. The Vehicle Security Professional Registry, hereafter referred to as “the Registry” and Secure Data Release Model, hereafter referred to as “SDRM”, give automakers a flexible system to support 24/7 access to vehicle security information for pre-approved locksmiths and technicians. It allows aftermarket

service providers to support consumer needs without undermining the integrity and basic purpose of the vehicle security systems.

- 1.3. This secure access to security related service information can include, but is not limited to, mechanical key codes, electronic key codes, immobilizer reset codes, PIN codes, immobilizer seed and key system information, radio lockout codes, remote codes, security related access to vehicle networks, confirmation of credential for security parts purchase, tool access authorization and successor technologies.
- 1.4. For the purposes of this document, automobile and truck manufacturers will be collectively referred to as “automakers”.
- 1.5. For purposes of “the Registry” and “SDRM”, automobiles are defined as passenger vehicles and light trucks are defined as pickup trucks, SUVs, vans and other light duty vehicles, excluding house cars, motor homes, motorcycles or other two-wheeled motor vehicles.
- 1.6. “The Registry” has been established in cooperation with participating automakers to facilitate the availability of security related service information to Vehicle Security Professionals, hereafter referred to as VSPs, to support vehicle owners.
- 1.7. Once accepted into “the Registry”, every “VSP” will be assigned a unique Vehicle Security Professional Identification number, referred to hereafter as “VSP ID”
- 1.8. NASTF reserves the right, in its sole discretion, to change these terms and conditions at any time as needed to respond to security threats.
- 1.9. NASTF reserves the right, in its sole discretion, to determine a breach in any term or condition set forth herein, and that all determinations of the “Registry Manager” upheld by the NASTF Appeals Review Process are final.

2. Policy

- 2.1. Under the “SDRM”, security related service information is typically obtained directly from participating automakers through internet websites and/or similar successor technologies. Automakers may require individual registration,

subscriptions, and/or use fees and adherence to their own terms and conditions for use of/access to the websites.

- 2.2. To gain access to security related service information from participating automakers, all users must be pre-validated by enrolling in “the Registry” and undergoing a criminal background check process.
- 2.3. “The Registry” is maintained by a registry manager appointed by NASTF (the “Registry Manager”). The Registry Manager oversees the operation of the Registry on behalf of “NASTF”. Contact information is identified in Attachment A – Contact Information.
- 2.4. “The Registry” is only available for use by individuals working in businesses (sole proprietorships, partnerships and corporations) that have a U.S. Federal taxpayer identification number or Canadian Business Number (which must be provided during the application process), are properly licensed and registered in all municipalities in which they do business, are in good standing in the jurisdictions where they conduct business and whose primary business provides repair or replacement services directly to the registered owners of the automobile for which the security related service information is being obtained to include privately owned, business owned, government owned vehicles (sold in North America) and in instances where a power of attorney has been granted in the case of collision repair or estate management of a deceased owner. Any other uses are at the sole discretion of participating automakers.
- 2.5. Registry VSP ID account holders fall into three categories, “Primary”, “Subordinate” or “Company Admin”. All registry applicants must be at least 18 years of age at the time of application and be authorized to work in the U.S. or Canada. NOTE: All Canadian accounts must be registered as a Primary VSP.
 - 2.5.1. Issued “VSP ID Registry” credentials are ONLY issued to persons who apply to access the registry who have granted access to obtain and utilize the information from automaker websites to service vehicles. “The Registry” credentials do not extend to other employees within the

business. Each member of the business staff will need to apply and be issued their own VSP ID credentials to use the automakers websites to acquire vehicle security data. Business owners should apply for additional primary and subordinate accounts deemed necessary to support their business operations. It is to be understood that sharing VSP ID account credentials between employees and technicians is not permitted by the automakers.

- 2.6. The Primary VSP ID account holder is often, but not required to be, the business owner. In a multiple VSP business, the primary account holder should be the person directly managing any subordinate accounts. The Primary VSP ID account holder will be required to register individually. The Primary account holder is responsible for all transactions and registry activity that occur on the business' account.
- 2.7. The Primary VSP ID account holder may:
 - 2.7.1. Add a Subordinate by completing an application in the SDRM Portal <https://sdrm.nastf.org>
 - 2.7.2. Change account access permissions for a "Subordinate or Company Admin"
 - 2.7.3. Manage account information for the business (phone numbers, addresses, e-mail addresses, etc)
 - 2.7.4. Sub-Accounts are only available in the US to W2 employees working in the US. All Canadian accounts are to be registered as Primary VSPs.
- 2.8. The Primary VSP ID account holder is responsible for all transactions that occur by Subordinates.
- 2.9. The Primary VSP account holder must be located within a "reasonable distance" of the subordinate's location to be able to properly manage operations.
 - 2.9.1. "Reasonable Distances" will be determined by the Registry Manager based on various criteria such as distance, business organizational plans, number of VSP ID accounts, and potential security risks.

- 2.10. Subordinate VSP ID account holders must manage their own passwords and generate Positive ID/Customer Authorization (D1) Forms.
- 2.11. Requests for support for Subordinates outside of these two areas shall be submitted by the Primary account holder.
- 2.12. Sub-Accounts are only available in the US to W2 employees working in the US. All Canadian accounts are to be registered Primary VSPs.
- 2.13. VSP ID number: Upon acceptance into “the Registry”, every VSP ID account holder, Primary, Subordinate or Company Admin, is assigned their own unique VSP ID that is associated with the registered business.
- 2.14. Subordinate VSP ID account holders require background checks that are performed by NASTF to the same standards as Primary account holders.
- 2.15. The Company Admin account holder is an account that allows the business to identify individuals who may assist with starting Customer Authorization forms and updating company documents within the SDRM portal. This account does not have access to security operations on automaker websites. The Primary VSP ID account holder will be required to register and manage Company Admin accounts.
- 2.16. Subcontractors: A business using “the Registry” shall not provide vehicle security information acquired through use of “the Registry” to a subcontractor or an independent contractor (as determined in accordance with the Internal Revenue Code and related rules and regulations).
- 2.17. A business using “the Registry” (Business A) may use subcontractors and / or independent contractors who are also registered VSP ID account holders under a different business account (Business B); however, Business B must acquire their vehicle security information under their own VSP ID business account and complete the appropriate customer authorization form for the operation.
- 2.18. It is a violation of the law for a VSP to access information on an automaker site without proper authorization or to use it in an unauthorized manner.

- 2.19. The Information, if mishandled, may pose a risk of property loss to the Vehicle Owner or others. Therefore, all VSP account holders shall:
- 2.19.1.1. treat the Information as strictly confidential;
 - 2.19.1.2. the Information is for single use and not to be stored;
 - 2.19.1.3. the information is not to be transmitted electronically;
 - 2.19.1.4. take all measures necessary to keep the Information secure, including, but not limited to, all measures requested by the automaker and NASTF;
 - 2.19.1.5. not disclose the information to anyone other than the Vehicle Owner, or his/her designee; and
 - 2.19.1.6. not use the Information for any unauthorized purpose whatsoever.
- 2.20. Expiration of VSP ID account: A VSP ID account is valid for two years.
- 2.21. Prior to account expiration, a renewal application must be submitted along with the appropriate fees and other information as indicated on the Registry website; adequate time must be provided for application validation and new background check to avoid gaps in information accessibility. NASTF recommends submitting renewal applications 60 days in advance and no less than 30 for uninterrupted access.
- 2.22. Initiating a dispute or chargeback with your credit card company without first opening a support case with NASTF shall constitute a violation of the Terms and Conditions and will result in permanent suspension from the Registry. If you wish to withdraw your application contact support@sdrm.nastf.org and provide a reason for withdrawal. Your request will be honored if the request comes later than 24 hours after the application is submitted. The \$100 application fee will become nonrefundable after that window.
- 2.23. If the applicant violates the terms and conditions and/or attempts to mislead the NASTF registry team by providing fraudulent information or altered documents, the application or account will be permanently suspended and refund requests

will not be honored. After the approval of an application, credit card charge backs will be classified as fraud. NASTF will, at its discretion, forward information concerning fraudulent acts to law enforcement for review.

- 2.24. When a Primary VSP ID account holder's account expires, the accounts of all Subordinate VSP IDs shall be suspended until the primary account is renewed and approved.
- 2.25. If any of the requirements for a VSP ID account change status during the two-year term of registration (i.e. expiration of insurance, licenses, fidelity bond, termination of a business entity), it is the responsibility of the Primary VSP ID account holder to upload current information within 15 days of the change. If current documentation is not on file in the SDRM portal, all accounts will be suspended.
- 2.26. If any required documentation expires during the two-year term of registration for any primary or subordinate account, the Primary VSP ID account holder is required to upload current replacement documents within a 15-day grace period of the expiration. Registry software will attempt to provide email notice as well as notifications upon login prior to expiration, but it is ultimately the responsibility of the Primary VSP ID account holder to maintain current documentation for all business accounts.
- 2.27. Conditions of access and use of information acquired through "the Registry":
 - 2.27.1. Security related service information acquired through use of "the Registry" is acquired by a VSP ID account holder for the direct and primary benefit of the registered vehicle owner and is provided under the condition that the VSP ID account holder follow all conditions of the "Positive Identification Policy" defined in Attachment D.
 - 2.27.2. All security related information may only be acquired at the time of service by the VSP ID account holder. The VSP ID account holder must be present with the customer and vehicle to positively confirm ownership

- and verification of the vehicle prior to utilizing the security related information to service the vehicle.
- 2.27.3. It is a violation of the terms of Registry use for a VSP ID account holder to retain, database or electronically transfer any security related information before, during or after a transaction has been completed with the registered owner.
 - 2.27.4. It is a violation of the terms of Registry use for a VSP ID account holder not to respond and/or provide information requested by the Registry Manager during the course of a Registry application or vehicle security information usage audit within 7 calendar days of the audit email request and notification being sent.
 - 2.27.5. Security related service information acquired or devices created through use of “the Registry” shall not be sold, bought, traded, bartered or shared in any way with any individual, business, entity, or person(s) other than the registered vehicle owner.
 - 2.27.6. Under no circumstances shall registry data be used to create and mail a vehicle security device to include keys, fobs or control modules.
- 2.28. The National Insurance Crime Bureau (NICB) or other law enforcement auto theft related activities: NICB and other law enforcement officials may submit auto theft inquiries to NASTF. If it is determined that there is an auto theft reported by NICB or other law enforcement agencies that is linked to a VSP ID holder, the account will be immediately suspended without notice pending the disposition of the auto theft report.
- 2.29. Violations of Registry terms of use: Any VSP ID account holder who is aware of any misuse of the Registry shall immediately report said misuse directly to “NASTF VSP ID Registry” by contacting NASTF support email or phone number (as identified in Attachment A – Contact Information).

- 2.30. Upon investigation and verification of misuse, the VSP ID account holder will be suspended from having access to “the Registry” and may be permanently restricted from being issued any subsequent VSP ID number/account.
- 2.31. Failure to report known misuse of the Registry constitutes violation of the Terms and Conditions of use of the Registry. “Failure to report” may result in removal from the Registry and permanent restriction from being issued any subsequent VSP ID number/account.
- 2.32. Sharing of user names and passwords between individuals is expressly prohibited. Breach of this policy will result in action against the VSP ID business owner, including potential removal from the Registry and permanent restriction from being issued any subsequent VSP ID number/account.
- 2.33. The VSP ID is to be used by one individual only. This individual must be present and performing the work on the vehicle or, in the case of auto repair, directly supervising the work with a technician.
 - 2.33.1. Allowing a technician to access the registry does not qualify as supervision.
 - 2.33.2. A business owner sharing access with the entire shop for Mercedes Benz Theft-Relevant Parts purchases is not an accepted use.
- 2.34. All requests for support and technical assistance must come from the registered VSP Primary account holder.
- 2.35. When a VSP ID account holder is suspended or terminated from the Registry, they can appeal the action to the NASTF Security Review Committee (the “APPEALS REVIEW COMMITTEE”). The full process is detailed in Attachment B - Registry Denial and Dispute Resolution Appeal Process.
- 2.36. Customer information: Use of the Registry may require the VSP ID account holder to collect, review, and record certain Personally Identifiable Information (PII) from the customer. Information that may be required includes, but is not limited to:
 - 2.36.1. The customer’s full legal name

- 2.36.2. Visual verification of a valid vehicle registration document
- 2.36.3. Visual verification of a valid U.S. or Canadian driver's license valid exception would be if the owner's license had been stolen (See below attachment D)
- 2.37. It is the responsibility of the VSP ID account holder to handle any Personally Identifiable Information in strict confidence of the registered vehicle owner and in compliance with all applicable federal, state and local regulations and/or statutes. (If SDRM software is used to take pictures they will not be stored on the VSPs device)
- 2.38. To enroll in "the Registry", a VSP/business must perform and or submit by upload the following:
 - 2.38.1. Complete online Registry Application and confirm acceptance of the User Agreement located at <https://sdrm.nastf.org>.
 - 2.38.2. Upload current and legible copies of all required and applicable supporting documents and information.

Application Checklist



Primary Application (New and Renewal) Checklist

To assist us in providing the fastest review of your application please use this check list to confirm that you have all of the necessary current documents to complete your application

- Commercial General Liability Insurance**
Primary accounts require at least a 1 million dollar aggregate/\$500,000 per event liability policy. Please note: NASTF's address for the certificate is 4501 Harlan St. Wheat Ridge, CO 80033. The COI must be emailed by your insurance agent to COI@nastf.org. Please ask your agent NOT to mail a certificate of insurance to NASTF. Your insurance agent must email a new copy when the policy renews or changes. NASTF will remind you by email 60 days prior of expiration to replace with a current document.
- Driver's License**
A valid US or Canadian Driver's license from the state or province in which you do business - Clear, color picture or copy. Please be sure it is legible. Temporary Driver's license or any other form of ID is not accepted.
- Proof of Business in Good Standing**
Please upload a dated Certificate of Good Standing from your secretary of state website. The Secretary of State Statements of Good Standing documents can be easily downloaded by visiting your state's Secretary of State website. The statement can also be displayed on screen and then captured for upload to SDRM by using Windows key + Shift + S in Windows 10. Apple users can use "Screenshot". Save the file to your computer and use the upload button in SDRM. NASTF will remind you by email 60 days prior to expiration.
NOTE: If operating as an auto repair business in the state of California, it is required to provide a copy of your certificate issued by the California Bureau of Automotive Repair.
- Proof of Ownership/Employment**
The proof of ownership/employment document must confirm that the applicant is the owner or full time (not contract or 1099) employee of the business. This may be done by uploading the most recent W2 with all but the last 4 digits of the social security number redacted or current pay stub identifying the employees and employer's name. W4s and W9s are not accepted.
- Locksmith License (if required by State, Province or Municipality)**
If you use registry data to acquire key codes you are a locksmith and in states, counties, and cities that require licensing a locksmith license for the individual applicant must be provided. Your Business Locksmith Certificate will not be accepted. This is required for all states/ provinces and municipalities in which you do business - Service repair providers who ONLY use immobilizer codes for repairs are exempt at this time.
- Additional Items.**
 - US -Federal Employer Identification number (FEIN) - Canadians, your Business Number - This number will be entered into your profile for cross-reference with government agencies.
 - Insurance agent name and phone are required - Please enter accurate information to allow NASTF to call and confirm coverage.
 - 2 professional references (not family) individual names and direct phone numbers - Business names or 800 numbers are not accepted as they delay processing your application.
 - Term and Conditions - It is the responsibility of ALL VSPs to understand the rules of the program. They are found at the bottom of every page on the website. Please be certain that you have read them and if you have questions ask support@nastf.org for assistance. Hours of operation are Monday through Friday, 9:00 AM to 6:00 PM Eastern Standard Time.

Important Notes:

- Vehicle Security Professional Registry access is granted to an individual not an organization.
- NASTF SDRM Credentials, vehicle security information, and keys originated with information obtained with your SDRM Credentials cannot be shared with employees or staff members.
- Registered VSPs must be present with the customer and vehicle to verify ownership and legal possession before using vehicle security information.
- If you have questions about your current business operating within policy, please contact the NASTF Support Center for assistance.

When you have all of your documents ready, start your application at sdrm.nastf.org



Subordinate Application (New and Renewal) Checklist

To assist us in providing the fastest review of your application please use this check list to confirm that you have all of the necessary current documents to complete your application

- Bonding**
In addition to the Liability policy for the Primary, businesses must carry a minimum \$100,000 employee dishonesty/surety bond for registered sub accounts. In many cases if there are only 1-3 sub accounts it may be more cost effective to register them as primary accounts than pay for a bond. The COI must be updated to include the employee dishonesty bond policy information and emailed by your insurance agent to COI@nastf.org. Please ask your agent NOT to mail a certificate of insurance to NASTF. Your insurance agent must email a new copy when the policy renews or changes. NASTF will remind you by email 60 days prior to expiration to replace with a current document.
- Driver's License**
A valid US license from the state or province in which you do business - Clear, color picture or copy. Please be sure it is legible. Temporary Driver's license or any other form of ID is not accepted.
- Locksmith License (if required by State or Municipality)**
If you use registry data to acquire key codes you are a locksmith and in states, counties, and cities that require licensing a locksmith license for the individual applicant must be provided. Your Business Locksmith Certificate will not be accepted. This is required for all states/ provinces and municipalities in which you do business - Service repair providers who ONLY use immobilizer codes for repairs are exempt at this time.
- Proof of employment**
The primary must attest and document that the employee is a full time (not contract or 1099) employee of the business. This may be by the following methods:
 Upload a current and complete W2 (the social security number should have all but the last 4 digits redacted)
 Upload a current pay stub with only the income redacted.
 Or by a letter signed by the principal/HR department of the corporation or municipality
W4s are no longer accepted.
 Additional information may be requested during the approval process.

Subordinate accounts are created by the Primary account holder. The primary account holder is responsible for the actions of subordinates. Subordinates **MUST BE** under the direct supervision of the Primary and within a reasonable geographical distance to affect actual oversight. Sub-Accounts are only available in the US to W2 employees working in the US. All Canadian accounts must be submitted as Primary accounts.

- Important Notes:**
- Vehicle Security Professional Registry access is granted to an individual not an organization.
 - NASTF SDRM Credentials, vehicle security information, and keys originated with information obtained with your SDRM Credentials cannot be shared with employees or staff members.
 - Registered VSPs must be present with the customer and vehicle to verify ownership and legal possession before using vehicle security information.
 - If you have questions about your current business operating within policy, please contact the NASTF Support Center for assistance.

When you have all of your documents ready, start your application at <https://nastf.org>

A VSP ID applicant will be background checked as per the procedures and to the standards established by NASTF and its background check partner.

A felony or equivalent criminal arrest or conviction may exclude an applicant. All denied applications can be referred to the NASTF Appeals Review Committee for review at the request of the applicant (see Attachment B – Registry Denial and Dispute Resolution Appeal Process).

VSP ID account enrollment denials and VSP ID terminations may be appealed to the NASTF Appeals Review Committee through the registry appeals process as outlined in Attachment B – Registry Denial and Dispute Resolution Appeal Process.

APPENDIX A - CONTACT INFORMATION

SDRM Support Desk	National Automotive Service Task Force SDRM Registry Manager	National Automotive Service Task Force Executive Officer/Managing Director
Hours 9-6pm Eastern		4501 Harlan St
Toll free (810-289-4809)	Toll free (810-289-4809)	Wheat Ridge, CO, 80033
Email: support@sdrm.NASTF.org	Email: support@NASTF.org	Toll free (810-289-4809)
		Email: support@NASTF.org

<p>Roles:</p> <ul style="list-style-type: none"> • Registry User Support • Payment questions • System use assistance • Application assistance 	<p>Roles:</p> <ul style="list-style-type: none"> • Registry Administration • Registry Info & Promotion • Application Processing • Background Checks • Record Maintenance • SDRM VSP Audits • Investigations • Law Enforcement Liaison 	<p>Roles:</p> <ul style="list-style-type: none"> • NASTF Administration • NASTF Media contact • OEM point of contact • NASTF.org and SDRM website content • Service Information Requests • Dispute Resolution • SDRM Appeals Reviews Committee • Maintenance and Implementation of OEM Information Standards Agreements • Assessment of Service Information products and diagnostic tools. • Identification of gaps in automotive service information, tools and training. • NASTF Team Support
---	---	--

APPENDIX B - REGISTRY DENIAL/DISPUTE RESOLUTION APPEAL PROCESS

An applicant or VSP ID account holder will have the right to appeal to the NASTF Appeals Review Committee for the following:

- (a) a decision by the Registry Manager to deny the applicants inclusion on the Registry,
- (b) a decision by the Registry Manager to suspend or terminate a VSP ID account holder’s access to the Registry, and
- (c) a denial by a Participating Automaker to permit access by the VSP ID account holder to Security Data on terms and conditions available to other VSP ID account holders.

RESPONSIBILITIES:

The NASTF SDRM Registry Managers duties, include without limitation:

- (1) administering the application process, managing background checks and making approval decisions on applicants based on criteria established by the NASTF Vehicle Security Policy Working Group.

(2) Reviewing all reports of improper use of the Registry, suspending accounts in cases of reported impropriety, and in response to receiving an official appeal, forwarding evidence of said improprieties to the NASTF Appeals Review Committee and Law Enforcement (as appropriate or requested) for final disposition. The Registry Manager is required to take adverse action on a VSP ID account if the NASTF Appeals Review Committee determines that reported impropriety is accurate.

The NASTF Appeals Review Committee is responsible for reviewing and making final decisions on rejected Registry applications that have been submitted for appeal.

The NASTF Appeals Review Committee will have seven (7) members. NASTF Appeals Review Committee members will be appointed by the NASTF Chairman. The NASTF Appeals Review Committee will include one (1) director from the NASTF Board of Directors who will serve as chairman of the Committee, and six (6) members from across all stakeholders in SDRM to include Service Repair, Automakers, Locksmiths and Tool companies. Appointments to the NASTF Appeals Review Committee will be for a period of two (2) years. Committee members may be reappointed and there is no limit on the number of years an individual may serve in this capacity.

Registry Application Denial Appeal Process

The NASTF Registry Manager may deny an applicant inclusion in the Registry for a number of reasons related to providing fraudulent information, prior or continued misuse of the Registry or non-compliance to automaker policies. The applicant may use the application denial appeal process by following these steps:

- 1) NASTF Appeals Review Committee: Upon receipt of the denial email notification from the Registry Manager, the applicant has ten (10) business days to provide email notification of an appeal to the NASTF Support Desk. (All support desk contacts are time and date stamped by the system)
- 2) Appeal must be addressed to support@sdrm.nastf.org

- 3) Appeal should contain supporting documents or information that refutes the Registry Manager's decision.
- 4) By submitting an appeal, it is agreed that:
 - a. The applicant grants permission for the NASTF Appeals Review Committee to access and review the same information that caused the denial for inclusion in the SDRM Registry.
 - b. The applicant acknowledges the determination of the NASTF Appeals Review Committee is final and the individual will not seek any remedy, legal or otherwise, beyond the scope of the appeals review process. A denied applicant cannot reapply for one (1) year from the date of receipt of the denied appeal decision unless otherwise noted in the final disposition NASTF Appeals Review Committee.
- 5) The Registry Manager or designee, upon receipt of the appeal, will provide electronic copies of supporting documents used to deny Registry access to the NASTF Executive Officer and will confirm whether or not the supporting documents and application are complete and sufficient to begin the appeal process.
- 6) Once determined complete, this information will be forwarded to the NASTF Appeals Review Committee opening the Dispute Resolution Appeal process.
- 7) The NASTF Appeals Review Committee will convene a meeting within ten (10) business days of receipt of supporting information from the NASTF Executive Officer or designee.
- 8) The applicant will be notified of the NASTF Appeals Review Committee decision within fourteen (14) days from the date of the NASTF Appeals Review Committee appeal hearing. The notification will be sent to the applicant by email from the account registered with SDRM.

Registry Suspension Dispute Resolution Appeal Process

The Dispute Resolution Appeal (DRA) process will allow a Primary VSP ID account holder to submit a rebuttal and appeal to the NASTF Appeals Review Committee in cases where a VSP ID account has been suspended. This is an opportunity for the VSP ID account holder to provide

additional information to the NASTF Appeals Review Committee, relevant to their circumstance. The appeals review process is outlined below:

- 1) Per Section 2.30, when a VSP knows of another's violation of the terms and conditions, they are obligated to report said violation along with evidence of said violation to the NASTF SDRM Support Desk. The NASTF Registry Manager, upon receipt of this evidence, shall suspend the account after completing an independent investigative inquiry. The Registry Manager will initiate communications with the VSP ID account holder as it concerns the policy violations allegations.
- 2) The VSP ID account holder may appeal a suspension to the NASTF Appeals Review Committee by following steps 2 through 8 of the Registry Denial Dispute Resolution Appeal process.

APPENDIX C – SECRETARY OF STATE GOOD STANDING

VSP Account applicants are required to provide a Certificate of Good Standing from your Secretary of State. These can be obtained in nearly all cases by a dated screen capture or file download. This document may be in the form of a dated downloaded PDF, a screen capture or a scanned file. This document must have the name of the business entity as registered with NASTF. If the VSP ID Account holder is operating as a DBA or filed under a fictitious name, you must provide a supporting government document that shows that relationship. As a standalone document, a DBA form and other notarized applications will not be accepted. Based on the classification of your business operations, if the state does not require a business license, please provide documentation from the state to confirm the exemption. In this instance, if you cannot provide a state document or a reference to the exception, please use the guidance provided to meet this NASTF requirement. NOTE: If operating as an auto repair business in the state of California, it is required to provide a copy of the certificate issued by the California Bureau of Automotive Repair.

Locksmith certificates are not accepted as business licenses. The point of this requirement is for the VSP ID account holder to show that your business is in good standing with the state

where your operations are located. Locksmith certificates do not provide information that your business is in good standing or active.

APPENDIX D – Positive Identification/Proof of Authority

The Positive Identification of the vehicle owner or proof of legal authority to access a vehicle has been outlined throughout this document. The following are general requirements. NASTF has produced several training videos to assist VSPs in learning to use the electronic D1 (named after this portion of the terms and conditions when the form was physical). These steps can be found within the SDRM Portal. All VSP Account Holders must take the following steps prior to accessing the Information for a Vehicle Owner:

Verify the identity of the Vehicle Owner.

- a. If the Vehicle Owner is an individual, this requires verifying the requesting individual's identity through a U.S or Canadian driver's license (no other form of identification is accepted. The only valid exception would be if the owner's license had been stolen and the owner could prove the theft. In this case, a passport or other government issued ID can be accepted). A picture of this proof of identity with the method of authorization confirmation (described in Attachment D items 2 and 3) shall be uploaded to the system.
- b. If the Vehicle Owner is a lienholder or other corporate entity, this requires verifying the requesting individual's authority and identity through a driver's license and photographic proof that the individual is an employee of the Vehicle Owner (e.g. an employee ID card). This ID is not required to be photographed and uploaded.
- c. If the Vehicle Owner is a family member, spouse, caretaker or other designated by the authorized owner, this requires verifying the requesting individual's authority and identity through a driver's license and photographic or written proof that the individual is a designated person of the Vehicle Owner. This photographic or written proof as well

as the designation should be verified by the VSP having direct contact the authorized owner.

1. Verify ownership of the vehicle. This requires verifying proof of title (or repossession title), vehicle registration, or similar documentation establishing clear ownership or authority to take possession of the vehicle.
2. Verify that the ownership documentation matches the Vehicle Owner's identity and address (or last name and address if the requesting party is a family member of the registered owner).
3. Verify that the vehicle identification number (VIN) of the vehicle matches the vehicle identification number on the ownership documentation.
4. Comply with all other applicable federal, state, and local regulations and/or statutes.
5. Complete the appropriate electronic NASTF Customer Authorization (D1) form for the type of transaction you perform in the SDRM portal within 5 days of the automaker transaction.
6. If in doubt, please contact support@sdrm.nastf.org for assistance.

APPENDIX E – Locksmith License requirements

Many states, Canadian provinces, cities and municipalities require that a security professional possess a locksmith license. To harmonize with these regulations, NASTF will require a locksmith license for anyone who uses the registry to access keycodes. By definition, any individual physically cutting keys will be considered a locksmith by NASTF in all jurisdictions that require a license. Currently, repair professionals who utilize immobilizer codes to replace, calibrate or reprogram modules during the course of repair are exempt from this rule. NASTF will adhere to all municipalities' rules. If a business operates in one of these locations, regardless of the business's physical address, the VSP must be credentialed in that locale. The following is a list of areas that require certification is provided as guidance and may not be all inclusive.

LOCKSMITH LICENSE

<p>Locations that require locksmiths to be registered/licensed. alabama.gov - Pocket card california.gov -DCA Pocket Card connecticut.gov Technician Certificate florida.hillsboroughcounty.org *Cities listed to the right-Each tech must be registered with the county via attachment florida.miamidade.gov *Pocket card-City listed to the right Illinois.com- PERC card for each tech louisiana.gov- Technician Certificate maryland.us Each tech must be registered with the state via attachment employee list north carolina.org- Pocket card lasvegasnevada.gov -Clark County Sheriff Registration Card new jersey.gov Technician Certificate new york city.gov New York City – Pocket card - All Boroughs oklahoma.gov Technician Certificate; Does not expired but must identify current business information oregon.gov -Technician Certificate texas.gov Each -Private Security Registration Card required virginia.gov- Technician Certificate or pocket card</p>	<p>Miami Dade County Cities that require Locksmith License</p> <ul style="list-style-type: none"> • Brownsville • Coral Terrace • Country Club • Country Walk • Fisher Island • Fontainebleau • Gladeview • Glenvar Heights • Golden Glades • Goulds • Homestead Base • Ives Estates • Kendale Lakes • Kendall • Kendall West • Leisure City • Naranja • Ojus • Olympia Heights • Palm Springs North 	<p>Miami Dade County continued...</p> <ul style="list-style-type: none"> • Palmetto Estates • Pinewood • Princeton Richmond Heights • Richmond West • South Miami Heights • Sunset • Tamiami • The Crossings • The Hammocks • Three Lakes • University Park • West Little River • West Perrine • Westchester • Westview • Westwood Lake 	<p>Hillsborough County Cities that require Locksmith License</p> <ul style="list-style-type: none"> • Apollo Beach • Balm • Brandon • Dover • Durant • Gibsonton • Lithia • Lutz • Mango • Odessa • Plant City • Riverview • Ruskin • Seffner • Sun City • Sun City Center • Sydney • Tampa • Thonotosassa • Valrico • Wimauma
--	---	--	--