



# **State of New Mexico**

**DATE OF REPORT: 2-7-2019**

## **Payment Card Industry (PCI) Data Security Standard**

---

### **Attestation of Compliance for Onsite Assessments – Merchants**

**Version 3.2.1**

June 2018

## Section 1: Assessment Information

### Instructions for Submission

This Attestation of Compliance must be completed as a declaration of the results of the merchant's assessment with the *Payment Card Industry Data Security Standard Requirements and Security Assessment Procedures (PCI DSS)*. Complete all sections: The merchant is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact your acquirer (merchant bank) or the payment brands for reporting and submission procedures.

#### Part 1. Merchant and Qualified Security Assessor Information

##### Part 1a. Merchant Organization Information

Company Name:	State of New Mexico	DBA (doing business as):	
Contact Name:	Ron Spilman	Title:	State Controller
Telephone:	505-827-3934	E-mail:	Ronald.Spilman@state.nm.us
Business Address:	180 Bataan Memorial Building	City:	Santa Fe
State/Province:	NM	Country:	USA
URL:	http://nmdfa.state.nm.us , http://www.newmexico.gov		
		Zip:	87501

##### Part 1b. Qualified Security Assessor Company Information (if applicable)

Company Name:	RiskSense, Inc.		
Lead QSA Contact Name:	Robert Childs	Title:	CSO, VP GRC
Telephone:	505-217-9422	E-mail:	robert.childs@risksense.com
Business Address:	4200 Osuna Rd NE	City:	Albuquerque
State/Province:	NM	Country:	USA
URL:	www.risksense.com		
		Zip:	87109

#### Part 2. Executive Summary

##### Part 2a. Type of Merchant Business (check all that apply)

- Retailer
  Telecommunication
  Grocery and Supermarkets  
 Petroleum
  E-Commerce
  Mail order/telephone order (MOTO)  
 Others (please specify): State Government Agencies

What types of payment channels does your business serve?

- Mail order/telephone order (MOTO)  
 E-Commerce  
 Card-present (face-to-face)

Which payment channels are covered by this assessment?

- Mail order/telephone order (MOTO)  
 E-Commerce  
 Card-present (face-to-face)

**Note:** If your organization has a payment channel or process that is not covered by this assessment, consult your acquirer or payment brand about validation for the other channels.

---

**Part 2b. Description of Payment Card Business**

---



How and in what capacity does your business store, process and/or transmit cardholder data?

The State of New Mexico (SONM) provides government services of various types for the SONM's citizens. Services are provided through a number of individual State agencies. A few agencies also provide products for sale. Services include but are not limited to: state tax administration and collection, driver's licenses, vehicle registrations, professional licenses and registrations, medical licenses, hunting and fishing licenses, tourism related products, state parks fees, museum tickets, corporate registrations, court fees, highway usage fees, airplane registrations, State Fair fees, and miscellaneous other services and products. Agencies accept credit card payment for these fees, services and products.

For the PCI audit, 23 State agencies, boards and commissions (collectively referred to as 'agencies') were identified and included in the scope of this PCI DSS audit for 2018. These agencies are:

1. (AOC) Administrative Office of the Courts
2. (BON) Board of Nursing
3. (CC) Compilation Commission
4. (CD) Corrections Department
5. (DCA) Department of Cultural Affairs
6. (DGF) Department of Game and Fish
7. (DOH) Department of Health
8. (DoIT) Department of Information Technology
9. (DOT) Department of Transportation
10. (DPS) Department of Public Safety
11. (DWS) Department of Workforce Solutions
12. (ENMRD) Energy Minerals and Natural Resources Department
13. (EXPO) Expo NM
14. (GSD) General Services Department
15. (LB) Livestock Board
16. (MB) Medical Board
17. (PED) Public Education Department
18. (RLD) Regulation and Licensing Department
19. (SA) Spaceport Authority
20. (SOS) Secretary of State
21. (STO) State Treasurer's Office
22. (TD) Tourism Department
23. (TRD) Taxation and Revenue Department

The Department of Information Technology (DoIT) is included as this agency provides the State's central physical data center, State's overall network backbone and Internet connections, and other services to agencies. As such, it's data center and certain services are in scope.

The State Treasurer's Office (STO) provides service provider (PCI DSS Requirement 12.8) support to all agencies using the common State Bank and card processor's, CyberSource / Wells Fargo.

Each agency is essentially an independent organization, mostly operating independently of the other agencies, though a few interact with other agencies. Each of the agencies in scope accepts credit card payments for their services and

products. Each agency has payment processes unique to their operational purposes. Collectively, card payments are accepted via e-commerce web sites (hosted and outsourced), over the phone, card present via Point of Sale (POS) devices or entered via workstations; and kiosk PC's.

**Part 2c. Locations**

List types of facilities (for example, retail outlets, corporate offices, data centers, call centers, etc.) and a summary of locations included in the PCI DSS review.

Type of facility	Number of facilities of this type	Location(s) of facility (city, country)
<i>Example: Retail outlets</i>	3	Boston, MA, USA
Agency Main Offices	23	Santa Fe, NM, and Albuquerque, NM
Field Offices - MVD (TRD)	70	Various cities and towns around the State of NM
Remote Offices , facilities – various	40+	Various locations around the State of NM for different agencies such as ports of entry, state parks, as well as remote offices.
Museums	7	Santa Fe, Albuquerque, Alamogordo, and Las Cruces, NM

**Part 2d. Payment Application**

Does the organization use one or more Payment Applications?  Yes  No

Provide the following information regarding the Payment Applications your organization uses:

Payment Application Name	Version Number	Application Vendor	Is application PA-DSS Listed?	PA-DSS Listing Expiry date (if applicable)
MyLicense eGov	2.4	System Automation Corp	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	NA
Online Sales and Vendor Sales e-Commerce Applications	NA	DGF In-house Developed	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	NA
Accela	7.3.3.3	Accela	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	NA
Clover Flex	Flex	Clover	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	2017-00893.001 (P2PE)
Grant Street Group PaymentExpress (using Voltage Point-to-Point Encryption P2PE on Ingenico iPP320 terminals)	iPP320 HPE Security / Voltage	Grant Street / Payment Express	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	NA



**Part 2e. Description of Environment**

Provide a **high-level** description of the environment covered by this assessment.

*For example:*

- *Connections into and out of the cardholder data environment (CDE).*
- *Critical system components within the CDE, such as POS devices, databases, web servers, etc., and any other necessary payment components, as applicable.*

This assessment covers 23 NM State agencies, boards and commissions (collectively referred to as 'agencies'), including the State's central data center operations and facility. 21 agencies provide various types of services, products or collect fees for which they accept credit card payments. Each agency has its own network and systems, and all use the central state data center for housing their equipment and use the State's backbone network to connect to the Internet and connections between sites. The STO provides bank card payment services management services on behalf of the agencies. For those agencies employing card acceptance processes connected to their networks, then some or all of their agency networks are in scope for the PCI DSS audit. The various payment processes for the agencies include:

- E-commerce card not present for payments
- E-commerce vendor hosted (outsourced) websites
- Over the phone at call centers
- Card present Point of Sale at agencies' offices
- Payment operational processes, call center processes, front counter processes

Technologies include:

- E-commerce web applications
- Firewalls, routers, switches
- Workstations (Call centers, counter agents, IT administrators, kiosks)
- DMZ's
- Point of Sales devices – connected via phone lines, cellular or networks
- Payment processors - various
- Payment application systems

Does your business use network segmentation to affect the scope of your PCI DSS environment?

*(Refer to "Network Segmentation" section of PCI DSS for guidance on network segmentation)*

Yes  No

## Part 2f. Third-Party Service Providers

Does your company use a Qualified Integrator & Reseller (QIR)?  Yes  No

**If Yes:**

Name of QIR Company:

QIR Individual Name:

Description of services provided by QIR:

Does your company share cardholder data with any third-party service providers (for example, Qualified Integrator & Resellers (QIR), gateways, payment processors, payment service providers (PSP), web-hosting companies, airline booking agents, loyalty program agents, etc.)?

Yes  No

**If Yes:**

Name of service provider:	Description of services provided:
Authorized.net	Card Processor
Big Commerce	Payment acceptance, processing for Tourism Department
Conway Greene	outsourced web site and transactions processing
CyberSource	Card processor
EventBrite	outsourced web site and transactions processing
Five9	Call Center outsourcer and application for TRD MVD, call recordings and transmissions
eTix	Online ticketing provider, used by museums
GCR, Inc.	payment application developer, for SOS
Gemalto (previously 3M Cogent)	Vendor- online vendor for DPS fingerprinting fees
GovDeals (Liquidity Solutions, Inc.)	outsourced vendor for GSD online auctions
Grant Street / Payment Express	Card Processor for Tax and MVD
Municipal Services Bureau (MSB)	Collection Agency for AOC
NM Interactive (NMI)	web hosting, MVD temporary tag registration and payment
NCSBN ORBS	Online application and processor for BON, for nursing registrations
Palm Coast	Payment acceptance, processing for Tourism Department
Paymentech (Chase)	card processor for Tyler Technologies, for AOC
PayPal	Card processor
Promiles	third-party Port of Entry fees collection
Reserve America	Card Processor
Saffire, LLC	outsourced web site vendor for EXPO
ShowWorks	Ticket sales for EXPO
Tyler Technologies	web hosting for payment processes

University of New Mexico	outsourced ticket sales – EXPO; also facilitates online teacher licensing for PED via another third party.
Vendini	outsourced agent, ticket sales, web site
VisionLink	Outsourced vendor for PED teacher registrations
VitalChek / LexisNexis	Card Processor
Wells Fargo	Card Processor
Wufoo/Survey Monkey	Outsourced vendor for Tourism Department sales

**Note:** Requirement 12.8 applies to all entities in this list.



## Section 2: Report on Compliance

This Attestation of Compliance reflects the results of an onsite assessment, which is documented in an accompanying Report on Compliance (ROC).

The assessment documented in this attestation and in the ROC was completed on:	2-7-2019
Have compensating controls been used to meet any requirement in the ROC?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
Were any requirements in the ROC identified as being not applicable (N/A)?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
Were any requirements not tested?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
Were any requirements in the ROC unable to be met due to a legal constraint?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No

## Section 3: Validation and Attestation Details

### Part 3. PCI DSS Validation

This AOC is based on results noted in the ROC dated 2-7-2019.

Based on the results documented in the ROC noted above, the signatories identified in Parts 3b-3d, as applicable, assert(s) the following compliance status for the entity identified in Part 2 of this document (**check one**):

<input checked="" type="checkbox"/>	<p><b>Compliant:</b> All sections of the PCI DSS ROC are complete, all questions answered affirmatively, resulting in an overall <b>COMPLIANT</b> rating; thereby <i>State of New Mexico</i> has demonstrated full compliance with the PCI DSS.</p>						
<input type="checkbox"/>	<p><b>Non-Compliant:</b> Not all sections of the PCI DSS ROC are complete, or not all questions are answered affirmatively, resulting in an overall <b>NON-COMPLIANT</b> rating, thereby (<i>Merchant Company Name</i>) has not demonstrated full compliance with the PCI DSS.</p> <p><b>Target Date</b> for Compliance:</p> <p>An entity submitting this form with a status of Non-Compliant may be required to complete the Action Plan in Part 4 of this document. <i>Check with your acquirer or the payment brand(s) before completing Part 4.</i></p>						
<input type="checkbox"/>	<p><b>Compliant but with Legal exception:</b> One or more requirements are marked "Not in Place" due to a legal restriction that prevents the requirement from being met. This option requires additional review from acquirer or payment brand.</p> <p><i>If checked, complete the following:</i></p> <table border="1" style="width: 100%;"> <thead> <tr> <th style="width: 35%;">Affected Requirement</th> <th style="width: 65%;">Details of how legal constraint prevents requirement being met</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> </tr> </tbody> </table>	Affected Requirement	Details of how legal constraint prevents requirement being met				
Affected Requirement	Details of how legal constraint prevents requirement being met						

### Part 3a. Acknowledgement of Status

Signatory(s) confirms:

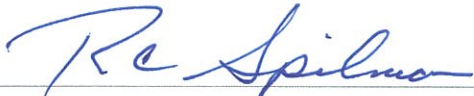
(Check all that apply)

<input checked="" type="checkbox"/>	The ROC was completed according to the <i>PCI DSS Requirements and Security Assessment Procedures, Version 3.2.1</i> , and was completed according to the instructions therein.
<input checked="" type="checkbox"/>	All information within the above-referenced ROC and in this attestation fairly represents the results of my assessment in all material respects.
<input checked="" type="checkbox"/>	I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization.
<input checked="" type="checkbox"/>	I have read the PCI DSS and I recognize that I must maintain PCI DSS compliance, as applicable to my environment, at all times.
<input checked="" type="checkbox"/>	If my environment changes, I recognize I must reassess my environment and implement any additional PCI DSS requirements that apply.

**Part 3a. Acknowledgement of Status (continued)**

- No evidence of full track data<sup>1</sup>, CAV2, CVC2, CID, or CVV2 data<sup>2</sup>, or PIN data<sup>3</sup> storage after transaction authorization was found on ANY system reviewed during this assessment.
- ASV scans are being completed by the PCI SSC Approved Scanning Vendor *RiskSense, Inc. and Cyber Security Works*


**Part 3b. Merchant Attestation**



Signature of Merchant Executive Officer ↑	Date: February 7, 2019
Merchant Executive Officer Name: Ronald C Spilman	Title: State Controller

**Part 3c. Qualified Security Assessor (QSA) Acknowledgement (if applicable)**

If a QSA was involved or assisted with this assessment, describe the role performed:	QSA performed an independent assessment of the various NM State agencies that accept payments via credit cards. Assessment was done against PCI DSS v3.2.1 to determine compliance status.
--	--



Signature of Duly Authorized Officer of QSA Company ↑	Date: 2-7-2019
Duly Authorized Officer Name: Mark Fidel	QSA Company: RiskSense, Inc.

**Part 3d. Internal Security Assessor (ISA) Involvement (if applicable)**

If an ISA(s) was involved or assisted with this assessment, identify the ISA personnel and describe the role performed:	NA
---	----

<sup>1</sup> Data encoded in the magnetic stripe or equivalent data on a chip used for authorization during a card-present transaction. Entities may not retain full track data after transaction authorization. The only elements of track data that may be retained are primary account number (PAN), expiration date, and cardholder name.

<sup>2</sup> The three- or four-digit value printed by the signature panel or on the face of a payment card used to verify card-not-present transactions.

<sup>3</sup> Personal identification number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.



### Part 4. Action Plan for Non-Compliant Requirements

Select the appropriate response for “Compliant to PCI DSS Requirements” for each requirement. If you answer “No” to any of the requirements, you may be required to provide the date your Company expects to be compliant with the requirement and a brief description of the actions being taken to meet the requirement. Check with your acquirer or the payment brand(s) before completing Part 4.

PCI DSS Requirement	Description of Requirement	Compliant to PCI DSS Requirements (Select One)		Remediation Date and Actions (If “NO” selected for any Requirement)
		YES	NO	
1	Install and maintain a firewall configuration to protect cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
2	Do not use vendor-supplied defaults for system passwords and other security parameters	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
3	Protect stored cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
4	Encrypt transmission of cardholder data across open, public networks	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
5	Protect all systems against malware and regularly update anti-virus software or programs	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
6	Develop and maintain secure systems and applications	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
7	Restrict access to cardholder data by business need to know	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
8	Identify and authenticate access to system components	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
9	Restrict physical access to cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
10	Track and monitor all access to network resources and cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
11	Regularly test security systems and processes	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12	Maintain a policy that addresses information security for all personnel	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

