COALFIRE

NCR CONNECTED PAYMENTS NON-LISTED ENCRYPTION SOLUTION ASSESSMENT

JUNE 2018

Prepared For:

NCR Corporation
https://www.ncr.com/retail/department-specialty-retail/payment/connected-payments

North America I Europe

877.224.8077 | info@coalfire.com | coalfire.com

Non-Listed Encryption Solution Assessment (NESA) Summary Documentation Template

Note: *This NESA summary documentation template is intended for use by the Non-Listed Encryption Solution Provider's P2PE Assessor in documenting assessments as per the PCI SSC's Assessment Guidance for Non-Listed Encryption Solutions.*

At the conclusion of the assessment, the P2PE Assessor should complete the P-ROV and NESA summary documentation template (with signature) and provide it to the solution provider of the non-listed encryption solution. The solution provider of the non-listed encryption solution should provide the most current NESA documentation to merchants or their assessors.

1.1 Description of the non-listed encryption solution

P2PE Assessor Company Name	Coalfire Systems, Inc
Company Name for the non-listed encryption solution provider	NCR Corporation
Description of the non-listed encryption solution provider (e.g., payment gateway, acquirer, multi-acquirer payment processor, etc.)	Payment gateway
Non-listed encryption solution Name and Version Number, as applicable	Connected Payments
Brief Description of product	Connected Payments offers a secure payment route and ensures complete data and transmission protection, from PIN pad to payment processor.
Document Name and versioning for the instruction manual	• NCR Connected Payments: NESA Solution Implementation Manual • Connected Payments OpenEPS Implementation Guide (PA-DSS) • Connected Payments User Guide
Additional comments, if needed:	Coalfire is a QSA(P2PE) company that was engaged by NCR to review the Connected Payments encryption solution, device configurations, gateway decryption environment, and key management practices for compliance against

	the P2PE 2.0 release 1.1 standards. Many aspects of the NCR solution are outside the control of NCR, including the device configurations and whitelists, however the critical aspects of key management and decryption security were found to be compliant against this rigorous standard. This Non-listed Encryption Solution Assessment (NESA) summary documentation is provided to help guide merchants and their assessors (QSA, ISA, and those conducting self-assessments) as to the recommended full or partial reduction of PCI DSS 3.2 controls that should be considered for environments that make use of the NCR Connected Payments encryption solution and platform. Merchant entities making use of this document should always ensure full confirmation of implementation according to the above referenced instruction manuals, and that any channels that store, process, or transmit cardholder data apart from the NCR Connected Payments solution (e.g., e-commerce) are segmented from and assessed independently of the guidance provided within this document. The information contained in this document is provided in alignment with the PCI SSC guidance on Non-listed Encryption Solution Assessments (NESA), published November 2016, using the PCI SSC NESA Summary Documentation template published February 2017 (modified slightly to improve clarity of control recommendations). Assessors are encouraged to leverage the control scope reduction recommendations and justification found in table 1.5 to simplify the merchant assessment process for merchants how have properly implemented NCR Connected Payments in their card present and MOTO environment(s).

1.2 Scoping Criteria/Implementation Tested

List of PCI-approved POI(s) assessed, including: • PTS Approval Number • Make/Model • Hardware # • Firmware # • All Applications on POI (Application Name and Version)	4-10177, Equinox Payments, L5300, Hardware: L501xx (SRED), L300xx (SRED), L502xx (SRED), 1200xx, L500xx, 1300xx, 1301xx, 1302xx, 1400xx, 1401xx, (Non-SRED), 1402xx, L301xx, L401xx, L503xx, L504xx, L302xx, L402xx, L505xx, L303xx, L506xx, L304xx, Firmware: L5x-OS-v07.05-20170831-2 **Not eligible for new deployments**

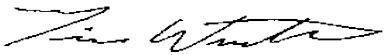
	4-60119, Equinox Payments, L5200/L5300, Hardware: L501xx(SRED), L300xx(SRED), L502xx(SRED), L301xx, L503xx, L504xx, L302xx, L402xx, (Non-SRED), L505xx, L303xx, L506xx, L304xx Firmware: L5x-OS-v07.xx-xxxxxxxx-3 4-10177, Verifone, Mx925/Mx915, Hardware: P177-40x-xx-xxx (Mx915), P177-50x-xx-xxx (Mx925), P177-409-xx-xxx (Mx915 ECR) Firmware: Vault: 11.x.x; 12.x.x, 13.x.x, AppM: 5.x.x; 5A.x.x; 6.x.x; 7.x.x, SRED: 4.x.x; 5.x.x, OP: 5.x.x; 6.x.x; 7.x.x, Vault: 14.x.x; AppM: 8.x.x; SRED: 7.x.x, Vault: 16.x.x; AppM: 10.x.x Applications: FormAgent/XPI 5200, FormAgent/XPI 5300 (P2PE) 4-10110, Verifone, Mx925/Mx915, Hardware: P132-509-01-R (MX 925), P132-509-11-R (MX 925), P132-509-21-R (MX 925), P132-509-11-PF (MX 925), P132-409-01-R (MX 915), P132-509-02-R (MX 925), P132-509-12-R (MX 925), P132-509-22-R (MX 925), P132-509-12-PF (MX 925), P132-409-02-R (MX 915) Firmware: Vault: 1.x.x, 3.x.x, 4.x.x, 11.x.x, 12.x.x, AppM: 1.x.x; 3.x.x; 4.x.x; 5.x.x, 5A.x.x, 6.x.x, SRED: 1.x.x, 3.x.x; 4.x.x; 5.x.x, OP: 1.x.x, 3.x.x; 4.x.x; 7.x.x, SRED 5.x.x.xxx, Vault: 13.x.x, AppM: 7.x.x, Vault: 14.x.x; AppM: 8.x.x; SRED: 7.x.x, Vault: 16.x.x; AppM: 10.x.x Applications: FormAgent/XPI 5200, FormAgent/XPI 5300 (P2PE) 4-30168, Verifone, e355, Hardware: M087-351-x1-xxx, M087-361-x0-xxx, M087-381-x0-xxx, M087-381-xx-xxx Firmware: QTE50301.xxxxxxxx, QTE50320.xxxxxxxx, QTE50330.xxxxxxxx, QTE50340.xxxxxxxx, Applications: CXPI 12.08.x, XPI 12.11.x (P2PE 2017-00154.036) 4-40054, Verifone, Vx820, Hardware: M282-XXX-XX-XXX-3, Firmware: Non-SRED: QT820245, QT820246.xxxxxxxx, Applications: CXPI 12.08.x, XPI 12.11.x (P2PE 2017-00154.036) 4-10106, Verifone, Vx805, Hardware: M280-70x-xx-xxx-3, Firmware: QT850017, SRED: QT850104, QT850109, QT850110, QT850120, QT850121, QT850240, QT850340, QT850245,

	QT850240.xxxxxxxx, QTyy0400.xxxxxxxx, QTyy0500.xxxxxxxx, Applications: XPI 12.11.x (P2PE 2017-00154.036) 4-30128, Verifone, VX690, Hardware: M260-x1x-xx-xxx-3, M260-x5x-xx-xxx-3, M260-x1x-xx-xxx-3B, M260-x5x-xx-xxx-3B, M260-x1x-xx-xxx-3C, M260-x5x-xx-xxx-3C, M260-x1x-xx-xxx-3D, M260-x5x-xx-xxx-3D, Firmware: QT690263, QT690264.xxxxxxxx, Applications: CXPI 12.09.x, XPI 12.11.x (P2PE 2017-00154.036) 4-30259, Verifone, VX690, Hardware: M260-xxB-Cx-xxx-3B (first B= 3;5;6;7;8 (keypad type)) Firmware: QT690500, Applications: CXPI 12.09.x 4-30053, Verifone, Vx680, Vx680-E1, Vx680 ECR, Hardware: M268-70x-xx-xxn-3, M268-73x-xx-xxn-3, M268-74x-xx-xxn-3, M268-76x-xx-xxn-3, M268-77x-xx-xxn-3, M268-78x-xx-xxn-3, M268-79x-xx-xxn-3, M268-77x-xx-xxx-3B, M268-72x-xx-xxx-3, M268-72x-xx-xxx-3B, Firmware: Non SRED: QT68x01D, QT680006, QT680010, QT680011, QT680012, QT680013, QT680014, QT680015, QT6B0015, QT6B0016, QT6B0017, QT6B0018, QT6B0019, QT6B0101, QT6B0102, QT6B0103, QT6B0104, SRED: QT680101, QT680102, QT680103, QT680104, QT680105, QT680106, QT680107, QT680108, QT680109, QT6G0109, QT680110, QT6G0110, QT6B0110, QT680111, QT6G0111, QT6B0111, QT680122, QT6G0122, QT6G0113, QT6G0114, QT6G0115, QT680120, QT6B0120, QT6G0240, QT680240, QT6B0240, QT680340, QT6G0340, QT6B0340, QT680301, QT6B0301, QT6B0121, QT6B0122, QT680243, QT6B0243, QT680241, QT680245, QT6B0245, QT6G0245, QT680240.xxxxxxxx, QT6B0240.xxxxxxxx, QT6G0240.xxxxxxxx, QTyy0400.xxxxxxxx, QTyy0500.xxxxxxxx, QTyy520.xxxxxxxx, QTyy0530.xxxxxxxx, Applications: XPI 12.11.x (P2PE 2017-00154.036) 4-10079, Verifone, Mx870, Hardware: M094-10X-XX-R, M094-10X-XX-RC, Firmware: MX0006US, MX0007US, SRED (CTLS): MX0008US, Applications: FormAgent 2.6.6 or greater, XPI 4200, **Not eligible for new deployments**

	4-10080, Verifone, Mx850/Mx860, Hardware: M094-207-xx-R (Mx850 Online Only), M094-209-xx-R (Mx850 Online/Offline), M094-407-01-R (Mx860 Online Only), M094-409-01-R (Mx860 Online/Offline), M094-207-xx-RC (Mx850 Online Only), M094-209-xx-RC (Mx850 Online/Offline), M094-407-01-RC (Mx860 Online Only), M094-409-01-RC (Mx860 Online/Offline), Firmware: MX0006US, MX0007US, SRED (CTLS): MX0008US, Applications: FormAgent 2.6.6 or greater, XPI 4200, **Not eligible for new deployments** 4-10081, Verifone, Mx880, Hardware: M094-507-xx-R (Online only), M094-509-xx-R, M094-507-xx-RC (Online only), M094-509-xx-RC, Firmware: MX0006US, MX0007US, SRED (CTLS): MX0008US, Applications: FormAgent 2.6.6 or greater, XPI 4200, **Not eligible for new deployments** 4-30062, Ingenico, iSC250, Hardware: iSC2xx-01Txxxxx, Firmware: 820518 V01.xx, 820518 V02.xx, SRED (Non CTLS): 820157 V01.xx, Applications: RBA 17.2.x, RBA 21.0.2 4-30132, Ingenico, iSC Touch 250, Hardware: iSC2xx-21Txxxxx, iSC2xx-31Txxxxx, Firmware: 820518 V12.xx, SRED (CTLS): 820528V02.xx, Applications: RBA 17.2.x, RBA 21.0.2 4-30135 Ingenico, iSC Touch 250, Hardware: iSC2xx-21Txxxxx, iSC2xx-31Txxxxx, Firmware: 820365 V02.xx, 820518 V02.xx, 820528V02.xx, Applications: RBA 17.2.x, RBA 21.0.2 4-30098, Ingenico, iSC Touch 480, Hardware: ISC4xx-01Txxxxx (no CTLS), ISC4xx-11Txxxxx (CTLS), Firmware: 820365 V02.xx, 820518V01.xx, 820518V02.xx, SRED (CTLS): 820528V02.xx, Applications: RBA 17.2.x, RBA 21.0.2 4-30098, Ingenico, iSC Touch 480, Hardware: ISC4xx-01Txxxxx, ISC4xx-11Txxxxx, Firmware: 820518 V11.xx, 820518 V12.xx, 820528V02.xx, Applications: RBA 17.2.x, RBA 21.0.2

Description of the non-listed encryption solution implementation(s) tested, including hardware and software dependencies:	A sample of 1 each of the listed POI were tested with the latest hardware, firmware, and application versions in the solution provider's lab.
Additional comments, if needed:	Connected Payments decryption environment accepts only transactions that are encrypted using Connected Payments encryption keys. Any non-encrypted transactions are rejected and an alert is generated in the decryption environment.

1.3 QSA (P2PE) Acknowledgment

Name of the P2PE Assessor who attests that: • The "Scoping Criteria" defined in the Assessment Guidance for Non-listed Encryption Solutions has been met; • Compliance to P2PE Domains 5 and 6 have been fully validated; and • Compliance to P2PE Domains 1, 2, and 3 have been validated as documented in section 1.4, *P-ROV Findings by Domain*, below.	Tim Winston
	June 4, 2018
Signature of QSA (P2PE) Duly Authorized Officer	Date
Tim Winston	Principal
QSA (P2PE) Name	Title
Coalfire Systems, Inc	
QSA (P2PE) Company	

1.4 P-ROV Findings by Domain

		Findings (check one)	
		Full Compliance	**Non-Compliant**
Domain 1: Encryption Device and Application Management			
1A	**Account data must be encrypted in equipment that is resistant to physical and logical compromise.**		
1A-1	*PCI-approved POI devices with SRED are used for transaction acceptance.*	☐	☒
1A-2	*Applications on POI devices with access to clear-text account data are assessed per Domain 2 before being deployed into a P2PE solution.*	☐	☒
1B	**Logically secure POI devices.**		
1B-1	*Solution provider ensures that logical access to POI devices deployed at merchant encryption environment(s) is restricted to authorized personnel.*	☒	☐
1B-2	*Solution provider secures any remote access to POI devices deployed at merchant encryption environments.*	☒	☐
1B-3	*The solution provider implements procedures to protect POI devices and applications from known vulnerabilities and securely update devices.*	☒	☐
1B-4	*Solution provider implements procedures to secure account data when troubleshooting*	☒	☐
1B-5	*The P2PE solution provides auditable logs of any changes to critical functions of the POI device(s).*	☐	☒
1C	**Use P2PE applications that protect PAN and SAD.**		
1C-1	*Applications are implemented securely, including when using shared resources and when updating applications and application functionality.*	☐	☒
1C-2	*All applications/software without a business need do not have access to account data.*	☒	☐
1D	**Implement secure application-management processes.**		
1D-1	*Integrity of applications is maintained during installation and updates.*	☒	☐
1D-2	*Maintain instructional documentation and training programs for the application's installation, maintenance/upgrades, and use.*	☒	☐
1E	**Component providers *ONLY*: report status to solution providers**		
1E-1	*For component providers of encryption-management services, maintain and monitor critical P2PE controls and provide reporting to the responsible solution provider.*	N/A	N/A
Domain 2: Application Security			

		Findings (check one)	
		Full Compliance	**Non-Compliant**
Assessor Note: POI vendors manage the applications loaded onto POI devices used in the NCR Connected Payments encryption solution. Where these applications have been validated by a PA-QSA(P2PE) and listed on the PCI Point to Point Encryption Applications website at https://www.pcisecuritystandards.org/assessors_and_solutions/point_to_point_encryption_applications, this controls in this domain may be deemed Fully Compliant to P2PE. Where any loaded application with access to cardholder data is not listed, this domain should be considered Non-Compliant.			
2A	**Protect PAN and SAD**		
2A-1	*The application executes on a PCI-approved POI device with SRED enabled and active.*	Not tested.	Not tested.
2A-2	*The application does not store PAN and/or SAD for any longer than business processes require.*	Not tested.	Not tested.
2A-3	*The application does not transmit clear-text PAN and/or SAD outside of the POI device, and only uses communication methods included in the scope of the PCI-approved POI device evaluation.*	Not tested.	Not tested.
2B	**Develop and maintain secure applications.**		
2B-1	*The application is developed and tested according to industry-standard software development life cycle practices that incorporate information security.*	Not tested.	Not tested.
2B-2	*The application is implemented securely, including the secure use of any resources shared between different applications.*	Not tested.	Not tested.
2B-3	*The application vendor uses secure protocols, provides guidance on their use, and performs integration testing on the final application.*	Not tested.	Not tested.
2B-4	*Applications do not implement any encryption functions in lieu of SRED encryption. All such functions are performed by the approved SRED firmware of the POI device.*	Not tested.	Not tested.
2C	**Implement secure application-management processes.**		
2C-1	*New vulnerabilities are discovered and applications are tested for those vulnerabilities on an ongoing basis.*	Not tested.	Not tested.
2C-2	*Applications are installed and updates are implemented only via trusted and cryptographically authenticated processes using an approved security mechanism evaluated for the PCI-approved POI device.*	Not tested.	Not tested.
2C-3	*Maintain instructional documentation and training programs for the application's installation, maintenance/upgrades, and use.*	Not tested.	Not tested.
Domain 3: P2PE Solution Management			
3A	**P2PE solution management**		
3A-1	*The solution provider maintains documentation detailing the P2PE solution architecture and data flows.*	☒	☐
3A-2	*The solution provider manages and monitors status reporting from P2PE component providers.*	☒	☐
3A-3	*Solution provider implements processes to respond to notifications from merchants, component providers and/or third parties, and provide notifications about any suspicious activity involving the P2PE solution.*	☐	☒

	Findings (check one)	
	Full Compliance	**Non-Compliant**
3A-4 *If the solution provider allows a merchant to stop P2PE encryption of account data, the solution provider manages the related process for merchants*	☒	☐
3B Third-party management		
3B-1 *The solution provider facilitates and maintains formal agreements with all third parties contracted to perform P2PE functions on behalf of the solution provider.*	☒	☐
3B-2 *Solution provider secures any remote access to POI devices deployed at merchant encryption environments.*	☒	☐
3B-3 *The solution provider implements procedures to protect POI devices and applications from known vulnerabilities and securely update devices.*	☒	☐
3B-4 *Solution provider implements procedures to secure account data when troubleshooting*	☒	☐
3B-5 *The P2PE solution provides auditable logs of any changes to critical functions of the POI device(s).*	☐	☒
3C Creation and maintenance of *P2PE Instruction Manual* for merchants		
3C-1 *Solution provider develops, maintains, and disseminates a* P2PE Instruction Manual *to merchants.*	☐	☒
Domain 5: Decryption Environment		
Note – *the solution must be fully compliant with Domain 5 to align with the Assessment Guidance for Non-listed Encryption Solutions.*	☒	☐
Domain 6: P2PE Cryptographic Key Operations and Device Management		
Note – *the solution must be fully compliant with Domain 6 to align with the Assessment Guidance for Non-listed Encryption Solutions.*	☒	☐

1.5 P2PE Assessor's recommendation(s) for possible PCI DSS control reductions

The P2PE Assessor's recommendations for PCI DSS control reductions are based on the following minimum criteria being met:

- The merchant/merchant's QSA must validate that the non-validated encryption solution was implemented in accordance with the instruction manual provided by the solution provider and in a PCI DSS compliant manner;
- The merchant/merchant's QSA must validate that there are no additional payment acceptance channels or the presence of any clear-text cardholder data within the merchant environment;

Note*: To understand how the use of PCI-listed P2PE Solutions versus the use of Non-listed Encryption Solutions affect a merchant's PCI DSS compliance validation efforts, please contact the merchant's acquirer and/or payment brands.*

Note: *The merchant's QSA should not solely rely on the NESA documentation to determine the appropriate scoping of the merchant's environment. The QSA should confirm the "Scoping Criteria" in the Assessment Guidance for Non-listed Encryption Solutions document is being met, as well as validate the scope is accurate and appropriate per the PCI DSS. Any reduction in scope should be recorded in the appropriate section in the ROC Reporting Template for use with PCI DSS.*	
• Other criteria, if applicable	Merchants may work directly with POI vendors to create POI system builds. Merchants that do this need to ensure: 1. Supported hardware, firmware, and application versions are used. 2. Whitelists, or BIN exclusion lists, can never exclude valid card brand BIN ranges and whitelist files are signed by the POI vendor before loading on POI. Merchants develop their own processes for deployment and on-going physical maintenance of POI. These procedures must ensure the integrity of POI before and during deployment and during servicing, return, and decommissioning. Merchants contract with key injection facilities (KIF). NCR does not have agreements directly with the KIF used by merchants. Merchants are responsible for managing KIFs as service providers. Merchants are advised to use KIF that are listed as PCI P2PE KIF Component Providers (https://www.pcisecuritystandards.org/assessors_and_solutions/point_to_point_encryption_components) for the highest assurance that POI are securely handled before deployment and during repair. NCR does not develop POI payment applications. NCR Connected Payments specifies POI vendor supplied applications for terminals that require payment applications to be installed, such as Ingenico and Verifone. Merchants are advised to use application versions that are on the P2PE Application list (https://www.pcisecuritystandards.org/assessors_and_solutions/point_to_point_encryption_applications) and specify the SRED capabilities are enabled on terminals for the greatest assurance for encryption of sensitive data. NCR OpenEPS point-of-sale (POS) workstation client, which is used to provide network access to serial or USB connected POI, was tested and found not to have any access to unencrypted account data or any ability to change or circumvent security configuration of POI devices. Merchants can be assured that installation of NCR OpenEPS on POS workstation does not impact control applicability for these systems.

PCI DSS Requirements v3.2 ***Requirement 1: Install and maintain a firewall configuration to protect cardholder data***	**Control Reduction Recommended?** Y	N	**If yes, provide brief justification for control reduction**
1.1 Establish and implement firewall and router configuration standards that include the following:	☒	☐	Merchant firewalls and routers cannot impact the security of PAN/SAD data which is encrypted within the POI.

1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations	☒	☐	Merchant firewalls and routers cannot impact the security of PAN/SAD data which is encrypted within the POI.
1.1.2 Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks	☐	☒	
1.1.3 Current diagram that shows all cardholder data flows across systems and networks	☐	☒	
1.1.4 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone	☒	☐	Merchant firewalls and routers cannot impact the security of PAN/SAD data which is encrypted within the POI.
1.1.5 Description of groups, roles, and responsibilities for management of network components	☒	☐	Merchant firewalls and routers cannot impact the security of PAN/SAD data which is encrypted within the POI.
1.1.6 Documentation of business justification and approval for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure.	☒	☐	Merchant firewalls and routers cannot impact the security of PAN/SAD data which is encrypted within the POI.
1.1.7 Requirement to review firewall and router rule sets at least every six months	☒	☐	Merchant firewalls and routers cannot impact the security of PAN/SAD data which is encrypted within the POI.
1.2 Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment. ***Note:*** *An "untrusted network" is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage.*	☒	☐	Merchant firewalls and routers cannot impact the security of PAN/SAD data which is encrypted within the POI.
1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.	☒	☐	Merchant firewalls and routers cannot impact the security of PAN/SAD data which is encrypted within the POI.
1.2.2 Secure and synchronize router configuration files.	☒	☐	Merchant firewalls and routers cannot impact the security of PAN/SAD data which is encrypted within the POI.
1.2.3 Install perimeter firewalls between all wireless networks and the cardholder data environment, and configure these firewalls to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment.	☒	☐	Merchant firewalls and routers cannot impact the security of PAN/SAD data which is encrypted within the POI.
1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.	☒	☐	Merchant firewalls and routers cannot impact the security of PAN/SAD data which is encrypted within the POI.
1.3.1 Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.	☒	☐	Merchant firewalls and routers cannot impact the security of PAN/SAD data which is encrypted within the POI.
1.3.2 Limit inbound Internet traffic to IP addresses within the DMZ.	☒	☐	Merchant firewalls and routers cannot impact the security of PAN/SAD data which is encrypted within the POI.
1.3.3 Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network. (For example, block traffic originating from the Internet with an internal source address.)	☒	☐	Merchant firewalls and routers cannot impact the security of PAN/SAD data which is encrypted within the POI.

1.3.4 Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.	☒	☐	Merchant firewalls and routers cannot impact the security of PAN/SAD data which is encrypted within the POI.
1.3.5 Permit only "established" connections into the network.	☐	☒	Coalfire still recommends against direct unrestricted inbound Internet access to the POIs.
1.3.6 Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.	☒	☐	Merchant firewalls and routers cannot impact the security of PAN/SAD data which is encrypted within the POI.
1.3.7 Do not disclose private IP addresses and routing information to unauthorized parties. ***Note:*** *Methods to obscure IP addressing may include, but are not limited to:* • *Network Address Translation (NAT)* • *Placing servers containing cardholder data behind proxy servers/firewalls,* • *Removal or filtering of route advertisements for private networks that employ registered addressing,* • *Internal use of RFC1918 address space instead of registered addresses.*	☒	☐	Merchant firewalls and routers cannot impact the security of PAN/SAD data which is encrypted within the POI.
1.4 Install personal firewall software or equivalent functionality on any portable computing devices (including company and/or employee-owned) that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the CDE. Firewall (or equivalent) configurations include: • Specific configuration settings are defined. • Personal firewall (or equivalent functionality) is actively running. • Personal firewall (or equivalent functionality) is not alterable by users of the portable computing devices.	☒	☐	Merchant firewalls and routers cannot impact the security of PAN/SAD data which is encrypted within the POI.
1.5 Ensure that security policies and operational procedures for managing firewalls are documented, in use, and known to all affected parties.	☐	☒	Even with the significant reduction of applicable controls warranted by the solution obtains
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters	**Control Reduction Recommended?**		**If yes, provide brief justification for control reduction,**
	Y	**N**	
2.1 Always change vendor-supplied defaults and remove or disable unnecessary default accounts **before** installing a system on the network. This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, payment applications, Simple Network Management Protocol (SNMP) community strings, etc.).	☐	☒	Merchants must ensure the POI devices are implemented as per POI device vendor security guidance and the solution implication guide. Review of non-POI system components configurations would not be applicable. Control is not applicable for other devices.
2.1.1 For wireless environments connected to the cardholder data environment or transmitting cardholder data, change ALL wireless vendor defaults at installation, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.	☒	☐	Merchant wireless networks cannot impact the security of PAN/SAD data which is encrypted within the POI.

2.2 Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. *Sources of industry-accepted system hardening standards may include, but are not limited to:* • *Center for Internet Security (CIS)* • *International Organization for Standardization (ISO)* • *SysAdmin Audit Network Security (SANS) Institute* • *National Institute of Standards Technology (NIST).*	☐	☒	POI device vendor guidance and solution implementation guide documents provided by NCR will have to be implemented and properly configured with the merchant's retail environment for the POI devices in scope. PCI requirements testing the configuration standards for all other system components on the merchant's retail network would not be applicable.
2.2.1 Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.) ***Note:*** *Where virtualization technologies are in use, implement only one primary function per virtual system component.*	☒	☐	Merchant system configuration cannot impact the security of PAN/SAD data which is encrypted within the POI.
2.2.2 Enable only necessary services, protocols, daemons, etc., as required for the function of the system.	☒	☐	Merchant system configuration cannot impact the security of PAN/SAD data which is encrypted within the POI.
2.2.3 Implement additional security features for any required services, protocols, or daemons that are considered to be insecure. ***Note:*** *Where SSL/early TLS is used, the requirements in Appendix A2 must be completed.*	☒	☐	Merchant system configuration cannot impact the security of PAN/SAD data which is encrypted within the POI.
2.2.4 Configure system security parameters to prevent misuse.	☒	☐	Merchant system configuration cannot impact the security of PAN/SAD data which is encrypted within the POI.
2.2.5 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.	☒	☐	Merchant system configuration cannot impact the security of PAN/SAD data which is encrypted within the POI.
2.3 Encrypt all non-console administrative access using strong cryptography. ***Note:*** *Where SSL/early TLS is used, the requirements in Appendix A2 must be completed.*	☒	☐	Merchant system configuration cannot impact the security of PAN/SAD data which is encrypted within the POI.
2.4 Maintain an inventory of system components that are in scope for PCI DSS.	☐	☒	Maintaining POI device inventory will always apply to the merchant environment. Control is not applicable for other devices.
2.5 Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties.	☐	☒	Even with the significant reduction of applicable controls warranted by the solution obtains
2.6 Shared hosting providers must protect each entity's hosted environment and cardholder data. These providers must meet specific requirements as detailed in *Appendix A1: Additional PCI DSS Requirements for Shared Hosting Providers.*	☒	☐	Merchants are not shared hosting providers.
Requirement 3: Protect stored cardholder data	**Control Reduction Recommended?**		**If yes, provide brief justification for control reduction,**
	Y	**N**	

3.1 Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes that include at least the following for all cardholder data (CHD) storage: • Limiting data storage amount and retention time to that which is required for legal, regulatory, and/or business requirements • Specific retention requirements for cardholder data • Processes for secure deletion of data when no longer needed • A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention.	☐	☒	If the merchant has any paper-based processes associated with this payment channel, then this requirement will still apply to their environment. Otherwise, this requirement can be considered not applicable.
3.2 Do not store sensitive authentication data after authorization (even if encrypted). If sensitive authentication data is received, render all data unrecoverable upon completion of the authorization process. It is permissible for issuers and companies that support issuing services to store sensitive authentication data if: • There is a business justification and • The data is stored securely. Sensitive authentication data includes the data as cited in the following Requirements 3.2.1 through 3.2.3:	☒	☐	PCI DSS does not permit requirement 3.2 to be Not Applicable. Merchants cannot store SAD after authorization, even when encrypted.
3.2.1 Do not store the full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere) after authorization. This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data. ***Note:*** *In the normal course of business, the following data elements from the magnetic stripe may need to be retained:* • *The cardholder's name* • *Primary account number (PAN)* • *Expiration date* • *Service code* *To minimize risk, store only these data elements as needed for business.*	☐	☒	PCI DSS does not permit requirement 3.2 to be Not Applicable. Merchants cannot store SAD after authorization, even when encrypted.
3.2.2 Do not store the card verification code or value (three-digit or four-digit number printed on the front or back of a payment card used to verify card-not-present transactions) after authorization.	☐	☒	PCI DSS does not permit requirement 3.2 to be Not Applicable. Merchants cannot store SAD after authorization, even when encrypted.
3.2.3 Do not store the personal identification number (PIN) or the encrypted PIN block after authorization.	☐	☒	PCI DSS does not permit requirement 3.2 to be Not Applicable. Merchants cannot store SAD after authorization, even when encrypted.
3.3 Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see more than the first six/last four digits of the PAN.***Note:*** *This requirement does not supersede stricter requirements in place for displays of cardholder data—for example, legal or payment card brand requirements for point-of-sale (POS) receipts.*	☐	☒	If the merchant has any paper-based processes associated with this payment channel, then this requirement will still apply to their environment. Otherwise, this requirement can be considered not applicable.

3.4 Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches: • One-way hashes based on strong cryptography, (hash must be of the entire PAN) • Truncation (hashing cannot be used to replace the truncated segment of PAN) • Index tokens and pads (pads must be securely stored) • Strong cryptography with associated key-management processes and procedures. ***Note:*** *It is a relatively trivial effort for a malicious individual to reconstruct original PAN data if they have access to both the truncated and hashed version of a PAN. Where hashed and truncated versions of the same PAN are present in an entity's environment, additional controls must be in place to ensure that the hashed and truncated versions cannot be correlated to reconstruct the original PAN.*	☐	☒	If the merchant has any paper-based processes associated with this payment channel, then this requirement will still apply to their environment. Otherwise, this requirement can be considered not applicable.
3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts. ***Note:*** *This requirement applies in addition to all other PCI DSS encryption and key-management requirements.*	☒	☐	If the merchant has any paper-based processes associated with this payment channel, then this requirement will still apply to their environment. Otherwise, this requirement can be considered not applicable.
3.5 Document and implement procedures to protect keys used to secure stored cardholder data against disclosure and misuse: ***Note:*** *This requirement applies to keys used to encrypt stored cardholder data, and also applies to key-encrypting keys used to protect data-encrypting keys—such key-encrypting keys must be at least as strong as the data-encrypting key.*	☒	☐	If the merchant has any paper-based processes associated with this payment channel, then this requirement will still apply to their environment. Otherwise, this requirement can be considered not applicable.
3.5.1 ***Additional requirement for service providers only:*** Maintain a documented description of the cryptographic architecture that includes: • Details of all algorithms, protocols, and keys used for the protection of cardholder data, including key strength and expiry date • Description of the key usage for each key. • Inventory of any HSMs and other SCDs used for key management ***Note:*** *This requirement is a best practice until January 31, 2018, after which it becomes a requirement.*	☒	☐	Not applicable to merchants.
3.5.2 Restrict access to cryptographic keys to the fewest number of custodians necessary.	☒	☐	Merchants do not have access to PAN/SAD data for storage, because it is encrypted within the POI using strong cryptographic keys that are not available to the merchant.
3.5.3 Store secret and private keys used to encrypt/decrypt cardholder data in one (or more) of the following forms at all times: • Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key • Within a secure cryptographic device (such as a hardware (host) security module (HSM) or PTS-approved point-of-interaction device) • As at least two full-length key components or key shares, in accordance with an industry-accepted method ***Note:*** *It is not required that public keys be stored in one of these forms.*	☒	☐	Merchants do not have access to PAN/SAD data for storage, because it is encrypted within the POI using strong cryptographic keys that are not available to the merchant.
3.5.4 Store cryptographic keys in the fewest possible locations.	☒	☐	Merchants do not have access to PAN/SAD data for storage, because it is encrypted within the POI

			using strong cryptographic keys that are not available to the merchant.
3.6 Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data, including the following: ***Note:*** *Numerous industry standards for key management are available from various resources including NIST, which can be found at http://csrc.nist.gov.*	☒	☐	Merchants do not have access to PAN/SAD data for storage, because it is encrypted within the POI using strong cryptographic keys that are not available to the merchant.
3.6.1 Generation of strong cryptographic keys	☒	☐	Merchants do not have access to PAN/SAD data for storage, because it is encrypted within the POI using strong cryptographic keys that are not available to the merchant.
3.6.2 Secure cryptographic key distribution	☒	☐	Merchants do not have access to PAN/SAD data for storage, because it is encrypted within the POI using strong cryptographic keys that are not available to the merchant.
3.6.3 Secure cryptographic key storage	☒	☐	Merchants do not have access to PAN/SAD data for storage, because it is encrypted within the POI using strong cryptographic keys that are not available to the merchant.
3.6.4 Cryptographic key changes for keys that have reached the end of their cryptoperiod (for example, after a defined period of time has passed and/or after a certain amount of cipher-text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (for example, NIST Special Publication 800-57).	☒	☐	Merchants do not have access to PAN/SAD data for storage, because it is encrypted within the POI using strong cryptographic keys that are not available to the merchant.
3.6.5 Retirement or replacement (for example, archiving, destruction, and/or revocation) of keys as deemed necessary when the integrity of the key has been weakened (for example, departure of an employee with knowledge of a clear-text key component), or keys are suspected of being compromised. ***Note:*** *If retired or replaced cryptographic keys need to be retained, these keys must be securely archived (for example, by using a key-encryption key). Archived cryptographic keys should only be used for decryption/verification purposes.*	☒	☐	Merchants do not have access to PAN/SAD data for storage, because it is encrypted within the POI using strong cryptographic keys that are not available to the merchant.
3.6.6 If manual clear-text cryptographic key-management operations are used, these operations must be managed using split knowledge and dual control. ***Note:*** *Examples of manual key-management operations include, but are not limited to: key generation, transmission, loading, storage and destruction.*	☒	☐	Merchants do not have access to PAN/SAD data for storage, because it is encrypted within the POI using strong cryptographic keys that are not available to the merchant.
3.6.7 Prevention of unauthorized substitution of cryptographic keys.	☒	☐	Merchants do not have access to PAN/SAD data for storage, because it is encrypted within the POI using strong cryptographic keys that are not available to the merchant.
3.6.8 Requirement for cryptographic key custodians to formally acknowledge that they understand and accept their key-custodian responsibilities.	☒	☐	Merchants do not have access to PAN/SAD data for storage, because it is encrypted within the POI using strong cryptographic keys that are not available to the merchant.
3.7 Ensure that security policies and operational procedures for protecting stored cardholder data are documented, in use, and known to all affected parties.	☐	☒	Even with the significant reduction of applicable controls warranted by the solution, Even with the significant reduction of applicable controls the solution obtains, Coalfire recommends that

			merchants have appropriate policies and operational procedures.
Requirement 4: Encrypt transmission of cardholder data across open, public networks	**Control Reduction Recommended?**		**If yes, provide brief justification for control reduction,**
	Y	**N**	
4.1 Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following: • Only trusted keys and certificates are accepted. • The protocol in use only supports secure versions or configurations. • The encryption strength is appropriate for the encryption methodology in use. ***Note:*** *Where SSL/early TLS is used, the requirements in Appendix A2 must be completed.* *Examples of open, public networks include but are not limited to:* • *The Internet* • *Wireless technologies, including 802.11 and Bluetooth* • *Cellular technologies, for example, Global System for Mobile communications (GSM), Code division multiple access (CDMA)* • *General Packet Radio Service (GPRS).* • *Satellite communications.*	☒	☐	Use of additional encryption via secure transmission protocols does not impact the security of PAN/SAD data which is encrypted within the POI.
4.1.1 Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices to implement strong encryption for authentication and transmission.	☒	☐	Use of additional encryption via secure transmission protocols does not impact the security of PAN/SAD data which is encrypted within the POI.
4.2 Never send unprotected PANs by end-user messaging technologies (for example, e-mail, instant messaging, SMS, chat, etc.).	☐	☒	Merchants will not have any access to cardholder data within their environment; however, employees will still have access to the physical credit card in retail environments. As such, a policy prohibiting the emailing of unprotected PAN is still appropriate for most retail environments.
4.3 Ensure that security policies and operational procedures for encrypting transmissions of cardholder data are documented, in use, and known to all affected parties.	☐	☒	Even with the significant reduction of applicable controls warranted by the solution obtains
Requirement 5: Use and regularly update anti-virus software or programs	**Control Reduction Recommended?**		**If yes, provide brief justification for control reduction,**
	Y	**N**	
5.1 Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).	☒	☐	Use of anti-virus software does not impact the security of PAN/SAD data which is encrypted within the POI.
5.1.1 Ensure that anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.	☒	☐	
5.1.2 For systems considered to be not commonly affected by malicious software, perform periodic evaluations to identify and evaluate evolving malware threats in order to confirm whether such systems continue to not require anti-virus software.	☒	☐	Use of anti-virus software does not impact the security of PAN/SAD data which is encrypted within the POI.

5.2 Ensure that all anti-virus mechanisms are maintained as follows: • Are kept current, • Perform periodic scans • Generate audit logs which are retained per PCI DSS Requirement 10.7.	☒	☐	Use of anti-virus software does not impact the security of PAN/SAD data which is encrypted within the POI.
5.3 Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period. ***Note:*** *Anti-virus solutions may be temporarily disabled only if there is legitimate technical need, as authorized by management on a case-by-case basis. If anti-virus protection needs to be disabled for a specific purpose, it must be formally authorized. Additional security measures may also need to be implemented for the period of time during which anti-virus protection is not active.*	☒	☐	Use of anti-virus software does not impact the security of PAN/SAD data which is encrypted within the POI.
5.4 Ensure that security policies and operational procedures for protecting systems against malware are documented, in use, and known to all affected parties.	☐	☒	Even with the significant reduction of applicable controls warranted by the solution obtains, Coalfire recommends that merchants have appropriate policies and operational procedures.

Requirement 6: Develop and maintain secure systems and applications	**Control Reduction Recommended?**		**If yes, provide brief justification for control reduction,**
	Y	**N**	
6.1 Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as "high," "medium," or "low") to newly discovered security vulnerabilities. ***Note:*** *Risk rankings should be based on industry best practices as well as consideration of potential impact. For example, criteria for ranking vulnerabilities may include consideration of the CVSS base score, and/or the classification by the vendor, and/or type of systems affected. Methods for evaluating vulnerabilities and assigning risk ratings will vary based on an organization's environment and risk-assessment strategy. Risk rankings should, at a minimum, identify all vulnerabilities considered to be a "high risk" to the environment. In addition to the risk ranking, vulnerabilities may be considered "critical" if they pose an imminent threat to the environment, impact critical systems, and/or would result in a potential compromise if not addressed. Examples of critical systems may include security systems, public-facing devices and systems, databases, and other systems that store, process, or transmit cardholder data.*	☐	☒	Vulnerability alerting for systems that only handle encrypted account data may be considered not applicable. However, merchants must understand and document the vulnerability alerting processes provided by the encryption solution provider and POI vendors, to ensure POI devices are updated when security vulnerabilities are identified.
6.2 Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release. ***Note:*** Critical security patches should be identified according to the risk ranking process defined in Requirement 6.1.	☒	☐	Vulnerability alerting for systems that only handle encrypted account data may be considered not applicable. However, merchants must understand and document the vulnerability alerting processes provided by the encryption solution provider and POI vendors, to ensure POI devices are updated when security vulnerabilities are identified.
6.3 Develop internal and external software applications (including web-based administrative access to applications) securely, as follows: • In accordance with PCI DSS (for example, secure authentication and logging) • Based on industry standards and/or best practices. • Incorporating information security throughout the software-development life cycle ***Note****: This applies to all software developed internally as well as bespoke or custom software developed by a third party.*	☒	☐	Software applications cannot impact the security of PAN/SAD data which is encrypted within the POI.
6.3.1 Remove development, test and/or custom application accounts, user IDs, and passwords before applications become active or are released to customers.	☒	☐	Software applications cannot impact the security of PAN/SAD data which is encrypted within the POI.

6.3.2 Review custom code prior to release to production or customers in order to identify any potential coding vulnerability (using either manual or automated processes) to include at least the following: • Code changes are reviewed by individuals other than the originating code author, and by individuals knowledgeable about code-review techniques and secure coding practices. • Code reviews ensure code is developed according to secure coding guidelines • Appropriate corrections are implemented prior to release. • Code-review results are reviewed and approved by management prior to release. ***Note**: This requirement for code reviews applies to all custom code (both internal and public-facing), as part of the system development life cycle. Code reviews can be conducted by knowledgeable internal personnel or third parties. Public-facing web applications are also subject to additional controls, to address ongoing threats and vulnerabilities after implementation, as defined at PCI DSS Requirement 6.6.*	☒	☐	Software applications cannot impact the security of PAN/SAD data which is encrypted within the POI.
6.4 Follow change control processes and procedures for all changes to system components. The processes must include the following:	☐	☒	Coalfire recommends change control processes be used for tracking POI devices within the environment. Change management processes for other systems would be not applicable.
6.4.1 Separate development/test environments from production environments, and enforce the separation with access controls.	☒	☐	Development/test environments cannot impact the security of PAN/SAD data which is encrypted within the POI.
6.4.2 Separation of duties between development/test and production environments	☒	☐	Development/test environments cannot impact the security of PAN/SAD data which is encrypted within the POI.
6.4.3 Production data (live PANs) are not used for testing or development	☒	☐	Development/test environments cannot impact the security of PAN/SAD data which is encrypted within the POI.
6.4.4 Removal of test data and accounts from system components before the system becomes active/goes into production.	☒	☐	Development/test environments cannot impact the security of PAN/SAD data which is encrypted within the POI.
6.4.5 Change control procedures must include the following:	☐	☒	Coalfire recommends change control processes be used for tracking POI devices within the environment. Change management processes for other systems would be not applicable.
6.4.5.1 Documentation of impact.	☐	☒	Coalfire recommends change control processes be used for tracking POI devices within the environment. Change management processes for other systems would be not applicable.
6.4.5.2 Documented change approval by authorized parties.	☐	☒	Coalfire recommends change control processes be used for tracking POI devices within the environment. Change management processes for other systems would be not applicable.
6.4.5.3 Functionality testing to verify that the change does not adversely impact the security of the system.	☐	☒	Coalfire recommends change control processes be used for tracking POI devices within the environment. Change management processes for other systems would be not applicable.
6.4.5.4 Back-out procedures.	☐	☒	Coalfire recommends change control processes be used for tracking POI devices within the

			environment. Change management processes for other systems would be not applicable.
6.4.6 Upon completion of a significant change, all relevant PCI DSS requirements must be implemented on all new or changed systems and networks, and documentation updated as applicable. ***Note:*** *This requirement is a best practice until January 31, 2018, after which it becomes a requirement.*	☐	☒	Coalfire recommends change control processes be used for tracking POI devices within the environment. Change management processes for other systems would be not applicable.
6.5 Address common coding vulnerabilities in software-development processes as follows: • Train developers at least annually in up-to-date secure coding techniques, including how to avoid common coding vulnerabilities. • Develop applications based on secure coding guidelines. ***Note:*** *The vulnerabilities listed at 6.5.1 through 6.5.10 were current with industry best practices when this version of PCI DSS was published. However, as industry best practices for vulnerability management are updated (for example, the OWASP Guide, SANS CWE Top 25, CERT Secure Coding, etc.), the current best practices must be used for these requirements.* ***Note:*** *Requirements 6.5.1 through 6.5.6, below, apply to all applications (internal or external).*	☒	☐	Software applications cannot impact the security of PAN/SAD data which is encrypted within the POI.
6.5.1 Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws.	☒	☐	Software applications cannot impact the security of PAN/SAD data which is encrypted within the POI.
6.5.2 Buffer overflows	☒	☐	Software applications cannot impact the security of PAN/SAD data which is encrypted within the POI.
6.5.3 Insecure cryptographic storage	☒	☐	Software applications cannot impact the security of PAN/SAD data which is encrypted within the POI.
6.5.4 Insecure communications	☒	☐	Software applications cannot impact the security of PAN/SAD data which is encrypted within the POI.
6.5.5 Improper error handling	☒	☐	Software applications cannot impact the security of PAN/SAD data which is encrypted within the POI.
6.5.6 All “high risk” vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.1). ***Note:*** *Requirements 6.5.7 through 6.5.10, below, apply to web applications and application interfaces (internal or external):*	☒ ☒	☐ ☐	Software applications cannot impact the security of PAN/SAD data which is encrypted within the POI.
6.5.7 Cross-site scripting (XSS)	☒	☐	Software applications cannot impact the security of PAN/SAD data which is encrypted within the POI.
6.5.8 Improper access control (such as insecure direct object references, failure to restrict URL access, directory traversal, and failure to restrict user access to functions).	☒	☐	Software applications cannot impact the security of PAN/SAD data which is encrypted within the POI.
6.5.9 Cross-site request forgery (CSRF)	☒	☐	Software applications cannot impact the security of PAN/SAD data which is encrypted within the POI.

6.5.10 Broken authentication and session management	☒	☐	Software applications cannot impact the security of PAN/SAD data which is encrypted within the POI.
6.6 For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods: • Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes ***Note:*** *This assessment is not the same as the vulnerability scans performed for Requirement 11.2.* • Installing an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) in front of public-facing web applications, to continually check all traffic.	☒	☐	Software applications cannot impact the security of PAN/SAD data which is encrypted within the POI.
6.7 Ensure that security policies and operational procedures for developing and maintaining secure systems and applications are documented, in use, and known to all affected parties.	☐	☒	Even with the significant reduction of applicable controls warranted by the solution obtains, Coalfire recommends that merchants have appropriate policies and operational procedures.
Requirement 7: Restrict access to cardholder data by business need to know	**Control Reduction Recommended?**		**If yes, provide brief justification for control reduction,**
	Y	**N**	
7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.	☒	☐	Access to system components cannot impact the security of PAN/SAD data which is encrypted within the POI.
7.1.1 Define access needs for each role, including: • System components and data resources that each role needs to access for their job function • Level of privilege required (for example, user, administrator, etc.) for accessing resources.	☒	☐	Access to system components cannot impact the security of PAN/SAD data which is encrypted within the POI.
7.1.2 Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.	☒	☐	Access to system components cannot impact the security of PAN/SAD data which is encrypted within the POI.
7.1.3 Assign access based on individual personnel's job classification and function.	☒	☐	Access to system components cannot impact the security of PAN/SAD data which is encrypted within the POI.
7.1.4 Require documented approval by authorized parties specifying required privileges.	☒	☐	Access to system components cannot impact the security of PAN/SAD data which is encrypted within the POI.
7.2 Establish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system(s) must include the following:	☒	☐	Access to system components cannot impact the security of PAN/SAD data which is encrypted within the POI.
7.2.1 Coverage of all system components	☒	☐	Access to system components cannot impact the security of PAN/SAD data which is encrypted within the POI.
7.2.2 Assignment of privileges to individuals based on job classification and function.	☒	☐	Access to system components cannot impact the security of PAN/SAD data which is encrypted within the POI.

7.2.3 Default "deny-all" setting.	☒	☐	Access to system components cannot impact the security of PAN/SAD data which is encrypted within the POI.
7.3 Ensure that security policies and operational procedures for restricting access to cardholder data are documented, in use, and known to all affected parties.	☐	☒	Even with the significant reduction of applicable controls warranted by the solution obtains, Coalfire recommends that merchants have appropriate policies and operational procedures.
Requirement 8: Assign a unique ID to each person with computer access	**Control Reduction Recommended?**		**If yes, provide brief justification for control reduction,**
	Y	**N**	
8.1 Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components as follows:	☒	☐	Access to system components cannot impact the security of PAN/SAD data which is encrypted within the POI.
8.1.1 Assign all users a unique ID before allowing them to access system components or cardholder data.	☒	☐	Access to system components cannot impact the security of PAN/SAD data which is encrypted within the POI.
8.1.2 Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.	☒	☐	Access to system components cannot impact the security of PAN/SAD data which is encrypted within the POI.
8.1.3 Immediately revoke access for any terminated users.	☒	☐	Access to system components cannot impact the security of PAN/SAD data which is encrypted within the POI.
8.1.4 Remove/disable inactive user accounts within 90 days.	☒	☐	Access to system components cannot impact the security of PAN/SAD data which is encrypted within the POI.
8.1.5 Manage IDs used by third parties to access, support, or maintain system components via remote access as follows: • Enabled only during the time period needed and disabled when not in use. • Monitored when in use.	☒	☐	Access to system components cannot impact the security of PAN/SAD data which is encrypted within the POI.
8.1.6 Limit repeated access attempts by locking out the user ID after not more than six attempts.	☒	☐	Access to system components cannot impact the security of PAN/SAD data which is encrypted within the POI.
8.1.7 Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.	☒	☐	Access to system components cannot impact the security of PAN/SAD data which is encrypted within the POI.
8.1.8 If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.	☒	☐	Access to system components cannot impact the security of PAN/SAD data which is encrypted within the POI.
8.2 In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components by employing at least one of the following methods to authenticate all users: • Something you know, such as a password or passphrase • Something you have, such as a token device or smart card • Something you are, such as a biometric.	☒	☐	Access to system components cannot impact the security of PAN/SAD data which is encrypted within the POI.

8.2.1 Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.	☒	☐	Access to system components cannot impact the security of PAN/SAD data which is encrypted within the POI.
8.2.2 Verify user identity before modifying any authentication credential—for example, performing password resets, provisioning new tokens, or generating new keys.	☒	☐	Access to system components cannot impact the security of PAN/SAD data which is encrypted within the POI.
8.2.3 Passwords/passphrases must meet the following: • Require a minimum length of at least seven characters. • Contain both numeric and alphabetic characters. Alternatively, the passwords/passphrases must have complexity and strength at least equivalent to the parameters specified above.	☒	☐	Access to system components cannot impact the security of PAN/SAD data which is encrypted within the POI.
8.2.4 Change user passwords/passphrases at least once every 90 days.	☒	☐	Access to system components cannot impact the security of PAN/SAD data which is encrypted within the POI.
8.2.5 Do not allow an individual to submit a new password/passphrase that is the same as any of the last four passwords/passphrases he or she has used.	☒	☐	Access to system components cannot impact the security of PAN/SAD data which is encrypted within the POI.
8.2.6 Set passwords/passphrases for first-time use and upon reset to a unique value for each user, and change immediately after the first use.	☒	☐	Access to system components cannot impact the security of PAN/SAD data which is encrypted within the POI.
8.3 Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication. ***Note:*** *Multi-factor authentication requires that a minimum of two of the three authentication methods (see Requirement 8.2 for descriptions of authentication methods) be used for authentication. Using one factor twice (for example, using two separate passwords) is not considered multi-factor authentication.*	☒	☐	Access to system components cannot impact the security of PAN/SAD data which is encrypted within the POI.
8.3.1 Incorporate multi-factor authentication for all non-console access into the CDE for personnel with administrative access. ***Note:*** *This requirement is a best practice until January 31, 2018, after which it becomes a requirement.*	☒	☐	Access to system components cannot impact the security of PAN/SAD data which is encrypted within the POI.
8.3.2 Incorporate multi-factor authentication for all remote network access (both user and administrator, and including third party access for support or maintenance) originating from outside the entity's network.	☒	☐	Access to system components cannot impact the security of PAN/SAD data which is encrypted within the POI.
8.4 Document and communicate authentication policies and procedures to all users including: • Guidance on selecting strong authentication credentials • Guidance for how users should protect their authentication credentials • Instructions not to reuse previously used passwords • Instructions to change passwords if there is any suspicion the password could be compromised.	☒	☐	Access to system components cannot impact the security of PAN/SAD data which is encrypted within the POI.
8.5 Do not use group, shared, or generic IDs, passwords, or other authentication methods as follows: • Generic user IDs are disabled or removed. • Shared user IDs do not exist for system administration and other critical functions. • Shared and generic user IDs are not used to administer any system components.	☒	☐	Access to system components cannot impact the security of PAN/SAD data which is encrypted within the POI.

8.5.1 ***Additional requirement for service providers only****:* Service providers with remote access to customer premises (for example, for support of POS systems or servers) must use a unique authentication credential (such as a password/phrase) for each customer. ***Note:*** *This requirement is not intended to apply to shared hosting providers accessing their own hosting environment, where multiple customer environments are hosted.*	☒	☐	Access to system components cannot impact the security of PAN/SAD data which is encrypted within the POI.
8.6 Where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, certificates, etc.), use of these mechanisms must be assigned as follows: • Authentication mechanisms must be assigned to an individual account and not shared among multiple accounts. • Physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access.	☒	☐	Access to system components cannot impact the security of PAN/SAD data which is encrypted within the POI.
8.7 All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted as follows: • All user access to, user queries of, and user actions on databases are through programmatic methods. • Only database administrators have the ability to directly access or query databases. • Application IDs for database applications can only be used by the applications (and not by individual users or other non-application processes).	☒	☐	Access to system components cannot impact the security of PAN/SAD data which is encrypted within the POI.
8.8 Ensure that security policies and operational procedures for identification and authentication are documented, in use, and known to all affected parties.	☐	☒	Even with the significant reduction of applicable controls warranted by the solution obtains, Coalfire recommends that merchants have appropriate policies and operational procedures.
Requirement 9: Restrict physical access to cardholder data	**Control Reduction Recommended?**		**If yes, provide brief justification for control reduction,**
	Y	**N**	
9.1 Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.	☐	☒	Appropriate physical controls to ensure that the POI devices cannot be physically altered and perimeter devices are properly protected should be in place. Physical controls also apply to protection of paper media containing cardholder data.
9.1.1 Use either video cameras or access control mechanisms (or both) to monitor individual physical access to sensitive areas. Review collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law. ***Note:*** *"Sensitive areas" refers to any data center, server room or any area that houses systems that store, process, or transmit cardholder data. This excludes public-facing areas where only point-of-sale terminals are present, such as the cashier areas in a retail store.*	☒	☐	Merchants do not have sensitive areas because cleartext PAN/SAD data is not available in the environment.
9.1.2 Implement physical and/or logical controls to restrict access to publicly accessible network jacks. For example, network jacks located in public areas and areas accessible to visitors could be disabled and only enabled when network access is explicitly authorized. Alternatively, processes could be implemented to ensure that visitors are escorted at all times in areas with active network jacks.	☒	☐	Merchants do not have sensitive areas because cleartext PAN/SAD data is not available in the environment.

9.1.3 Restrict physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines.	☒	☐	Merchants do not have sensitive areas because cleartext PAN/SAD data is not available in the environment.
9.2 Develop procedures to easily distinguish between onsite personnel and visitors, to include: • Identifying onsite personnel and visitors (for example, assigning badges) • Changes to access requirements • Revoking or terminating onsite personnel and expired visitor identification (such as ID badges).	☐	☒	Controls should ensure that identity and authorization of any personnel servicing POI is verified.
9.3 Control physical access for onsite personnel to sensitive areas as follows: • Access must be authorized and based on individual job function. • Access is revoked immediately upon termination, and all physical access mechanisms, such as keys, access cards, etc., are returned or disabled.	☐	☒	Controls should ensure that identity and authorization of any personnel servicing POI is verified.
9.4 Implement procedures to identify and authorize visitors. Procedures should include the following:	☐	☒	Controls should ensure that identity and authorization of any personnel servicing POI is verified.
9.4.1 Visitors are authorized before entering, and escorted at all times within, areas where cardholder data is processed or maintained.	☐	☒	Controls should ensure that identity and authorization of any personnel servicing POI is verified.
9.4.2 Visitors are identified and given a badge or other identification that expires and that visibly distinguishes the visitors from onsite personnel.	☐	☒	Controls should ensure that identity and authorization of any personnel servicing POI is verified.
9.4.3 Visitors are asked to surrender the badge or identification before leaving the facility or at the date of expiration.	☐	☒	Controls should ensure that identity and authorization of any personnel servicing POI is verified.
9.4.4 A visitor log is used to maintain a physical audit trail of visitor activity to the facility as well as computer rooms and data centers where cardholder data is stored or transmitted. Document the visitor's name, the firm represented, and the onsite personnel authorizing physical access on the log. Retain this log for a minimum of three months, unless otherwise restricted by law.	☐	☒	Controls should ensure that identity and authorization of any personnel servicing POI is verified.
9.5 Physically secure all media.	☐	☒	If the merchant has any paper-based processes associated with this payment channel, then this requirement will still apply to their environment. Otherwise, this requirement can be considered not applicable.
9.5.1 Store media backups in a secure location, preferably an off-site facility, such as an alternate or backup site, or a commercial storage facility. Review the location's security at least annually.	☐	☒	If the merchant has any paper-based processes associated with this payment channel, then this requirement will still apply to their environment. Otherwise, this requirement can be considered not applicable.
9.6 Maintain strict control over the internal or external distribution of any kind of media, including the following:	☐	☒	If the merchant has any paper-based processes associated with this payment channel, then this requirement will still apply to their environment. Otherwise, this requirement can be considered not applicable.
9.6.1 Classify media so the sensitivity of the data can be determined.	☐	☒	If the merchant has any paper-based processes associated with this payment channel, then this

			requirement will still apply to their environment. Otherwise, this requirement can be considered not applicable.
9.6.2 Send the media by secured courier or other delivery method that can be accurately tracked.	☐	☒	If the merchant has any paper-based processes associated with this payment channel, then this requirement will still apply to their environment. Otherwise, this requirement can be considered not applicable.
9.6.3 Ensure management approves any and all media that is moved from a secured area (including when media is distributed to individuals).	☐	☒	If the merchant has any paper-based processes associated with this payment channel, then this requirement will still apply to their environment. Otherwise, this requirement can be considered not applicable.
9.7 Maintain strict control over the storage and accessibility of media.	☐	☒	If the merchant has any paper-based processes associated with this payment channel, then this requirement will still apply to their environment. Otherwise, this requirement can be considered not applicable.
9.7.1 Properly maintain inventory logs of all media and conduct media inventories at least annually.	☐	☒	If the merchant has any paper-based processes associated with this payment channel, then this requirement will still apply to their environment. Otherwise, this requirement can be considered not applicable.
9.8 Destroy media when it is no longer needed for business or legal reasons as follows:	☐	☒	If the merchant has any paper-based processes associated with this payment channel, then this requirement will still apply to their environment. Otherwise, this requirement can be considered not applicable.
9.8.1 Shred, incinerate, or pulp hard-copy materials so that cardholder data cannot be reconstructed. Secure storage containers used for materials that are to be destroyed.	☐	☒	If the merchant has any paper-based processes associated with this payment channel, then this requirement will still apply to their environment. Otherwise, this requirement can be considered not applicable.
9.8.2 Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.	☒	☐	There will be no electronic instances of cardholder data storage within the merchant environment.
9.9 Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution. ***Note**: These requirements apply to card-reading devices used in card-present transactions (that is, card swipe or dip) at the point of sale. This requirement is not intended to apply to manual key-entry components such as computer keyboards and POS keypads.*	☐	☒	
9.9.1 Maintain an up-to-date list of devices. The list should include the following: • Make, model of device • Location of device (for example, the address of the site or facility where the device is located) • Device serial number or other method of unique identification.	☐	☒	

9.9.2 Periodically inspect device surfaces to detect tampering (for example, addition of card skimmers to devices), or substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device). ***Note:*** *Examples of signs that a device might have been tampered with or substituted include unexpected attachments or cables plugged into the device, missing or changed security labels, broken or differently colored casing, or changes to the serial number or other external markings.*	☐	☒	
9.9.3 Provide training for personnel to be aware of attempted tampering or replacement of devices. Training should include the following: • Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices. • Do not install, replace, or return devices without verification. • Be aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices). • Report suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer).	☐	☒	
9.10 Ensure that security policies and operational procedures for restricting physical access to cardholder data are documented, in use, and known to all affected parties.	☐	☒	Even with the significant reduction of applicable controls warranted by the solution obtains, Coalfire recommends that merchants have appropriate policies and operational procedures.
Requirement 10: Track and monitor all access to network resources and cardholder data	**Control Reduction Recommended?**		**If yes, provide brief justification for control reduction,**
	Y	**N**	
10.1 Implement audit trails to link all access to system components to each individual user.	☒	☐	System components cannot impact the security of PAN/SAD data which is encrypted within the POI.
10.2 Implement automated audit trails for all system components to reconstruct the following events:	☒	☐	System components cannot impact the security of PAN/SAD data which is encrypted within the POI.
10.2.1 All individual user accesses to cardholder data	☒	☐	System components cannot impact the security of PAN/SAD data which is encrypted within the POI.
10.2.2 All actions taken by any individual with root or administrative privileges	☒	☐	System components cannot impact the security of PAN/SAD data which is encrypted within the POI.
10.2.3 Access to all audit trails	☒	☐	System components cannot impact the security of PAN/SAD data which is encrypted within the POI.
10.2.4 Invalid logical access attempts	☒	☐	System components cannot impact the security of PAN/SAD data which is encrypted within the POI.
10.2.5 Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges	☒	☐	System components cannot impact the security of PAN/SAD data which is encrypted within the POI.
10.2.6 Initialization, stopping, or pausing of the audit logs	☒	☐	System components cannot impact the security of PAN/SAD data which is encrypted within the POI.
10.2.7 Creation and deletion of system-level objects	☒	☐	System components cannot impact the security of PAN/SAD data which is encrypted within the POI.
10.3 Record at least the following audit trail entries for all system components for each event:	☒	☐	System components cannot impact the security of PAN/SAD data which is encrypted within the POI.

10.3.1 User identification	☒	☐	System components cannot impact the security of PAN/SAD data which is encrypted within the POI.
10.3.2 Type of event	☒	☐	System components cannot impact the security of PAN/SAD data which is encrypted within the POI.
10.3.3 Date and time	☒	☐	System components cannot impact the security of PAN/SAD data which is encrypted within the POI.
10.3.4 Success or failure indication	☒	☐	System components cannot impact the security of PAN/SAD data which is encrypted within the POI.
10.3.5 Origination of event	☒	☐	System components cannot impact the security of PAN/SAD data which is encrypted within the POI.
10.3.6 Identity or name of affected data, system component, or resource.	☒	☐	System components cannot impact the security of PAN/SAD data which is encrypted within the POI.
10.4 Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time. ***Note:*** *One example of time synchronization technology is Network Time Protocol (NTP).*	☒	☐	System components cannot impact the security of PAN/SAD data which is encrypted within the POI.
10.4.1 Critical systems have the correct and consistent time.	☒	☐	System components cannot impact the security of PAN/SAD data which is encrypted within the POI.
10.4.2 Time data is protected.	☒	☐	System components cannot impact the security of PAN/SAD data which is encrypted within the POI.
10.4.3 Time settings are received from industry-accepted time sources.	☒	☐	System components cannot impact the security of PAN/SAD data which is encrypted within the POI.
10.5 Secure audit trails so they cannot be altered.	☒	☐	System components cannot impact the security of PAN/SAD data which is encrypted within the POI.
10.5.1 Limit viewing of audit trails to those with a job-related need.	☒	☐	System components cannot impact the security of PAN/SAD data which is encrypted within the POI.
10.5.2 Protect audit trail files from unauthorized modifications.	☒	☐	System components cannot impact the security of PAN/SAD data which is encrypted within the POI.
10.5.3 Promptly back up audit trail files to a centralized log server or media that is difficult to alter.	☒	☐	System components cannot impact the security of PAN/SAD data which is encrypted within the POI.
10.5.4 Write logs for external-facing technologies onto a secure, centralized, internal log server or media device.	☒	☐	System components cannot impact the security of PAN/SAD data which is encrypted within the POI.
10.5.5 Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).	☒	☐	System components cannot impact the security of PAN/SAD data which is encrypted within the POI.
10.6 Review logs and security events for all system components to identify anomalies or suspicious activity. ***Note:*** *Log harvesting, parsing, and alerting tools may be used to meet this Requirement.*	☒	☐	System components cannot impact the security of PAN/SAD data which is encrypted within the POI.
10.6.1 Review the following at least daily: • All security events • Logs of all system components that store, process, or transmit CHD and/or SAD • Logs of all critical system components • Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.).	☒	☐	System components cannot impact the security of PAN/SAD data which is encrypted within the POI.

10.6.2 Review logs of all other system components periodically based on the organization's policies and risk management strategy, as determined by the organization's annual risk assessment.	☒	☐	System components cannot impact the security of PAN/SAD data which is encrypted within the POI.
10.6.3 Follow up exceptions and anomalies identified during the review process.	☒	☐	System components cannot impact the security of PAN/SAD data which is encrypted within the POI.
10.7 Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup).	☒	☐	System components cannot impact the security of PAN/SAD data which is encrypted within the POI.
10.8 ***Additional requirement for service providers only:*** Implement a process for the timely detection and reporting of failures of critical security control systems, including but not limited to failure of: • Firewalls • IDS/IPS • FIM • Anti-virus • Physical access controls • Logical access controls • Audit logging mechanisms • Segmentation controls (if used) ***Note:*** *This requirement is a best practice until January 31, 2018, after which it becomes a requirement.*	☒	☐	This NESA is intended for use by merchants, and not for service providers. This control requirement is not applicable to merchants.
10.8.1 ***Additional requirement for service providers only*:** Respond to failures of any critical security controls in a timely manner. Processes for responding to failures in security controls must include: • Restoring security functions • Identifying and documenting the duration (date and time start to end) of the security failure • Identifying and documenting cause(s) of failure, including root cause, and documenting remediation required to address root cause • Identifying and addressing any security issues that arose during the failure • Performing a risk assessment to determine whether further actions are required as a result of the security failure • Implementing controls to prevent cause of failure from reoccurring • Resuming monitoring of security controls ***Note:*** *This requirement is a best practice until January 31, 2018, after which it becomes a requirement.*	☒	☐	This NESA is intended for use by merchants, and not for service providers. This control requirement is not applicable to merchants.
10.9 Ensure that security policies and operational procedures for monitoring all access to network resources and cardholder data are documented, in use, and known to all affected parties.	☐	☒	Even with the significant reduction of applicable controls warranted by the solution obtains, Coalfire recommends that merchants have appropriate policies and operational procedures.

Requirement 11: Regularly test security systems and processes	**Control Reduction Recommended?**		**If yes, provide brief justification for control reduction,**
	Y	**N**	
11.1 Implement processes to test for the presence of wireless access points (802.11), and detect and identify all authorized and unauthorized wireless access points on a quarterly basis. ***Note:*** *Methods that may be used in the process include but are not limited to wireless network scans, physical/logical inspections of system components and infrastructure, network access control (NAC), or wireless IDS/IPS. Whichever methods are used, they must be sufficient to detect and identify both authorized and unauthorized devices.*	☒	☐	System components cannot impact the security of PAN/SAD data which is encrypted within the POI.
11.1.1 Maintain an inventory of authorized wireless access points including a documented business justification.	☒	☐	System components cannot impact the security of PAN/SAD data which is encrypted within the POI.
11.1.2 Implement incident response procedures in the event unauthorized wireless access points are detected.	☒	☐	System components cannot impact the security of PAN/SAD data which is encrypted within the POI.
11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades). ***Note:*** *Multiple scan reports can be combined for the quarterly scan process to show that all systems were scanned and all applicable vulnerabilities have been addressed. Additional documentation may be required to verify non-remediated vulnerabilities are in the process of being addressed.* *For initial PCI DSS compliance, it is not required that four quarters of passing scans be completed if the assessor verifies 1) the most recent scan result was a passing scan, 2) the entity has documented policies and procedures requiring quarterly scanning, and 3) vulnerabilities noted in the scan results have been corrected as shown in a re-scan(s). For subsequent years after the initial PCI DSS review, four quarters of passing scans must have occurred.*	☒	☐	System components cannot impact the security of PAN/SAD data which is encrypted within the POI.
11.2.1 Perform quarterly internal vulnerability scans. Address vulnerabilities and perform rescans to verify all “high risk” vulnerabilities are resolved in accordance with the entity’s vulnerability ranking (per Requirement 6.1). Scans must be performed by qualified personnel.	☒	☐	System components cannot impact the security of PAN/SAD data which is encrypted within the POI.
11.2.2 Perform quarterly external vulnerability scans, via an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC). Perform rescans as needed, until passing scans are achieved. ***Note:*** *Quarterly external vulnerability scans must be performed by an Approved Scanning Vendor (ASV), approved by the Payment Card Industry Security Standards Council (PCI SSC). Refer to the ASV Program Guide published on the PCI SSC website for scan customer responsibilities, scan preparation, etc.*	☒	☐	System components cannot impact the security of PAN/SAD data which is encrypted within the POI.
11.2.3 Perform internal and external scans, and rescans as needed, after any significant change. Scans must be performed by qualified personnel.	☒	☐	System components cannot impact the security of PAN/SAD data which is encrypted within the POI.

11.3 Implement a methodology for penetration testing that includes the following: • Is based on industry-accepted penetration testing approaches (for example, NIST SP800-115) • Includes coverage for the entire CDE perimeter and critical systems • Includes testing from both inside and outside the network • Includes testing to validate any segmentation and scope-reduction controls • Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5 • Defines network-layer penetration tests to include components that support network functions as well as operating systems • Includes review and consideration of threats and vulnerabilities experienced in the last 12 months • Specifies retention of penetration testing results and remediation activities results.	☒	☐	System components cannot impact the security of PAN/SAD data which is encrypted within the POI.
11.3.1 Perform *external* penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).	☒	☐	System components cannot impact the security of PAN/SAD data which is encrypted within the POI.
11.3.2 Perform *internal* penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).	☒	☐	System components cannot impact the security of PAN/SAD data which is encrypted within the POI.
11.3.3 Exploitable vulnerabilities found during penetration testing are corrected and testing is repeated to verify the corrections.	☒	☐	System components cannot impact the security of PAN/SAD data which is encrypted within the POI.
11.3.4 If segmentation is used to isolate the CDE from other networks, perform penetration tests at least annually and after any changes to segmentation controls/methods to verify that the segmentation methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE.	☒	☐	System components cannot impact the security of PAN/SAD data which is encrypted within the POI.
11.3.4.1 ***Additional requirement for service providers only:*** If segmentation is used, confirm PCI DSS scope by performing penetration testing on segmentation controls at least every six months and after any changes to segmentation controls/methods. ***Note:*** *This requirement is a best practice until January 31, 2018, after which it becomes a requirement.*	☒	☐	This NESA is intended for use by merchants, and not for service providers. This control requirement is not applicable to merchants.
11.4 Use intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up to date.	☒	☐	System components cannot impact the security of PAN/SAD data which is encrypted within the POI.
11.5 Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly. ***Note:*** *For change-detection purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. Change-detection mechanisms such as file-integrity monitoring products usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is, the merchant or service provider).*	☒	☐	System components cannot impact the security of PAN/SAD data which is encrypted within the POI.

11.5.1 Implement a process to respond to any alerts generated by the change-detection solution.	☒	☐	System components cannot impact the security of PAN/SAD data which is encrypted within the POI.
11.6 Ensure that security policies and operational procedures for security monitoring and testing are documented, in use, and known to all affected parties.	☐	☒	Even with the significant reduction of applicable controls warranted by the solution obtains, Coalfire recommends that merchants have appropriate policies and operational procedures.
Requirement 12: Maintain a policy that addresses information security for all personnel	**Control Reduction Recommended?**		**If yes, provide brief justification for control reduction,**
	Y	**N**	
12.1 Establish, publish, maintain, and disseminate a security policy.	☐	☒	
12.1.1 Review the security policy at least annually and update the policy when the environment changes.	☐	☒	
12.2 Implement a risk-assessment process that: • Is performed at least annually and upon significant changes to the environment (for example, acquisition, merger, relocation, etc.), • Identifies critical assets, threats, and vulnerabilities, and • Results in a formal, documented analysis of risk. *Examples of risk-assessment methodologies include but are not limited to OCTAVE, ISO 27005 and NIST SP 800-30.*	☐	☒	
12.3 Develop usage policies for critical technologies and define proper use of these technologies. ***Note:*** *Examples of critical technologies include, but are not limited to, remote access and wireless technologies, laptops, tablets, removable electronic media, e-mail usage and Internet usage.* *Ensure these usage policies require the following:*	☐	☒	
12.3.1 Explicit approval by authorized parties	☐	☒	
12.3.2 Authentication for use of the technology	☐	☒	
12.3.3 A list of all such devices and personnel with access	☐	☒	
12.3.4 A method to accurately and readily determine owner, contact information, and purpose (for example, labeling, coding, and/or inventorying of devices)	☐	☒	
12.3.5 Acceptable uses of the technology	☐	☒	
12.3.6 Acceptable network locations for the technologies	☐	☒	
12.3.7 List of company-approved products	☐	☒	
12.3.8 Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity	☐	☒	
12.3.9 Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use	☐	☒	

12.3.10 For personnel accessing cardholder data via remote-access technologies, prohibit the copying, moving, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need. Where there is an authorized business need, the usage policies must require the data be protected in accordance with all applicable PCI DSS Requirements.	☒	☐	Cardholder data will not be accessible within the merchant environment
12.4 Ensure that the security policy and procedures clearly define information security responsibilities for all personnel.	☐	☒	
12.4.1 ***Additional requirement for service providers only***: Executive management shall establish responsibility for the protection of cardholder data and a PCI DSS compliance program to include: • Overall accountability for maintaining PCI DSS compliance • Defining a charter for a PCI DSS compliance program and communication to executive management ***Note:*** *This requirement is a best practice until January 31, 2018, after which it becomes a requirement.*	☒	☐	This NESA is intended for use by merchants, and not for service providers. This control requirement is not applicable to merchants.
12.5 Assign to an individual or team the following information security management responsibilities:	☐	☒	
12.5.1 Establish, document, and distribute security policies and procedures.	☐	☒	
12.5.2 Monitor and analyze security alerts and information, and distribute to appropriate personnel.	☐	☒	
12.5.3 Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.	☐	☒	
12.5.4 Administer user accounts, including additions, deletions, and modifications.	☐	☒	
12.5.5 Monitor and control all access to data.	☐	☒	
12.6 Implement a formal security awareness program to make all personnel aware of the cardholder data security policy and procedures.	☐	☒	
12.6.1 Educate personnel upon hire and at least annually. ***Note:*** *Methods can vary depending on the role of the personnel and their level of access to the cardholder data.*	☐	☒	
12.6.2 Require personnel to acknowledge at least annually that they have read and understood the security policy and procedures.	☐	☒	
12.7 Screen potential personnel prior to hire to minimize the risk of attacks from internal sources. (Examples of background checks include previous employment history, criminal record, credit history, and reference checks.) ***Note:*** *For those potential personnel to be hired for certain positions such as store cashiers who only have access to one card number at a time when facilitating a transaction, this requirement is a recommendation only.*	☐	☒	
12.8 Maintain and implement policies and procedures to manage service providers, with whom cardholder data is shared, or that could affect the security of cardholder data, as follows	☐	☒	The encryption solution provider is a particularly import service provider for the merchant.
12.8.1 Maintain a list of service providers including a description of the service provided.	☐	☒	

12.8.2 Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process or transmit on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment. ***Note:*** *The exact wording of an acknowledgement will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgement does not have to include the exact wording provided in this requirement.*	☐	☒	
12.8.3 Ensure there is an established process for engaging service providers including proper due diligence prior to engagement.	☐	☒	
12.8.4 Maintain a program to monitor service providers' PCI DSS compliance status at least annually.	☐	☒	
12.8.5 Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity.	☐	☒	
12.9 ***Additional requirement for service providers only*****:** Service providers acknowledge in writing to customers that they are responsible for the security of cardholder data the service provider possesses or otherwise stores, processes, or transmits on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment. ***Note:*** *The exact wording of an acknowledgement will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgement does not have to include the exact wording provided in this requirement.*	☒	☐	This NESA is intended for use by merchants, and not for service providers. This control requirement is not applicable to merchants.
12.10 Implement an incident response plan. Be prepared to respond immediately to a system breach.	☐	☒	The merchant incident response plan must include both notifying and receiving notifications from the encryption solution provider.
12.10.1 Create the incident response plan to be implemented in the event of system breach. Ensure the plan addresses the following, at a minimum: • Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum • Specific incident response procedures • Business recovery and continuity procedures • Data backup processes • Analysis of legal requirements for reporting compromises • Coverage and responses of all critical system components • Reference or inclusion of incident response procedures from the payment brands.	☐	☒	
12.10.2 Review and test the plan, including all elements listed in Requirement 12.10.1, at least annually.	☐	☒	
12.10.3 Designate specific personnel to be available on a 24/7 basis to respond to alerts.	☐	☒	
12.10.4 Provide appropriate training to staff with security breach response responsibilities.	☐	☒	
12.10.5 Include alerts from security monitoring systems, including but not limited to intrusion-detection, intrusion-prevention, firewalls, and file-integrity monitoring systems.	☐	☒	
12.10.6 Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.	☐	☒	

12.11 ***Additional requirement for service providers only:*** Perform reviews at least quarterly to confirm personnel are following security policies and operational procedures. Reviews must cover the following processes: • Daily log reviews • Firewall rule-set reviews • Applying configuration standards to new systems • Responding to security alerts • Change management processes ***Note:*** *This requirement is a best practice until January 31, 2018, after which it becomes a requirement.*	☒	☐	This NESA is intended for use by merchants, and not for service providers. This control requirement is not applicable to merchants.
12.11.1 ***Additional requirement for service providers only:*** Maintain documentation of quarterly review process to include: • Documenting results of the reviews • Review and sign off of results by personnel assigned responsibility for the PCI DSS compliance program ***Note:*** *This requirement is a best practice until January 31, 2018, after which it becomes a requirement.*	☒	☐	This NESA is intended for use by merchants, and not for service providers. This control requirement is not applicable to merchants.