US Signal Company, LLC

Payment Card Industry (PCI)
Data Security Standard (DSS)
Attestation of Compliance - Service Providers

July 30, 2024

Payment Card Industry
Data Security Standard

Attestation of Compliance for Report on Compliance – Service Providers

Version 4.0

Revision 2

Publication Date: August 2023

PCI DSS v4.0 Attestation of Compliance for Report on Compliance – Service Providers

Entity Name: US Signal Company, LLC

Assessment End Date: July 30, 2024

Date of Report as noted in the Report on Compliance: July 30, 2024

Section 1: Assessment Information

Instructions for Submission

This Attestation of Compliance (AOC) must be completed as a declaration of the results of the service provider's assessment against the *Payment Card Industry Data Security Standard (PCI DSS) Requirements and Testing Procedures (*"Assessment"). Complete all sections. The service provider is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact the entity(ies) to which this AOC will be submitted for reporting and submission procedures.

This AOC reflects the results documented in an associated Report on Compliance (ROC). Associated ROC sections are noted in each AOC Part/Section below.

Capitalized terms used but not otherwise defined in this document have the meanings set forth in the PCI DSS Report on Compliance Template.

Part 1. Contact Information

Part 1a. Assessed Entity (ROC Section 1.1)	
Company name:	US Signal Company, LLC
DBA (doing business as):	
Company mailing address:	201 Ionia Street SW Grand Rapids, MI 49503
Company main website:	https://ussignal.com
Company contact name:	Trevor Bidle
Company contact title:	Chief Information Security Officer
Contact phone number:	616-233-7609
Contact e-mail address:	tbidle@ussignal.com

Part 1b. Assessor (ROC Section 1.1)	
Provide the following information for all assessors involved in the Assessment. If there was no assessor for a given assessor type, enter Not Applicable.	
PCI SSC Internal Security Assessor(s)	
ISA name(s):	Not applicable.
Qualified Security Assessor	
Company name:	BDO USA
Company mailing address:	800 Nicollet Mall Suite 600 Minneapolis, MN 55402
Company website:	https://www.bdo.com
Lead Assessor name:	Brian Hill

Assessor phone number:	612-367-3128
Assessor e-mail address:	bhill@bdo.com
Assessor certificate number:	QSA, 203-807

Part 2. Executive Summary

Part 2a. Scope Verification

Services that were INCLUDED in the scope of the Assessment (select all that apply):

Name of service(s) assessed:	Hosting and managed services

Type of service(s) assessed:

Hosting Provider:	**Managed Services:**	**Payment Processing:**
☐ Applications / software	☒ Systems security services	☐ POI / card present
☒ Hardware	☒ IT support	☐ Internet / e-commerce
☒ Infrastructure / Network	☐ Physical security	☐ MOTO / Call Center
☒ Physical space (co-location)	☐ Terminal Management System	☐ ATM
☒ Storage	☐ Other services (specify):	☐ Other processing (specify):
☐ Web-hosting services		
☒ Security services		
☐ 3-D Secure Hosting Provider		
☐ Multi-Tenant Service Provider		
☐ Other Hosting (specify):		
☐ Account Management	☐ Fraud and Chargeback	☐ Payment Gateway/Switch
☐ Back-Office Services	☐ Issuer Processing	☐ Prepaid Services
☐ Billing Management	☐ Loyalty Programs	☐ Records Management
☐ Clearing and Settlement	☐ Merchant Services	☐ Tax/Government Payments
☐ Network Provider		
☐ Others (specify):		

Note: *These categories are provided for assistance only and are not intended to limit or predetermine an entity's service description. If these categories do not apply to the assessed service, complete "Others." If it is not clear whether a category could apply to the assessed service, consult with the entity(ies) to which this AOC will be submitted.*

Part 2. Executive Summary *(continued)*

Part 2a. Scope Verification *(continued)*

Services that are provided by the service provider but were NOT INCLUDED in the scope of the Assessment (select all that apply):

Name of service(s) not assessed:	Not applicable.

Type of service(s) not assessed:

Hosting Provider:	**Managed Services:**	**Payment Processing:**
☐ Applications / software	☐ Systems security services	☐ POI / card present
☐ Hardware	☐ IT support	☐ Internet / e-commerce
☐ Infrastructure / Network	☐ Physical security	☐ MOTO / Call Center
☐ Physical space (co-location)	☐ Terminal Management System	☐ ATM
☐ Storage	☐ Other services (specify):	☐ Other processing (specify):
☐ Web-hosting services		
☐ Security services		
☐ 3-D Secure Hosting Provider		
☐ Multi-Tenant Service Provider		
☐ Other Hosting (specify):		
☐ Account Management	☐ Fraud and Chargeback	☐ Payment Gateway/Switch
☐ Back-Office Services	☐ Issuer Processing	☐ Prepaid Services
☐ Billing Management	☐ Loyalty Programs	☐ Records Management
☐ Clearing and Settlement	☐ Merchant Services	☐ Tax/Government Payments
☐ Network Provider		
☐ Others (specify):		

Provide a brief explanation why any checked services were not included in the Assessment:	Not applicable.

Part 2b. Description of Role with Payment Cards (ROC Section 2.1)

Describe how the business stores, processes, and/or transmits account data.	US Signal is a colocation and a managed services provider to businesses. For colocation customers, US Signal provides space in its data centers, and provides power, physical security, and Internet connectivity. US Signal also offers managed services, which may include cloud, managed firewall, backup, network and system administration, and other services. US Signal does not directly interact with cardholder data. US Signal does not store, process or transmit cardholder data. US Signal does have administrative

	access to some systems that are within scope for its clients' PCI DSS compliance, and is therefore, assessing as a service provider for those services.
Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.	US Signal does not store, process or transmit cardholder data. US Signal does have administrative access to some systems that are within scope for its clients' PCI DSS compliance, and is therefore, assessing as a service provider for those services.
Describe system components that could impact the security of account data.	US Signal does not store, process or transmit cardholder data. US Signal does have administrative access to some systems that are within scope for its clients' PCI DSS compliance, and is therefore, assessing as a service provider for those services.

Part 2. Executive Summary *(continued)*

Part 2c. Description of Payment Card Environment

Provide a high-level description of the environment covered by this Assessment. *For example:* • *Connections into and out of the cardholder data environment (CDE).* • *Critical system components within the CDE, such as POI devices, databases, web servers, etc., and any other necessary payment components, as applicable.* • *System components that could impact the security of account data.*	US Signal is a colocation and a managed services provider to businesses. US Signal does not directly interact with cardholder data. The PCI environment is separate from the corporate environment. Technologies that protect and provide services to the CDE include: • Networking devices – used for controlling, managing, and monitoring traffic. • Multi-factor authentication (MFA) – for remote access and non-console access to systems for user and administrative authentication. • Domain controllers, intrusion detection, logging, security monitoring (alerting), anti-virus, file integrity monitoring, patch management, and vulnerability management.
Indicate whether the environment includes segmentation to reduce the scope of the Assessment. (Refer to the "Segmentation" section of PCI DSS for guidance on segmentation)	☒ Yes ☐ No

Part 2d. In-Scope Locations/Facilities (ROC Section 4.6)

List all types of physical locations/facilities (for example, corporate offices, data centers, call centers and mail rooms) in scope for this Assessment.

Facility Type	Total Number of Locations (How many locations of this type are in scope)	Location(s) of Facility (city, country)
Example: Data centers	*3*	*Boston, MA, USA*
US Signal Corporate Office	1	Grand Rapids, MI
Data centers	8	• Southfield, MI, USA • Kentwood, MI, USA • Byron Center, MI, USA • Oakbrook, IL, USA • Indianapolis, IN, USA • South Bend, IN, USA • Madison, WI, USA • Belleville, MI, USA

Part 2. Executive Summary *(continued)*

Part 2e. PCI SSC Validated Products and Solutions (ROC Section 3.3)

Does the entity use any item identified on any PCI SSC Lists of Validated Products and Solutions♦?

☐ Yes ☒ No

Provide the following information regarding each item the entity uses from PCI SSC's Lists of Validated Products and Solutions:

Name of PCI SSC-validated Product or Solution	Version of Product or Solution	PCI SSC Standard to which Product or Solution Was Validated	PCI SSC Listing Reference Number	Expiry Date of Listing
Not applicable.	Not applicable.	Not applicable.	Not applicable.	Not applicable.

♦ For purposes of this document, "Lists of Validated Products and Solutions" means the lists of validated products, solutions, and/or components appearing on the PCI SSC website (www.pcisecuritystandards.org)—for example, 3DS Software Development Kits, Approved PTS Devices, Validated Payment Software, Payment Applications (PA-DSS), Point to Point Encryption (P2PE) solutions, Software-Based PIN Entry on COTS (SPoC) solutions, and Contactless Payments on COTS (CPoC) solutions.

Part 2f. Third-Party Service Providers *(***ROC Section 4.4***)*	
For the services being validated, does the entity have relationships with one or more third-party service providers that:	
• Store, process, or transmit account data on the entity's behalf (for example, payment gateways, payment processors, payment service providers (PSPs, and off-site storage))	☐ Yes ☒ No
• Manage system components included in the entity's Assessment (for example, via network security control services, anti-malware services, security incident and event management (SIEM), contact and call centers, web-hosting companies, and IaaS, PaaS, SaaS, and FaaS cloud providers)	☐ Yes ☒ No
• Could impact the security of the entity's CDE (for example, vendors providing support via remote access, and/or bespoke software developers).	☐ Yes ☒ No

If Yes:	
Name of Service Provider:	**Description of Services Provided:**
Not applicable.	Not applicable.

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

Part 2. Executive Summary *(continued)*

Part 2g. Summary of Assessment (ROC Section 1.8.1)

Indicate below all responses provided within each principal PCI DSS requirement.

For all requirements identified as either "Not Applicable" or "Not Tested," complete the "Justification for Approach" table below.

Note: *One table to be completed for each service covered by this AOC. Additional copies of this section are available on the PCI SSC website.*

Name of Service Assessed: Hosting and managed services

PCI DSS Requirement	Requirement Finding More than one response may be selected for a given requirement. Indicate all responses that apply.				Select If Below Method(s) Was Used	
	In Place	Not Applicable	Not Tested	Not in Place	Customized Approach	Compensating Controls
Requirement 1:	☒	☒	☐	☐	☐	☐
Requirement 2:	☒	☒	☐	☐	☐	☐
Requirement 3:	☒	☒	☐	☐	☐	☐
Requirement 4:	☒	☒	☐	☐	☐	☐
Requirement 5:	☒	☒	☐	☐	☐	☐
Requirement 6:	☒	☒	☐	☐	☐	☐
Requirement 7:	☒	☒	☐	☐	☐	☐
Requirement 8:	☒	☒	☐	☐	☐	☐
Requirement 9:	☒	☒	☐	☐	☐	☐
Requirement 10:	☒	☒	☐	☐	☐	☐
Requirement 11:	☒	☒	☐	☐	☐	☒
Requirement 12:	☒	☒	☐	☐	☐	☐
Appendix A1:	☐	☒	☐	☐	☐	☐
Appendix A2:	☐	☒	☐	☐	☐	☐

Justification for Approach

For any Not Applicable responses, identify which sub-requirements were not applicable and the reason.	1.4.4 - Not applicable. US Signal does not store cardholder data. 2.3.2 - Not applicable. Inquired of US Signal personnel to determine wireless is not utilized within the CDE. Observed network diagrams and network rulesets to determine wireless is not utilized within the CDE. 3.1.1 - Not applicable. US Signal is a colocation, cloud service and managed service provider that does not have access to cardholder data and does not store cardholder data. 3.1.2 - Not applicable. US Signal is a colocation, cloud service and managed service provider that does not have access to cardholder data and does not store cardholder data. 3.2.1 - Not applicable. US Signal is a colocation, cloud service and managed service provider that does not have access to cardholder data and does not store cardholder data. 3.3.1 - Not applicable. US Signal is a colocation, cloud service and managed service provider that does not have access to cardholder data and does not store cardholder data. 3.3.1.1 - Not applicable. US Signal is a colocation, cloud service and managed service provider that does not have access to cardholder data and does not store cardholder data. 3.3.1.2 - Not applicable. US Signal is a colocation, cloud service and managed service provider that does not have access to cardholder data and does not store cardholder data. 3.3.1.3 - Not applicable. US Signal is a colocation, cloud service and managed service provider that does not have access to cardholder data and does not store cardholder data. 3.3.2 - Not applicable. US Signal is a colocation, cloud service and managed service provider that does not have access to cardholder data and does not store cardholder data. 3.3.3 - Not applicable. US Signal is a colocation, cloud service and managed service provider that does not have access to cardholder data and does not store cardholder data. 3.4.1 - Not applicable. US Signal is a colocation, cloud service and managed service provider that does not have access to cardholder data and does not store cardholder data. 3.4.2 - Not applicable. US Signal is a colocation, cloud service and managed service provider that does not have access to cardholder data and does not store cardholder data. 3.5.1 - Not applicable. US Signal is a colocation, cloud service and managed service provider that does not have access to cardholder data and does not store cardholder data. 3.5.1.1 - Not applicable. US Signal is a colocation, cloud service and managed service provider that

	does not have access to cardholder data and does not store cardholder data. 3.5.1.2 - Not applicable. US Signal is a colocation, cloud service and managed service provider that does not have access to cardholder data and does not store cardholder data. 3.5.1.3 - Not applicable. US Signal is a colocation, cloud service and managed service provider that does not have access to cardholder data and does not store cardholder data. 3.6.1 - Not applicable. US Signal is a colocation, cloud service and managed service provider that does not have access to cardholder data and does not store cardholder data. 3.6.1.1 - Not applicable. US Signal is a colocation, cloud service and managed service provider that does not have access to cardholder data and does not store cardholder data. 3.6.1.2 - Not applicable. US Signal is a colocation, cloud service and managed service provider that does not have access to cardholder data and does not store cardholder data. 3.6.1.3 - Not applicable. US Signal is a colocation, cloud service and managed service provider that does not have access to cardholder data and does not store cardholder data. 3.6.1.4 - Not applicable. US Signal is a colocation, cloud service and managed service provider that does not have access to cardholder data and does not store cardholder data. 3.7.1 - Not applicable. US Signal is a colocation, cloud service and managed service provider that does not have access to cardholder data and does not store cardholder data. 3.7.2 - Not applicable. US Signal is a colocation, cloud service and managed service provider that does not have access to cardholder data and does not store cardholder data. 3.7.3 - Not applicable. US Signal is a colocation, cloud service and managed service provider that does not have access to cardholder data and does not store cardholder data. 3.7.4 - Not applicable. US Signal is a colocation, cloud service and managed service provider that does not have access to cardholder data and does not store cardholder data. 3.7.5 - Not applicable. US Signal is a colocation, cloud service and managed service provider that does not have access to cardholder data and does not store cardholder data. 3.7.6 - Not applicable. US Signal is a colocation, cloud service and managed service provider that does not have access to cardholder data and does not store cardholder data. 3.7.7 - Not applicable. US Signal is a colocation, cloud service and managed service provider that

	does not have access to cardholder data and does not store cardholder data. 3.7.8 - Not applicable. US Signal is a colocation, cloud service and managed service provider that does not have access to cardholder data and does not store cardholder data. 3.7.9 - Not applicable. US Signal is a colocation, cloud service and managed service provider that does not have access to cardholder data and does not store cardholder data. 4.1.1 - Not applicable. US Signal offers hosting and managed services to its customers, which customers may use to store, process or transmit CHD. US Signal's customers are responsible for the security of the CHD they store, process or transmit. 4.1.2 - Not applicable. US Signal offers hosting and managed services to its customers, which customers may use to store, process or transmit CHD. US Signal's customers are responsible for the security of the CHD they store, process or transmit. 4.2.1 - Not applicable. US Signal offers hosting and managed services to its customers, which customers may use to store, process or transmit CHD. US Signal's customers are responsible for the security of the CHD they store, process or transmit. 4.2.1.1 - Not applicable. US Signal offers hosting and managed services to its customers, which customers may use to store, process or transmit CHD. US Signal's customers are responsible for the security of the CHD they store, process or transmit. 4.2.1.2 - Not applicable. US Signal offers hosting and managed services to its customers, which customers may use to store, process or transmit CHD. US Signal's customers are responsible for the security of the CHD they store, process or transmit. 4.2.2 - Not applicable. US Signal offers hosting and managed services to its customers, which customers may use to store, process or transmit CHD. US Signal's customers are responsible for the security of the CHD they store, process or transmit. 5.2.3 - Not applicable. Per interview discussion, there are no systems considered out of scope for malicious software. In-scope systems are currently running anti-virus and endpoint protection software. 5.2.3.1 - Not applicable. This requirement is a best practice until March 31, 2025. 5.3.2.1 - Not applicable. This requirement is a best practice until March 31, 2025. 5.3.3 - Not applicable. This requirement is a best practice until March 31, 2025. 5.4.1 - Not applicable. This requirement is a best practice until March 31, 2025. 6.2.1 - Not applicable. US Signal does not perform application or software development. 6.2.2 - Not applicable. US Signal does not perform application or software development.

	6.2.3 - Not applicable. US Signal does not perform application or software development. 6.2.3.1 - Not applicable. US Signal does not perform application or software development. 6.2.4 - Not applicable. US Signal does not perform application or software development. 6.3.2 - Not applicable. This requirement is a best practice until March 31, 2025. 6.4.1 - Not applicable. US Signal does not have in-scope, public facing web applications. 6.4.2 - Not applicable. This requirement is a best practice until March 31, 2025. 6.4.3 - Not applicable. This requirement is a best practice until March 31, 2025. 6.5.2 - Not applicable. No significant changes occurred in the past year. 6.5.3 - Not applicable. US Signal does not perform application or software development. 6.5.4 - Not applicable. US Signal does not perform application or software development. 6.5.5 - Not applicable. US Signal does not perform application or software development. 6.5.6 - Not applicable. US Signal does not perform application or software development. 7.2.5 - Not applicable. This requirement is a best practice until March 31, 2025. 7.2.5.1 - Not applicable. This requirement is a best practice until March 31, 2025. 7.2.6 - Not applicable. US Signal does not store cardholder data. 8.2.2 - Not applicable. Observed documented policies, user listings, and conducted interview discussions to determine that group, shared, generic accounts, or other shared authentication credentials are not in use and not allowed. 8.2.3 - Not applicable. Observed documented policies and conducted interview discussions, which determined US Signal does not have remote access to customer premises. 8.2.7 - Not applicable. Conducted interview discussions and observed documented policies and user listings to determine that there are no third-party accounts with remote access to the CDE and determined third-party accounts are disabled. 8.3.10 - Not applicable. Through interview discussions, determined that there are no customer user accounts with access to cardholder data. 8.3.10.1 - Not applicable. Through interview discussions, determined that there are no customer user accounts with access to cardholder data. 8.5.1 - Not applicable. This requirement is a best practice until March 31, 2025. 8.6.1 - Not applicable. This requirement is a best practice until March 31, 2025.

	8.6.2 - Not applicable. This requirement is a best practice until March 31, 2025. 8.6.3 - Not applicable. This requirement is a best practice until March 31, 2025. 9.2.2 - Not applicable. There are no publicly accessible network jacks. 9.2.4 - Not applicable. US Signal does not process, store, or transmit cardholder data. 9.4.1 - Not applicable. US Signal does not process, store, or transmit cardholder data. 9.4.1 - Not applicable. US Signal does not process, store, or transmit cardholder data. 9.4.1.2 - Not applicable. US Signal does not process, store, or transmit cardholder data. 9.4.2 - Not applicable. US Signal does not store, process, or transmit cardholder data as part of its business, therefore no data is stored on removable media. 9.4.3 - Not applicable. US Signal does not store, process, or transmit cardholder data as part of its business, therefore no data is stored on removable media. 9.4.4 - Not applicable. US Signal does not store, process, or transmit cardholder data as part of its business, therefore no data is stored on removable media. 9.4.5 - Not applicable. US Signal does not store, process, or transmit cardholder data as part of its business, therefore no data is stored on removable media. 9.4.5.1 - Not applicable. US Signal does not store, process, or transmit cardholder data as part of its business, therefore no data is stored on removable media. 9.4.6 - Not applicable. Cardholder data is not stored on US Signal's systems. Cardholder data is not backed up to tape and is not on removable electronic media, paper receipts, paper reports, or faxes. 9.4.7 - Not applicable. Cardholder data is not stored on US Signal's systems. Cardholder data is not backed up to tape and is not on removable electronic media, paper receipts, paper reports, or faxes. 9.5.1 - Not applicable. US Signal does not have a store front or accept card-present transactions resulting in POI devices at the US Signal facilities. 9.5.1.1 - Not applicable. US Signal does not have a store front or accept card-present transactions resulting in POI devices at the US Signal facilities. 9.5.1.2 - Not applicable. US Signal does not have a store front or accept card-present transactions resulting in POI devices at the US Signal facilities. 9.5.1.2.1 - Not applicable. This requirement is a best practice until March 31, 2025. 9.5.1.3 - Not applicable. US Signal does not have a store front or accept card-present transactions resulting in POI devices at the US Signal facilities.

	10.2.1.1 - Not applicable. Cardholder data is not stored by US Signal. Individuals have no access to cardholder data. 10.3.4 - Not applicable. Conducted INT-02 and observed the Rapid7 platform to determine that logs on the Rapid7 platform cannot be modified or deleted and thus, file integrity monitoring or change-detection mechanisms are unnecessary. 10.4.1.1 - Not applicable. This requirement is a best practice until March 31, 2025. 10.4.2.1 - Not applicable. This requirement is a best practice until March 31, 2025. 10.7.2 - Not applicable. This requirement is a best practice until March 31, 2025. 11.3.1.1 - Not applicable. This requirement is a best practice until March 31, 2025. 11.3.1.2 - Not applicable. This requirement is a best practice until March 31, 2025. 11.3.1.3 - Not applicable. This requirement is a best practice until March 31, 2025. 11.3.2.1 - Not applicable. Conducted interview discussions and observed change control documentation to determine that there were no significant changes within the past 12 months. 11.4.7 - Not applicable. US Signal is not a multi-tenant service provider. 11.5.1.1 - Not applicable. This requirement is a best practice until March 31, 2025. 11.6.1 - Not applicable. This requirement is a best practice until March 31, 2025. 12.3.1 - Not applicable. This requirement is a best practice until March 31, 2025. 12.3.2 - Not applicable. The entity is not using a customized approach. 12.3.3 - Not applicable. This requirement is a best practice until March 31, 2025. 12.3.4 - Not applicable. This requirement is a best practice until March 31, 2025. 12.5.2.1 - Not applicable. This requirement is a best practice until March 31, 2025. 12.5.3 - Not applicable. This requirement is a best practice until March 31, 2025. 12.6.2 - Not applicable. This requirement is a best practice until March 31, 2025. 12.6.3.1 - Not applicable. This requirement is a best practice until March 31, 2025. 12.6.3.2 - Not applicable. This requirement is a best practice until March 31, 2025. 12.8.1 - Not applicable. US Signal does not use third-party service providers or vendors with regard to its PCI DSS requirements. 12.8.2 - Not applicable. US Signal does not use third-party service providers or vendors with regard to its PCI DSS requirements.

	12.8.4 - Not applicable. US Signal does not use third-party service providers or vendors with regard to its PCI DSS requirements. 12.8.5 - Not applicable. US Signal does not use third-party service providers or vendors with regard to its PCI DSS requirements. 12.9.2 - Not applicable. US Signal does not use third-party service providers or vendors with regard to its PCI DSS requirements. 12.10.4.1 - Not applicable. This requirement is a best practice until March 31, 2025. 12.10.7 - Not applicable. This requirement is a best practice until March 31, 2025. A1.1.1 - Not applicable. US Signal is not a multi-tenant service provider. A1.1.2 - Not applicable. US Signal is not a multi-tenant service provider. A1.1.3 - Not applicable. US Signal is not a multi-tenant service provider. A1.1.4 - Not applicable. US Signal is not a multi-tenant service provider. A1.2.1 - Not applicable. US Signal is not a multi-tenant service provider. A1.2.2 - Not applicable. US Signal is not a multi-tenant service provider. A1.2.3 - Not applicable. US Signal is not a multi-tenant service provider. A2.1.1 - Not applicable. US Signal does not use card-present POS POI terminals. A2.1.2 - Not applicable. US Signal does not use card-present POS POI terminals. A2.1.3 - Not applicable. US Signal does not use card-present POS POI terminals.
For any Not Tested responses, identify which sub-requirements were not tested and the reason.	Not applicable.

Section 2 Report on Compliance

(**ROC Sections 1.2 and 1.3.2**)

Date Assessment began: ***Note:*** *This is the first date that evidence was gathered, or observations were made.*			May 6, 2024
Date Assessment ended: ***Note:*** *This is the last date that evidence was gathered, or observations were made.*			July 30, 2024
Were any requirements in the ROC unable to be met due to a legal constraint?			☐ Yes ☒ No
Were any testing activities performed remotely? If yes, for each testing activity below, indicate whether remote assessment activities were performed:			☒ Yes ☐ No
• Examine documentation	☒ Yes	☐ No	
• Interview personnel	☒ Yes	☐ No	
• Examine/observe live data	☒ Yes	☐ No	
• Observe process being performed	☒ Yes	☐ No	
• Observe physical environment	☒ Yes	☐ No	
• Interactive testing	☐ Yes	☒ No	
• Other:	☐ Yes	☒ No	

Section 3 Validation and Attestation Details

Part 3. PCI DSS Validation (ROC Section 1.7)

This AOC is based on results noted in the ROC dated July 30, 2024.

Indicate below whether a full or partial PCI DSS assessment was completed:

☒ **Full Assessment** – All requirements have been assessed and therefore no requirements were marked as Not Tested in the ROC.

☐ **Partial Assessment** – One or more requirements have not been assessed and were therefore marked as Not Tested in the ROC. Any requirement not assessed is noted as Not Tested in Part 2g above.

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

☒	**Compliant:** All sections of the PCI DSS ROC are complete, and all assessed requirements are marked as being either In Place or Not Applicable, resulting in an overall **COMPLIANT** rating; thereby US Signal Company, LLC has demonstrated compliance with all PCI DSS requirements except those noted as Not Tested above.
☐	**Non-Compliant:** Not all sections of the PCI DSS ROC are complete, or one or more requirements are marked as Not in Place, resulting in an overall **NON-COMPLIANT** rating; thereby *(Service Provider Company Name)* has not demonstrated compliance with PCI DSS requirements. **Target Date** for Compliance: *YYYY-MM-DD* An entity submitting this form with a Non-Compliant status may be required to complete the Action Plan in Part 4 of this document. Confirm with the entity to which this AOC will be submitted before completing Part 4.
☐	**Compliant but with Legal exception:** One or more assessed requirements in the ROC are marked as Not in Place due to a legal restriction that prevents the requirement from being met and all other assessed requirements are marked as being either In Place or Not Applicable, resulting in an overall **COMPLIANT BUT WITH LEGAL EXCEPTION** rating; thereby *(Service Provider Company Name)* has demonstrated compliance with all PCI DSS requirements except those noted as Not Tested above or as Not in Place due to a legal restriction. This option requires additional review from the entity to which this AOC will be submitted. *If selected, complete the following:*

Affected Requirement	Details of how legal constraint prevents requirement from being met

Part 3. PCI DSS Validation *(continued)*

Part 3a. Service Provider Acknowledgement

Signatory(s) confirms:
(Select all that apply)

☒	The ROC was completed according to *PCI DSS*, Version 4.0 and was completed according to the instructions therein.
☒	All information within the above-referenced ROC and in this attestation fairly represents the results of the Assessment in all material respects.
☒	PCI DSS controls will be maintained at all times, as applicable to the entity's environment.

Part 3b. Service Provider Attestation

DocuSigned by:
Trevor Bidle
ED1779A92BD84F1...

Signature of Service Provider Executive Officer ↑	Date: 7/30/2024
Service Provider Executive Officer Name: Trevor Bidle	Title: Chief Information Security Officer

Part 3c. Qualified Security Assessor (QSA) Acknowledgement

If a QSA was involved or assisted with this Assessment, indicate the role performed:	☒ QSA performed testing procedures.
	☒ QSA provided other assistance. If selected, describe all role(s) performed: QSA participated in interviews, observations, and status meeting, provided oversight to staff and feedback to US Signal regarding test results for the PCI DSS requirements.

DocuSigned by:
Brian Hill
955740C0E18A43F...

Signature of Lead QSA ↑	Date: 7/30/2024
Lead QSA Name: Brian Hill	

DocuSigned by:
Greg Schu
1D0CADC8B6AE45B...

Signature of Duly Authorized Officer of QSA Company ↑	Date: 7/30/2024
Duly Authorized Officer Name: Greg Schu	QSA Company:

Part 3d. PCI SSC Internal Security Assessor (ISA) Involvement

If an ISA(s) was involved or assisted with this Assessment, indicate the role performed:	☐ ISA(s) performed testing procedures.
	☐ ISA(s) provided other assistance. If selected, describe all role(s) performed:

Part 4. Action Plan for Non-Compliant Requirements

Only complete Part 4 upon request of the entity to which this AOC will be submitted, and only if the Assessment has Non-Compliant results noted in Section 3.

If asked to complete this section, select the appropriate response for "Compliant to PCI DSS Requirements" for each requirement below. For any "No" responses, include the date the entity expects to be compliant with the requirement and provide a brief description of the actions being taken to meet the requirement.

PCI DSS Requirement	Description of Requirement	Compliant to PCI DSS Requirements (Select One)		Remediation Date and Actions (If "NO" selected for any Requirement)
		YES	NO	
1	Install and maintain network security controls	☐	☐	
2	Apply secure configurations to all system components	☐	☐	
3	Protect stored account data	☐	☐	
4	Protect cardholder data with strong cryptography during transmission over open, public networks	☐	☐	
5	Protect all systems and networks from malicious software	☐	☐	
6	Develop and maintain secure systems and software	☐	☐	
7	Restrict access to system components and cardholder data by business need to know	☐	☐	
8	Identify users and authenticate access to system components	☐	☐	
9	Restrict physical access to cardholder data	☐	☐	
10	Log and monitor all access to system components and cardholder data	☐	☐	
11	Test security systems and networks regularly	☐	☐	
12	Support information security with organizational policies and programs	☐	☐	
Appendix A1	Additional PCI DSS Requirements for Multi-Tenant Service Providers	☐	☐	
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections	☐	☐