MDTA - TransCore Consolidated List
IT PBC (Prepared by Client) List
For the Audit Period 7/1/XXXX to June 30, XXXX

Item #	Description	SOC 1 CO#	SOC 2 CC#	Date Requested	Received	Notes
Policies and Procedures						
P1.1	CSR check reconciliation procedures, if changed from last year	CO2				
P1.2	Refund processing procedures	CO2				
P1.3	Accounting Reconciliation Procedures	CO3				
P1.4	The Security Awareness Training Program policy	CO8				
P1.5	Documented Change Management Policy	CO9	CC8			
P1.6	Job descriptions for all key roles in the organization		CC1			
P1.7	A copy of the Ops Plan		CC7			
P1.8	Maintenance Plan		Avl			
P1.9	Data Retention and Disposal Policy		CC6			
P1.10	Data Classification Policy		CC2			
P1.11	Incident Response Plan		CC4			
P1.12	Security Plan		CC4			
P1.13	Backup and Recovery Plan		CC7			
P1.14	Configuration Management Plan		CC8			
DriveEzMD Account Establishment (CO 1)						
1.1	A list of new private and business accounts for the audit period	CO1				
1.2	Support for a smaple of new accounts, selected from 2.1 above, showing that all of the required information was cptured.	CO1				
1.3	Screen print illustrating the error message displayed upon entry of a duplicate license plate number	CO1				
1.4	A list of the QA audits performed for the audit period	CO1				
1.5	Support for a sample of QA audits selected from 2.5 showing the QA audits were performed	CO1				
E-ZPass Customer Service and Account Maintenance (CO 2)						
2.1	A list of a customer check payments for the audit period	CO2				
2.2	Support for a sample of check payments select from 3.1 above showing that they were applied to the customer's account	CO2				
2.3	A list of account replenishment transactions for MONTH, YEAR	CO2				
2.4	Support for a sample of account replenishments selected from 3.3 above showing that the customer accounts were appropriately replenished based on the replenishment rules.	CO2				
2.5	System generated listing of refunds and closures during the audit period	CO2				
2.6	Support for the sample of refunds selected from 3.5 showing that the refund was generated and applied to the customer's account.	CO2				
2.7	The check reconciliation of MDTA refunds with the customer's accounts for the weeks of (weeks selected).	CO2				
2.8	Support for a sample of Mailroom Reconcilitions showing supervisor verifies all incoming check payments. **See Day Selection tab for a list of dates selected.**	CO2				
E-ZPass Financial Operations (CO 3)						
	The following reconciliations for the weeks of (weeks selected).					
3.1	Bank deposits Receipt and processing of cash and checks ACH and credit card transactions	CO3				
3.2	Support showing the reconciliations are reviewed on a daily basis for the weeks of (weeks selected).	CO3				
3.3	Support shonwing that the monthly reconciliations were prepared for the months of MONTH, YEAR and MONTH, YEAR.	CO3				
E-ZPass Reciprocity (CO 4)						
4.1	Support for the reconciliation of the transactions on the dailyTransaction Reconciliation, Correction Reconciliation, and Disputed Tolls files are reconciled to the IAG Reconciliation Spreadsheet for the months of (list of months/years)	CO4				
4.2	Support to show the Transaction and Transaction Check files for transmission to each of the IAG members were generated and a Transaction Acknowledgment was received for the months of (list of months, years).	CO4				
4.3	Support to show the Transaction Acknowledgments were generated to acknowledge the Transaction and Transaction Check files received from each of the IAG members for the months of (list of months, years).	CO4				
4.4	Support showing credit card transaction fees listed in the daily Transaction Reconciliation and Correction Reconciliation files are reconciled by the accounting supervisor to other IAG member credit card calculations using the IAG Credit Card Equity Calculations Spreadsheet for Q2 and Q3 of the audit period .	CO4				
4.5	Support showing the IAG Credit Card Equity Calculations Spreadsheet is shared with MDTA for Q2 and Q3 of the audit period.	CO4				
Transponder Inventory Reconciliation (CO 5)						
5.1	Support showing that one transponder type a week is randomly tested to verify that the transponders are located at the CIC facility and locked in the Transponder room. **See Week Selection tab for a list of weeks selected.**	CO5				
5.2	Support showing a Retailer Transponder Fulfillment Orders file is generated to track all On The Go transponders being shipped out to retailers. **See Week Selection tab for a list of weeks selected.**	CO5				
5.3	Support showing a Transponder Distribution file is generated to confirm all transponders processed are assigned to customer accounts. **See Week Selection tab for a list of weeks selected.**	CO5				
5.4	Support showing that transponder room is physically counted and reconciled Integrity application. **See Week Selection tab for a list of weeks selected.**	CO5				

Unregistered Account Invoicing and Reconciliation (CO 6)

6.1	A list of toll transactions received from the lanes for all vehicles for (date).	CO6	
6.2	Support for samples selected from 7.1 above to show that the toll transactions are posted to the customer's account for customers that have an EZ Pass account.	CO6	
6.3	Support for samples selected from 7.1 above to show that a NOTD is generated for each toll transaction associated with unregistered customer accounts.	CO6	
6.4	Support showing that the status of NOTD's are automatically escalated if there is an outstanding balance.	CO6	
6.5	Support showing that a civil penalty fee is assessed on NOTD's with an outstanding balance based on its age.	CO6	
6.6	Support showing the Host Reconciliation Summary Report is compared and reconciled to a report provided by the Toll Host. Any variances are communicated by email to the Toll Host. **See Day Selection tab for a list of weeks selected.**	CO6	

Physical Access to Integrity Systems and Data (CO 7, CC 6)

7.1	A list of users with access to the EOF data center, their job titles, and the reason for their access.	CO7	
7.2	Support showing that the list of employees is sent to MDTA and reviewd for Q2 and Q3 of the audit period.	CO7	
7.3	On-site walkthrough to verify that key fob access is required to the Middle River, Maryland location.	CO7	
7.4	Support to show that the latest review of the employes with access to the Middle River and Union, NJ offices was performed.	CO7	
7.5	The forms sent to MDTA to grant access to the Beltsville Data Center (EOF) for the TransCore employees that have badge access		CC6

Logical Access to Integrity Programs and Data (CO 8, CC1, CC 6)

8.1	Print screens of the network and Integrity application password policy.	CO8	
8.2	Support for the latest management review of user access	CO8	
8.3	A list of users with administrator access to the SQL database, their job titles, and the reason for their access	CO8	
8.4	A list of TransCore new hires for the audit period.	CO8	
8.5	Support for a sample of new and existing, selected from 9.4 above, users to show that they received computer security training and have acknowledged corporate policies.		CC1
8.6	Support for a sample of new hires, selected from 9.4 above, to show that they have signed necessary confidentiality agreements and have acknowledged their job descriptions at the time of onboarding.		CC1
8.7	The Information Security Forms for a sample of new hires selected from 9.4.	CO8	
8.8	Support for a sample of new hires, selected from 9.4 above, to show that a background check was performed		CC1
8.9	A list of terminated TransCore employees for the audit period.	CO8	
8.10	For a sample of terminated users, selected from 8.9 above, ISSA forms filled out for termination.		CC6
8.11	Support showing that access to the applications, networks, and servers were disabled and the date of the last sign on by the user.	CO8	
8.12	For a sample of terminated users, selected from 8.9 above, support for the latest quarterly management review of Integrity application access permissions, including segregation of duties.	CO8	CC6
8.13	A list of users with administrator access to the Integrity application, their job titles, and the reason for their access	CO8	
8.14	A list of all users including their system roles and user ID's		CC1/CC6
8.15	Support for a sample of users, selected from 8.14 above, to show that their roles are appropriate based on their job titles.		CC1
8.16	Support for a sample of users, selected from 8.14 above, to show that they received Code of Conduct training for the audit period.		CC1
8.17	Support for a sample of users, selected from 8.14 above, to show that received their annual evaluation		CC1
8.18	A list of users with administrator access to the servers hosting the Integrity application, their job titles, and the reason for their access.	CO8	

Integrity System Program Changes (CO 9, CC 6, CC 8)

9.1	A list of changes made to the Integrity application for the audit period.	CO9	
9.2	Support for a sample of changes selected from 9.2 to show that the changes were made in compliance with the Change Management Policy, including release notes.	CO9	CC8
9.3	A list of users authorized to promote changes to production	CO9	CC6

Integrity Computer Operations (CO 10)

10.1	A list of users with access to the SQL job scheduler, their job titles, and reason for their access.	C10
10.2	Support/print screens showing that the job scheduler is configured to email IT administrators regarding job aborts and errors.	C10
10.3	Support/print screens/logs showing Integreity was backed up via Veeam on a continual basis for the week of (date).	C10
10.4	A list of changes made to the job scheduler and support showing they were appropriately approved by the project manager.	C10
10.5	Support of the last back up restoration test	C10

Integrity backup jobs (CO 11)

11.1	Support showing that the backup of critical data, server configuration settings, and system states is configured to be performed daily	C11
11.2	Support showing that the database and network configuration are backed up and replicated to the DR location on a daily basis for the week of (date).	C11

Common Core

Control Environment (CC 1)

CC1.1	Support showing that quarterly leadership meetings are held for the most recent meeting for the audit period.	CC1
CC1.2	Support for the most recent phishing test for the period for the audit period.	CC1
CC1.3	Org chart	CC1
CC1.4	Monthly reports showing the call center metrics for each month of the audit period	CC1

Communication and Information (CC 2)

CC2.1	The most recent inventory of production information assets for the period for the audit period.	CC2
CC2.2	Screen print of the dash board used to monitor risks.	CC2
CC2.3	Sample vendor agreement which acknowledges their compliance on security and confidentiality commitments. (Dial America)	CC2

Risk Assessment (CC 3)

CC3.1	Project risk assessment	CC3
CC3.2	Sample of company wide email notification sent for procedural changes	CC3
CC3.3	Support showing that a penetration test was performed for the audit period.	CC3
CC3.4	The results of the Nessus vulnerability scans for (months).	CC3

Monitoring Activities (CC 4)

CC4.1	Sample email notification of functionality change (Release Notes, Desk Drops).	CC4
CC4.2	Screen shot of solar winds showing monitoring of capacity and system performance	CC4
CC4.3	Screenshot showing that all log in attempts are reviewed as a part of the daily checklist	CC4
CC4.4	Support showing that the leadership team meets on a quarterly basis to discuss operations, issues relating to internal controls and information security (this can be entries in a calendar application).	CC4
CC4.5	A last of incidents that occurred for the audit period.	CC4
CC4.6	For a sample of incidents selected from 16.5 above, support showing that the incident was tracked to resolution	CC4

Control Activities (CC 5)

CC5.1	IT Checklists used in conjunction with the intrusion detection systems	CC 5

Logical and Physical Access Controls (CC 6)

CC6.1	Support showing that remote access is secured by an encrypted VPN (GlobalProtect VPN client) or remote desktop application (screen shots are fine)	CC6
CC6.2	A list of workstations that were disposed of for the audit period.	CC6
CC6.3	Network Diagram with all IP addresses redacted	CC6
CC6.4	Support showing use of encryption to send sensitive information to third parties	CC6
CC6.5	Support showing that automated alerts are generated if errors are generated on any outbound data interfaces and the resulting documentation generated for those errors.	CC6
CC6.6	Support showing anti-virus software is in place	CC6

System Operations (CC 7)

CC7.1	Support for the disaster recovery test run for the audit period.	CC7

Change Management (CC 8)

CC8.1	None (see above)	

Risk Mitigation (CC 9)

CC9.1	A list of vendors and contractors who have access to the network and applications for the audit period.	CC9
CC9.2	For a sample of the vendors/contractors selected from 21.1, support showing vendor and contractor access to the network and applications is approved.	CC9

Additional Criteria
Availability (AVL)

AVL1.1	Support showing capacity management tools are in place and operational	AVL
AVL1.2	Release notes for storage expansion, changes, and/or forcasts sent to MDTA for the audit period.	AVL
AVL1.3	Support showing detection measures are in place to identify environmental threat events	AVL

Processing Integrity (PI)

PI1.1	Support showing that SFTP and other secure methods are used when receiving data from third parties	PI

Confidentiality (CON)

24.1	None	