DRAFT

Contracts Audit
January 2011 Recommendations
Status of Recommendations

Internal Audit Observation	Internal Audit Recommendation	Management Response	Management Action Plan	Responsible Party	Due Date
7. Account Adjustment Approval Limits in TRIMS: Section IV B in the scope of services section of the ACS contract indicates that personal E-PASS account adjustments over $200 and commercial E-PASS account adjustments in excess of $500 must be approved by an ACS manager in TRIMS. Currently, TRIMS is not configured to prevent the approval of adjustments to personal E-PASS accounts in excess of $200 by CSC Supervisors. Internal Audit obtained all adjustments processed in TRIMS between August 1, 2009 and September 30, 2010 and noted that 93 of 140 adjustments to private accounts between $200 and $500 were approved in TRIMS by CSC Supervisors instead of a manager, as required. As a mitigating control, ACS indicated that all adjustments are reviewed by the Financial Analyst and Accounting Assistant, with the exception of voids, which should only be approved by CSC Managers in TRIMS. However, Internal Audit noted that 482 of 587 void adjustments were approved in TRIMS by CSC Supervisors. Furthermore, a CSC Manager or CSC Supervisor enters their PIN in TRIMS to approve adjustments; however, PINs are never changed which may result in the sharing of PINs between employees. Data analytics were performed related to the approval of adjustments in excess of $200 to personal E-PASS accounts and $500 to commercial E-PASS accounts and no adjustments were identified for additional follow-up; however, the strengthening of the controls related to the review and approval of adjustments in TRIMS may reduce the risk of fraud.	The Authority should utilize CSC Manager and CSC Supervisor passwords, rather than PINs, to approve adjustment transactions in TRIMS (passwords are required to be changed on a regular basis by the system).	The Authority concurs that moving to a password based approval is in its best interest. However, the change to a password based approval key would be a fairly significant change to the existing system. The current system is currently being reviewed for replacement as part of the Toll System Replacement (TSR) project. Making these changes now may be waste of valuable IT resources if the current system were to be disposed of in the near term. Based on the outcome of the TSR project the Authority would make this change as a part of a newly procured system or would be developed and implemented in the existing system once it was determined that we would be retaining the existing system.	Toll Operations will require passwords to be used for approvals in any new toll collection software procured by the Authority or its existing software if it is retained and that the password be changed on a regular basis by the system.	Rene Rodrigue, Director of IT David Wynne, Director of Toll Operations	Original: 12/31/13 Revised: 12/31/15 Revised: 3/31/16

DRAFT

Toll Violations Audit
March 2012 Recommendations
Status of Recommendations

Internal Audit Observation	Internal Audit Recommendation	Management Response	Management Action Plan	Responsible Party	Due Date
6. Process Improvement: There is no process to pursue collections for habitually delinquent toll violators that exceed a certain number of transactions or a certain dollar threshold. Enhancing collection efforts could increase collection rates and associated revenue.	Management should determine if it is cost beneficial and within the business objectives of the Authority to turn over delinquent violators to a collection agency. The Authority should consider if the UTC is outstanding with the court. Additionally, the Authority should implement a policy containing a time and dollar threshold of how long a UTN or UTC violator should be outstanding before the Authority pursues collections, as well as, a dollar amount the UTN or UTC must reach prior to sending it to collections.	Concur	Director of Toll Operations will facilitate a review of potential revenue to be collected, possible collection rates, industry practices, legal ramifications and consideration of community perception.	David Wynne, Director of Toll Operations	Original: 1/1/13 Revised: 3/31/13 Revised: 1/1/14 Revised: 12/31/15

DRAFT

Toll Revenue Audit
March 2013 Recommendations
Status of Recommendations

Internal Audit Observation	Internal Audit Recommendation	Management Response	Management Action Plan	Responsible Party	Due Date
6. Potential Revenue Leakage: The potential extrapolated discrepancies in the toll collections audit highlighted above total approximately $1,000 for the six month period ended December 2012. A root cause of this appears to be the manual nature of the Attendant's Shift Record used as a reconciling item during toll collections audits, for which third party contractor auditors are required to make assumptions as to what is being communicated by the TSA. Additionally, during the review of the toll collections audit , Internal Audit found that system purges and reverse run through transactions, system functions used to reset the toll lane if the lane server is out of sync, generates an expected revenue amount . Also the description on the Unusual Occurrence report for these transactions have the same overclass description as small vehicle transactions that do not engage the toll lane treadles. The third party contractor uses the Unusual Occurrence report to reduce the expected revenue for the system purges and reverse run through transactions, while maintaining the expected revenue related to the smaller vehicles that do not engage the treadles . Internal Audit performed a review of the overclass transactions (excluding purges, re-syncs, and reverse run throughs) and found that the third party contractor reversed the expected revenue inappropriately in 4 out of 25 transactions tested, an error rate of 13%. The potential extrapolated variance when applied to all overclass transactions for the six month period ended December 31, 2012 is estimated to be approximately $700.	6. b) The Authority should also consider automating certain aspects of the Attendant's Shift Record log by integrating the unusual occurrence, violations, and insufficient fund transactions within the MLT system. This would reduce the subjectivity of the FTS auditor's interpretation of the manual ASR log.	Concur	The Authority currently has this recommendation as a function in the planned Toll System Replacement project that is currently ongoing at this time. The Authority would expect to have the new system in place and operating by July 1, 2015.	David Wynne, Director of Toll Operations	Original: 7/1/15 Revised: 4/30/16 Revised: 12/31/17

DRAFT

Intelligent Transportation Systems Security Review
February 2015 Recommendations
Status of Recommendations

Internal Audit Observation	Internal Audit Recommendation	Management Response	Responsible Party	Due Date
1. Generic Key Access to Roadside Cabinets: A common key is used to lock the roadside cabinets that house ITS network equipment. There are over 300 roadside cabinets in the ITS environment, each containing computer equipment that supports the digital message boards, cameras, RFID readers and other ITS roadside equipment. These cabinets are accessed by ITS contractors and ITS staff to install, troubleshoot, and repair issues on the ITS network. This common key (termed "universal #2 key") used to lock the ITS roadside cabinets is also used by FDOT, CalTrans, and other state organizations. Potentially unauthorized access could be gained to the roadside cabinets because of the wide usage of the universal #2 keys that are used to lock them. Additionally, once these cabinets are unlocked, the computer equipment that supports the digital message boards and RFID readers can be accessed, as well as the rest of the ITS internal network. This, coupled with the risk described in Observation #2 of this report, could allow unwanted changes to the message boards that project travel times, and could allow Denial of Service attacks on the traffic pattern equipment in the environment. Also, because the universal #2 key is not assigned to a single person (but is given to anyone who needs to perform work on equipment in the cabinets), administrators may not be able to assign accountability to the person opening a roadside cabinet. Additionally, ITS cannot grant access to specific cabinets based on the work that is to be performed. This does not follow the principle of least privilege, in which a person is granted access to only those systems required based on their job duties.	Review the feasibility of deploying a stronger access control tool to the ITS network cabinets so only authorized personnel (ITS staff or ITS contractors) can access them. This tool should allow ITS to grant access to only those cabinets necessary (not all cabinets in the environment), and should be unique to the ITS environment.	Though ITS is not aware of unauthorized access occurring, we recognize the risk of utilizing a generic key. ITS will develop a plan to implement a five year project to address the risk of unauthorized access to the cabinets due to the use of a generic key. Update July 21, 2015: Cyberlock will be installed as part of project 599-525. Estimated completion date is December 31, 2016.	Corey Quinn	12/31/16

2. Default Credentials: The default user name and password are used on the digital message board controllers that give travelers an estimated time of arrival while travelling, as well as the RFID controllers that receive signals from E-pass or Sun-pass devices in traveler's vehicles. These passwords are quickly discoverable by analyzing vendor documentation or attempting commonly used defaults. Additionally, the default user name has the ability to modify configurations, add local users, view all data, or even disable those systems. The utilization of default credentials on both the digital message board controllers and the RFID controllers, coupled with the risk described in Observation #1 in this report, could allow an attacker to disable both the digital message boards and RFID controllers. This may not allow ITS to maintain its uptime requirements and may not allow ITS to give travelers accurate travel time estimates. A listing of these vulnerabilities has been provided to ITS in a separate document.	Change all current credentials which are default or easily guessable. Implement a requirement to change all vendor supplied credentials before moving a system to deployment as part of the ITS standard system build. Ensure that all passwords are changed at least every 90 days.	ITS will change the default credentials on the digital message board controllers where possible (the credentials are hard-coded in some models, and therefore cannot be changed). We will research the feasibility of changing these credentials every quarter, in addition to relying on our response outlined in Observation #1 (Devices that do not have remote password modification capabilities from the manufacturer must rely on the response outlined in Observation #1), and detective controls surrounding the cabinets. Update July 21, 2015: Where possible, RADIUS authentication technology will be used to subsume authentication under the normal CFX password requirements. Where RADIUS cannot be used due to functionality limitations, passwords will be rotated twice a year beginning November 2015.	Corey Quinn	11/30/15
4. Documented Policies and Procedures: Though ITS leverages CFX policies and procedures where possible, defined policies, procedures, and roles and responsibilities are not documented for operations specific to ITS, such as procedures for adding and removing user access and the incident response process. While there is very little change of users in the ITS environment, the process should be documented to prevent loss of knowledge should an ITS employee or long-term contractor leave the organization. Without strong governance over standard practices throughout the environment, current activities may not outline Management's current expectations.	Create a document for the ITS process to add and remove users, and document the ITS Incident Response Plan. Ensure all policies are reviewed at least annually to ensure each policy is still relevant.	ITS is currently creating a document outlining formalized security procedures to be implemented in the environment. The processes outline above will be included in this document. Additionally, ITS will work with CFX to determine a clear delineation of responsibility between the environments to ensure all processes at ITS, including those listed above, are formally documented. Update July 21, 2015: Development is complete, review to be completed by September 1, 2015.	Corey Quinn	9/1/15

6. Outdated Software: 44 applications utilized on 373 of the 1627 systems scanned have vulnerabilities that could lead to compromise due to missing patches or upgrades. The vulnerabilities in these applications could allow for denial of service attacks, arbitrary code execution, information disclosure, or authentication bypass. Each of these attacks affects the confidentiality, integrity or availability of the applications listed above, which may cause difficulties when conducting normal business operations or system and application maintenance. A listing of these vulnerabilities has been provided to ITS in a separate document.	Update these applications to the most recent version available from their vendors. Analyze their business use, and remove them should they be deemed unnecessary. Develop and deploy a formal vulnerability management process that includes periodic vulnerability scans to allow for the identification and application of all updates to systems which do not have the most recent patch level.	ITS will remove unnecessary applications, and then discuss the remaining outdated software with CFX IT to refine a process to keep these updated (currently, ITS systems do not have Internet access, and as such, updating these applications would require CFX's involvement and a manual process). Update July 21, 2015: Software update or removal will be completed by February 28, 2016.	Corey Quinn	2/28/16
7. Log Configuration: System and database logs within the ITS network are not secured, managed, correlated, or alerted upon. System, Application, and Security log configurations within the network remains at the default settings for systems, and are not moved off the system to a log aggregation tool. As a result, these logs will be lost after the default log size limit of 20 megabytes is reached, preventing ITS from performing investigative actions with these logs. Depending on the activity on the system, the default log size could be filled within a few days. Without centralizing, securing, correlating, and alerting upon all types of logs in the environment, unwanted, and potentially disruptive, actions may occur in the environment without management's knowledge. Logs which are not kept may limit ITS' ability to perform investigative actions.	Deploy a log aggregation tool to the environment and feed all logs into this tool so that they may be centralized, correlated and protected. Review these logs periodically to identify actions within the environment which are unwanted or unauthorized.	ITS will research the feasibility of including this functionality into the current logging system "What'sup Gold". Update July 21, 2015: Research complete. Implementation of Secure Information and Event Management solution pending upcoming organizational changes.	Corey Quinn	6/30/15

8. System Hardening: Procedures to enforce secure system configurations such as removing unnecessary services, disabling open shares, and other configuration weaknesses listed below have not been performed on 93 of the 1627 systems assessed during this project. System hardening is the process of identifying and remediating weaknesses in system configurations to prevent the possibility of compromise due to those weaknesses. The vulnerabilities in these configurations could allow for eavesdropping or impersonation attacks, information disclosure, or authentication bypass. Each of these attacks affects the confidentiality, integrity or availability of the applications listed above, potentially placing ITS' business processes and / or data at risk. A listing of these vulnerabilities has been provided to ITS in a separate document.	Define hardening procedures and incorporate them into a checklist format to be included in the current build guidelines for all systems. Modify the configuration settings on the above noted systems to ensure they are hardened against attack. The National Institute of Standards and Technologies (NIST) publication on server security is an industry standard regarding system hardening and can be found here: csrc.nist.gov/publications/nistpubs/800-123/SP800-123.pdf Implement a validation process within the current change control procedures to identify unauthorized modifications to systems in the environment to ensure that they remain configured as required by management. This validation process should be performed upon initial system build and at periodic intervals, and should not be performed by the employee who configured the changes to preserve the separation of duties principle.	ITS will research the feasibility of removing the functionality outlined above, and include system hardening in the "ITS security procedure" document. Update July 21, 2015: Reconfiguration or removal to be completed by March 31, 2016 pending upcoming organizational changes.	Corey Quinn	3/31/16
9. Insecure Services: The clear text protocols FTP (File Transfer Protocol), Telnet, and rlogin are utilized on 1131 of the 1627 systems scanned within the ITS environment. They require a user to enter a username and password for authentication to the remote system. This username and password and all other data are transferred between the client and server without encryption on the network. Since the username and password are unencrypted while on the network, there is a possibility that an unauthorized user could capture them for later use. Below are the number of systems running each service: • FTP (50 systems) • Telnet (1114 systems) • Rlogin (271 systems) A listing of the insecure services has been provided to ITS in a separate document.	Disable the services FTP, Telnet, and rlogin and use their secure alternatives SFTP (Secure File Transfer Protocol) and SSH (Secure Shell) 2.0. If disabling these services is not viable, consider applying compensating controls such as segmentation, Intrusion Prevention Systems, or Network Access Control technologies. Additionally, because Rlogin can be configured to allow users to login without providing a password, ITS and CFX should review the deployment of Rlogin on all systems in the environment to ensure that this service is not configured in this manner.	ITS will research the feasibility of removing the functionality outlined above, and include disabling insecure services in the "ITS security procedure" document (assuming this functionality is not needed). Update July 21, 2015: Research complete. Documented business justification for necessary clear text protocols will be added to the security manual, and the remaining items will be removed by April 30, 2016.	Corey Quinn	4/30/16

10. Default SNMP Strings: The default SNMP community string is utilized on 1538 of the 1627 systems scanned within the ITS network. SNMP utilizes community strings as a form of password to read and write to many types of network devices, appliances, switches, routers and firewalls. An attacker who is able to obtain either the SNMP read string or SNMP write string can view or modify the configuration of critical network devices. This could result in compromise of sensitive data through interception, modification of devices to allow additional malicious traffic through the network, or interruption of legitimate business processes. A listing of these vulnerabilities has been provided to ITS in a separate document.	Change the community strings of all devices within the network from the default values to avoid the possibility of unwanted information leakage or configuration changes. Additionally, disable legacy versions of SNMP (Versions 1 and 2), and utilize the current version of SNMP (Version 3).	ITS will develop a plan to modify the default SNMP strings in the environment. Update July 21, 2015: Research complete. Documented business justification for necessary SNMP strings will be added to the security manual, and the remaining items will be removed by July 31, 2016.	Corey Quinn	7/31/16
11. Dual-Factor Authentication: ITS users are not required to utilize dual-factor authentication for connecting remotely to the network. Dual-factor authentication within the environment is controlled by the CFX IT staff, and currently, only CFX employees are required to connect remotely using dual-factor authentication. Dual-factor authentication requires two (2) of these three (3) items to verify the identity of the user attempting to gain access to the network: • Something a user knows (a password) • Something a user has (a token) • Something a user is (biometrics) Without dual-factor authentication, the compromise of a password can potentially lead to the compromise of sensitive data due to the lack of an additional requirement to authenticate.	Leverage CFX dual-factor technology for all ITS contractors who need to connect to the ITS network remotely.	ITS will discuss adding contractors and those who need to connect to the ITS environment through the CFX technology with the CFX IT group. Update July 21, 2015: ITS will deploy trial with Atkins personnel to test the impact to personnel responsible for provisioning accounts by August 31, 2015.	Corey Quinn	8/31/15
12. SSL Weaknesses: The Secure Sockets Layer (SSL) deployment within the ITS environment has multiple weaknesses. There are 5559 related SSL vulnerabilities across 813 of the 1627 systems scanned within the environment. A full listing of the vulnerabilities has been provided in a separate document. Each of these vulnerabilities can allow for a man-in-the-middle attack, potentially leading to compromise of systems and data.	Test configurations changes for upgrading to TLS 1.2, deploying strong cipher suites, disabling SSL renegotiation and disabling compression. Should these configuration changes be successful without causing business disruption, deploy these changes to the environment. Generate new certificates for those that are self-signed, expired, have the wrong hostname, or have weak hashing algorithms.	ITS will research the feasibility of removing the functionality outlined above (assuming this functionality is not needed), and move to TLS 1.2 (if supported by ITS systems). Update July 21, 2015: SSL solution dependent on pending organizational changes.	Corey Quinn	10/31/15

13. Web Server Configuration Weaknesses: Two (2) web servers of the 1627 systems scanned within the environment has HTTP Trace and Track methods enabled. These features are installed to assist developers in debugging web page programming and are not necessary on production servers. A listing of these web servers has been provided in a separate document. Servers supporting this method are subject to cross-site-scripting attacks, dubbed XST for 'Cross-Site-Tracing', when used in conjunction with various weaknesses in browsers. Although difficult to exploit, an unauthorized user may use this flaw to trick legitimate web users into giving them their credentials. Security vulnerabilities are often identified in unnecessary server functionality that is enabled.	The Trace / Track method should be disabled or disallowed on identified web servers. Additionally, the PUT and/or DELETE method should be disabled or disallowed on identified web servers. ITS and CFX should also consider applying the principle of least privileges to these servers and remove all unnecessary HTTP Methods, unless there is a business critical need.	The system contractor (who administers this system) will be asked to research the feasibility of disabling this functionality when it is not being used, or find other functionality with less risk.	Corey Quinn	12/31/15

DRAFT

Back Office Customer Call Center Review
May 2015 Recommendations
Status of Recommendations

Internal Audit Observation	Internal Audit Recommendation	Management Response	Management Action Plan	Responsible Party	Due Date
The call center has a target Average speed of Answer (ASA) of 60 seconds. Currently the call center's ASA is approximately 128 seconds, which is consistent across all call types and skills. There are several factor that play a role in the prolonged ASAtimes. Call center agents spend approximately 50% of their time handling inbound calls while 30% of agent time is spent in various auxiliarystates, including After-Call-Work (ACW), which represents about 50% of agent auxiliary time on average. The Authority's Avaya AutomaticCall Distribution ("ACD") systemisprogrammed to provide an automatic 20secondsof ACW at the end of each call for the call center agent to complete servicing the call, make notation on the customer's account, etc. The industry average ACW is between 12-15 seconds. Based on the 400 calls observed, there is not a great deal of after-call work activity	The Authority should consider making changes to the call center agent scheduling to leverage part-time staff and improve agent utilization to increase agent availability and lower average speed of answer to the call center's target of 60 seconds. There are several inexpensive staffing tools that can be utilized to effectively manage the call center schedule, such as ccModeler. The Authority and third party vendor should also consider performing additional analysis into the factors that drive the ACW time to determine if the ACW time can be reduced in an effort to improve agent availability and improve the ASA. The analysis should include an evaluation of the actual time utilized to capture call servicing notations and other information after the call has ended, and evaluate the extent to which these activities are utilized to service customers or improve the efficiency of future calls.	Concur	The Authority will utilize the recommended ccModelerprogram to analyze the leverage call center resources more effectively and increase agent availability. The Authority will also adjust the After-Call-Work (ACW) timeto 15 seconds.	David Wynne, Director of Toll Operations, and Joann Chizlett, former Director of IT	6/30/15

Each inbound call to the call center routes the customer to the Intelligent Voice Response (“IVR”) system from which the customer selects service options from a prompt. The customer is then routed to the Vector Steps, which provides additional messaging and routes the call to an available call center agent. Within the IVR and Vector steps the following inconsistencies and duplicative information are delivered to the customer, which if corrected, could improve the overall customer call experience: 1.The call prompts utilize a mix of different male and female voices leading to an abrupt and inconsistent customer experience. 2.The inter-prompt and queue treatment consists of a mixed use of silence, ringing, messaging, and music while the customer is on-hold and as the customer transitions from one vector step to another. 3.E-PASS main menu has redundant options to “return to main menu” and “repeat options”. The menu also allows callers to opt out to a customer service representative using option “0” which may lead to prolonged call handling times. 4.Hours of operation and locations are given to callers even though the center is open. This information would normally only be presented after-hours. 5.The center does not leverage Estimated Wait Time (“EWT”) prompting to inform callers of wait times and potentially redirect callers to online servicing.	There are opportunities to improve the prompts and messaging delivered to customers contacting the Authority by improving prompt and call treatment consistency and attempting to direct more callers to online servicing. The Authority should consider the points above and conduct a thorough evaluation of vector programming and IVR prompting during the implementation of the centralized back office contact center IVR platform to ensure consistent treatment and the use of EWT to inform callers of high wait times and reinforce the use of online or other servicing options.	Concur	The Authority is in the process of procuring and implementing a new IVR system for E-PASS which will include back-up hardware, and the improvement recommendations will be taken to into account at that time. In addition, the Authority will provide the recommendations to the centralized back office contact center vendor for consideration during the development of any IVR technology, if the Authority were to agree to move forward with the centralized back office contact center.	Rene Rodrigue, Director of IT	6/30/16
The Avaya Phone system can provide reporting that would allow the Authority and the third party vendor to monitor the overall customer service experience and the effectiveness and efficiency of the call center operations. Currently, the Authority utilizes reports to assess the key metrics listed below. However, the Authority does not routinely monitor reporting that would give insight into the underlying factors that drive key metrics in order to achieve performance targets.	The Authority should use detailed reporting to more accurately measure and assess performance factors that drive key statistics. Internal Audit has partnered with the Authority to develop many of these reports as a part of this review. The Authority should use the reports to develop process improvements to improve the call center’s operations and achieve the performance targets. Specific reports that should be leveraged include agent attendance and agent aux reports.	Concur	The Authority will track daily, weekly and monthly service level data to assess and improve the performance targets. Service Level is currently set at 80% and will be modified accordingly.	David Wynne, Director of Toll Operations	6/1/15

Aligning call quality attributes to a standardized call flow process enables an organization to assess, measure and address specific behaviors that are aligned to call handling performance objectives, such as call handle time and use of ACW. The standard segments of a call flow include Greeting, Caller Identification, Caller Validation, Service identification, Service Delivery and Wrap up. The Authority's call center quality assurance program is aligned to measure quality in a generalized manner and is not aligned to a standardized call flow. The current call center quality assurance forms are made up of 29 Yes or No questions and 5 additional questions that are measured on a gradient of 1-3. The form does not include "automatic fail" questions/responses that would indicate the need for immediate re-training. As a leading quality assurance practice, all questions should be measured on a gradient whenever feasible. Aligning the quality form to a standardized call flow enables the use of gradients more easily because it allows the behaviors measured to be compared against a specific business process and related goals.	To improve the quality assurance process, the Authority should identify a standardized call flow for the types of calls handled by the call center and identify the specific behaviors and skills that should be measured within each segment of the call. This process would enhance the quality assurance process to allow for specific guidance to CSR's and align quality criteria to measurable business goals and objectives (e.g. reduction of call handle time).	Concur	The Authority will work with the third party call center vendor to revise the current quality assurance process to align with the call quality attributes to measure business objectives.	David Wynne, Director of Toll Operations	Original: 7/1/15 Revised: 11/30/15
While the messaging delivered to callers in both the IVR and Vector messaging reminds callers that unpaid toll notices can be paid online, the Authorities web presence could be improved to make the process of making payments online more intuitive. Links to unpaid toll payment options are not plainly visible and require additional navigation that we believe is deterring customers from utilizing the online service and instead placing calls into the center. In addition, throughout the course of the 400 call observations, there were only a handful of calls (fewer than 5) where the agent reminded the caller that purchasing a transponder or replenishing their account would allow them to avoid toll violations in the future. Also, the Authority's corporate phone number is often called when a customer is trying to contact the call center. These calls are received by the Authority's receptionist and transferred to the call center.	The Authority should consider launching an E-PASS product and services website, independent of the corporate website, that would focus on the customer experience and E-PASS activity. An E-PASS focused website would allow customers to navigate the site with ease and would help to deflect customer service activities, such as making unpaid toll notice payment and account replenishments, to the website. Also, call center agent training should also be considered to reinforce the importance of reminding customers to replenish their accounts and/or purchase a transponder in cases where an in-state customer is contacting the authority about a toll violation or citation. These improvements can deflect calls and reduce volume of calls received by the call center. The Authority should also consider adding prompts to the treatment provided on the main number to route callers to the call center in order to limit the number of call center calls received by the receptionist.	Concur	1.The Director of Toll Operation and IT will schedule a meeting with the CFX Communication Department to discuss the recommendations to the website and evaluate which recommendation can be implemented. 2.The call center scripts will be updated to include a reminder to customers to replenish and/or purchase a transponder at the end of each call. 3.The Authority will consider adding prompts to the treatment provided on the main number to route callers to the call center in order to limit the number of call center calls received by the receptionist.	1. David Wynne, Director of Toll Operations, and Joann Chizlett, former Director of IT 2. David Wynne, Director of Toll Operations 3. Joann Chizlett, former Director of IT	1. 8/1/15 2. Original: 6/1/15 Revised: 11/30/15 3. 8/1/15

The majority of calls handled by the Authority are payment related, including payment of Unpaid Pay Notices and Citations and account replenishment. During these calls, agents spend an average of 68 seconds identifying the caller and accessing their account. This represents approximately one-third of the total talk time of the call. A combination of call automation (attempting to identify the caller via the phone number that they are calling from) and agent training to obtain the information required to identify the customer and access their account as efficiently as possible could significantly reduce the handle time of calls.	The Authority should conduct further analysis to determine the percentage of inbound calling line ID's that can be linked to one or more existing accounts in the Authority's servicing applications. If this percentage is greater than 40-50%, this would indicate a substantial opportunity to automate inbound calls and thereby reduce overall handle times. In addition, the Authority should consider developing and conducting agent training to enable agents to take control of inbound calls and identify the information needed to access the caller's notifications, citations, and/or the caller's account as efficiently as possible.	Concur	1.Further analysis will be conducted to determine the percentage of inbound calls associated with active customer accounts. Based on results of the analysis, The Authority will determine if it is feasible to incorporate call automation based on strategic direction as it relates to the deployment and CFX involvement in centralized back office contact center. 2.The third party call center vendor will provide refresher training on "Call Control" and incorporate "Call Control" techniques into new agent training.	1. David Wynne, Director of Toll Operations, and Rene Rodrigue, Director of IT 2. David Wynne, Director of Toll Operations	1. Original: 7/1/15 Revised: 11/30/15 2. Original: 8/1/1/5 Revised: 11/30/15