DRAFT CONTINUITY PLAN

For the Conduct of the Automated Election System (AES)
In Connection with the May 9, 2016 National, Local and ARMM Regional Elections

I. **Contingency Procedures Applicable to the National/Central Canvass Service**

A. **The Data Storage is not available and there is Database Service Interruption.**	
	1. The Network Monitor System triggers an alarm related with the storage system, or
	2. The Database Server presents errors in the database log, or
	3. Application Servers (REIS or REIS Listener) presents DATABASE errors in the application log.
	4. Perform the following activities:
	4.1. Access the Database Server, and check kernel messages for access errors.
	4.2. Check System Logs messages for access errors.
	4.3. "Unmount" and "mount" the storage system.
	4.4. Check for warnings or error in the front panel of the storage system.
	4.5 Check power cable connection with the storage.
	4.6. Check SAS cables connections between servers and storage.
	5. If the result of the previous activities implies a failing storage system, then the Storage is marked with the status of "failing".
	Recovery:
	6. Notifies the Technology Manager of the System failure, and ask for authorization.
	7. Gives authorization for the execution of the recovery procedures.
	8. Block Firewall access to the server from the external network.

	9. Shutdown the database service in the first node (primary node).
	10. Check integrity and status of the database back-up in the standby server.
	11. If the back-up data files are corrupted or the status is incorrect, check for the contingency procedures for the Back-Up Center.
	12. If the back-up data files are correct:
	12.1. Restore the Database with the back-up files, start the database service in the secondary node, and execute the scripts for primary database transition.
	12.2. Check logs system messages in the database server and application servers.
	13. Notifies the Technology Manager that the system has been recovered.
	14. Gives authorization for firewall activation, and declares the end of the Recovery process.
	15. Open Firewall access to the server from the external network.
B. **There is Server Hardware Failure and Database Service Interruption.**	
	1. The Network Monitor System triggers an alarm related with the Database Server, or
	2. Application Servers (REIS or REIS Listener) presents DATABASE errors in the application log.
	3. The Back-up Server should execute the contingency procedures and scripts automatically:
	3.1. Check log messages in the database and application server.
	3.2. Check network connection.
	3.3. If the service is up and running, no further actions are required.

	4. If the secondary server doesn't start automatically, then the following steps are required:
	4.1. Check Database server network reachability.
	4.2. Check for warnings or error in the front panel of the Database Server.
	4.3. Check power cable connection with the Server.
	4.4. If the Server is off, try to start-up the server and access the BIOS looking for message errors.
	4.5. Check SAS cables connections between servers and storage.
	5. If the result of the previous activities implies a failing database server, then the Primary Server is marked with the status of "failing".
	Recovery:
	6. Notifies the Technology Manager of the System failure, and ask for authorization.
	7. Gives authorization for the execution of the recovery procedures.
	8. Block Firewall access to the server from the external network.
	9. Shutdown the database service in the first node (primary node).
	10. Check integrity and status of the database files in the storage.
	11. If the storage files are corrupted or the status is incorrect, check for the contingency procedures for the Back-Up Center.
	12. If the storage data files are correct:
	12.1. Mount the storage device, and start the database service in the secondary node, and execute the scripts for primary database transition.

	12.2. Check logs system messages in the database server and application servers.
	13. Notifies the Technology Manager that the system has been recovered.
	14. Gives authorization for firewall activation, and declares the end of the Recovery process.
	15. Open Firewall access to the server from the external network.
C. **There is Server Hardware Failure and Real-Time Election Information System (REIS) Listener Service Interruption.**	
	1. The Network Monitor System triggers an alarm related with the REIS Listener Server, or
	2. The active monitoring of the regional technician detects the failure.
	3. The Back-up REIS Listener Server should execute the contingency procedures and scripts automatically:
	3.1. Check log messages in the REIS Listener server.
	3.2. Check network connection.
	3.3. If the service is up and running, no further actions are required.
	4. If the secondary server doesn't start automatically, then the following steps are required:
	4.1. Check REIS Listener server network reachability.
	4.2. Check for warnings or error in the front panel of the REIS Listener Server.
	4.3. Check power cable connection with the Server.
	4.4. If the Server is off, try to start-up the server and access the BIOS looking for message errors.

	5. If the result of the previous activities implies a failing REIS Listener server, then the Primary Server is marked with the status of "failing".
	Recovery:
	6. Notifies the Technology Manager of the System failure, and ask for authorization.
	7. Gives authorization for the execution of the recovery procedures.
	8. Block Firewall access to the server from the external network.
	9. Shutdown the Primary REIS Listener Server in the first node.
	10. Check status of the secondary server.
	11. If the secondary server failed, check for the contingency procedures for the Back-Up Center.
	12. If the secondary server is working properly:
	12.1. Check the Application status in the secondary node, and execute the scripts for primary REIS Listener transition.
	12.2. Check logs system messages in the REIS Listener server.
	13. Notifies the Technology Manager that the system has been recovered.
	14. Gives authorization for firewall activation, and declares the end of the Recovery process.
	15. Open Firewall access to the server from the external network.
D. **There is Server Hardware Failure and REIS Service Interruption.**	
	1. The Network Monitor System triggers an alarm related with the REIS Server, or
	2. The active monitoring of the regional technician detects the failure.
	3. The Back-up REIS Server should execute the

	contingency procedures and scripts automatically:
	3.1. Check log messages in the REIS server.
	3.2. Check network connection.
	3.3. If the service is up and running, no further actions are required.
	4. If the secondary server doesn't start automatically, then the following steps are required:
	4.1. Check REIS Listener server network reachability.
	4.2. Check for warnings or error in the front panel of the REIS Server.
	4.3. Check power cable connection with the Server
	4.4. If the Server is off, try to start-up the server and access the BIOS looking for message errors.
	5. If the result of the previous activities implies a failing REIS server, then the Primary Server is marked with the status of "failing".
	Recovery:
	6. Notifies the Technology Manager of the System failure, and ask for authorization.
	7. Gives authorization for the execution of the recovery procedures.
	8. Block Firewall access to the server from the external network.
	9. Shutdown the Primary REIS Server in the first node.
	10. Check status of the secondary server.
	11. If the secondary server failed, check for the contingency procedures for the Back-Up Center.
	12. If the secondary server is working properly:
	12.1. Check the Application status in the secondary node, and execute the scripts for primary REIS

	transition.
	12.2. Check logs system messages in the REIS server.
	13. Notifies the Technology Manager that the system has been recovered.
	14. Gives authorization for firewall activation, and declares the end of the Recovery process.
	15. Open Firewall access to the server from the external network.
E. **There is Power Supply Interruption (Blackout) and the National Service is Interrupted.**	
	1. The UPS triggers an alarm.
	Recovery:
	2. Notifies the Technology Manager of the Power Supply failure, and ask for authorization.
	3. Gives authorization for the execution of the recovery procedures.
	4. Power on Generator Set.
	5. Check status of the Generator Set.
	6. Change power connection from the external source to the Generator Set.
	7. Check Status of the UPS Systems.
	8. Continually check status of the External Electricity Source.
	9. When the external source is up (at least 30 minutes), and the UPS system has enough charge, change back the power connection to the external source.
	10. Declare the end of the Recovery process.
F. **There is Power Supply Interruption (Blackout) and the Central Service is Interrupted.**	
	1. The UPS triggers an alarm, or

	2. The lighting system fails.
	3. Check the scope of the power failure.
	4. If the scope of the power failure is only the Regional Building and the System has network connectivity, go to the brownout procedure.
	5. If the scope of the failure affects the network connection, and the failure lasts more than 1 hour, the Recovery procedure is activated.
	Recovery:
	6. Notify the Technology Manager of the Power Supply failure, and ask for authorization.
	7. Ask the COMELEC Project Manager for authorization.
	8. Gives the Authorization for the Recovery Plan.
	9. Check Status of REIS Listener Queues and latest transactions.
	10. Check the Status of the Servers.
	10.1. Check Status of the Database, based on the latest transaction from the Regional Center.
	10.2. Check application servers' status. (Applications and System logs).
	10.3. Check network connection status: network reachability with the routers and firewall in the Region.
	11. If the status of the systems is correct, then:
	11.1. Change the database mode from Stand-by to Primary and check databases services.
	11.2. Start-up REIS and REIS Listener services, and check application log messages.
	12. Ask for authorization from the Technology Manager.
	13. Give the authorization for the activation of the back-up Center Firewall.

	14. Open the Back-up Center Firewall, allowing incoming transmissions.
	15. Check for incoming transmissions in the REIS Listener logs.
	16. Finalize the Recovery Procedures
G. **There is Network Access Failure and National Service is Interrupted.**	
	1. The Network Monitor System triggers an alarm related with the Network Access, or
	2. The active monitoring of the regional technicians detects the network failure.
	3. Perform the following checks:
	3.1. Check network access with the different location (ICMP Testing packets).
	3.2. Check Main router interfaces status.
	4. If the network is unavailable, then the recovery procedure must be activated.
	Recovery:
	5. Notify the Technology Manager of the network failure, and ask for authorization.
	6. Give authorization for the execution of the recovery procedures.
	7. Check connections with the back-up provider:
	7.1. Check network access with all the locations.
	7.2. Check interfaces status.
	8. Disable the connection with the Primary Network provider, and activate the back-up network provider.
	9. Check for incoming connection from the different locations.
	10. Call the Primary Network provider support center, and together check the status of the Network.

	11. When the primary network provider is ready, ask for authorization.
	12. Give authorization for the change.
	13. Disable the connection with the back-up network provider, and activate the primary network provider.
	14. Finalize the recovery procedures.
H. **Critical Weather/High Temperature Conditions and there is National Service Interruption.**	
	1. Check status of air conditioning system. (temperature level indicators).
	2. If the temperature is high (over 30 C), then check the air-conditioning system.
	3. If the air conditioning system is not responding, then call the electricity technician.
	4. Check the air conditioning system. If the air conditioning is not working after 20 minutes, then apply the Recovery procedures.
	Recovery:
	5. Notify the Technology Manager of the air conditioning failure, and ask for authorization.
	6. Give authorization for the execution of the recovery procedures.
	7. Shutdown all Servers in the Datacenter, except for the AES servers.
	8. Start FAN systems in the Datacenter, and watch the temperature level.
	9. Once the air conditioning system has been recovered, the recovery process ends.
I. **Fire, Flooding and Earthquake Occur and there is Central Service Interruption**	
	1. COMELEC Security personnel give instructions for leaving the Regional Data Center.

	Recovery:
	2. Direct all Central Technical personnel to leave the building, and if possible, move to the back-up Center.
	3. Ask the COMELEC Project Manager for authorization.
	4. Give the Authorization for the Recovery Plan.
	5. Check Status of REIS Listener Queues and latest transactions.
	6. Check the Status of the Servers.
	6.1. Check Status of the Database, based on the latest transaction from the Central Center.
	6.2. Check application servers' status (Applications and System logs).
	6.3. Check network connection status: network reachability with the routers and firewall in the Region.
	7. If the status of the systems is correct, then:
	7.1. Change the database mode from Stand-by to Primary and check databases services.
	7.2. Start-up REIS and REIS Listener services, and check application log messages.
	8. Ask for authorization from the Technology Manager.
	9. Give the authorization for the activation of the back-up Center Firewall.
	10. Open the Back-up Center Firewall, allowing incoming transmissions.
	11. Check for incoming transmissions in the REIS Listener logs.
	12. Finalize the Recovery Procedures.

II. **Contingency Procedures Applicable to the Provincial/District/City/Municipal Board of Canvassers**

A. **There is Hard Disk Failure and there is DATABASE/REIS/REIS Listener Service Interruption, the System will freeze, and no further operation can be performed on the System, or CCS Graphical Interface is not responding, or does not start, or shows a blank screen indicating an error boot, or does not turn-on.**	
	1. If the Hard Disk fails, the System will freeze, and no further operation can be performed on the System.
	1.1. The technician must call the National Technical Support Center (NTSC).
	2. If the CCS fails to start, and then the CCS is considered failing, a CCS Hardware failure procedure must be applied.
	Recovery:
	3. The NTSCO presents the failure to his/her supervisor, indicating the name of the server and the location.
	4. Ask the CCST to repeat the turn-off and turn-on procedure.
	5. If the problem persists, then authorize to replace the CCS.
	6. Take the replacement CCS.
	7. Turn off the defective CCS.
	8. Remove the removable memory card from the defective CCS.
	9. Place the replacement CCS in the designated location.
	10. Install the removable memory card into the replacement CCS.
	11. Connect the replacement CCS to the main

	power source and turn it on.
	12. Store the defective CCS in its original packaging.
	13. Call the NTSC and inform about the replacement.
B. **There is power supply interruption (Brownout/Blackout) and Provincial/ District/City/Municipal Canvass Service is Interrupted.**	
	1. The CCS triggers an alarm.
	2. Check CCS and UPS Power connections. If the connections are OK and the power system is failing, then call the National Technical Support Center (NTSC).
	3. Record the location and activate the Recovery Procedures.
	Recovery:
	4. Check the status of the generator set: gasoline level and cable connections.
	5. Start-up the generator set: check for the activity indicator in the generator set.
	6. Unplug the CCS power cables from the external electricity source, and plug the cable in the generator set outlet.
	7. Call the NTSC indicating the status of the system.
	8. Record the new status for the location.
	9. Continually check status of the external electricity source.
	10. When the external electricity source come back, and last for more than one hour, then the CCST must call the NTSC for authorization.
	11. Record the location and give authorization for the change.

	12. Unplug CCS UPS power cable from the generator set and connect it to the external power source.
	13. Call the NTSC indicating the new status of the location.
	14. Record the new status and end the recovery plan for the Center.
C. **There is Wide Area Network (WAN) Access Failure and the Provincial/District/City/Municipal Canvass Service is Interrupted.**	
	1. The active monitoring of the CCST detects the network failure, or
	2. The Provincial/Municipal Canvass Server is unable to forward/receive the canvass results to the next level (from the previous level), and calls the National Support Center for assistance.
	Recovery:
	3. Check the status of the network device.
	4. Unplug the network device, plug again, and test the connection.
	5. If the CCS can't connect, then call the NTSC indicating the status of the system.
	6. Record the new status for the location.
	7. Check the network status with the Network Providers.
	8. Call the network technicians in order to supply back-up network devices.
	9. Check provincial connection with the back-up device.
	10. Plug the back-up network device into the CCS and test the connection.
	11. If CCS is able to connect to the network, then no further action is needed. If unable to connect, the network technician needs to check the network device and network availability with the

	Provider.
	12. Once the connection is ready, call the NTSC indicating the status of the system.
	13. Record the new status for the location.
D. **There is a Catastrophe: Fire, Flood, Earthquake and others, and the Provincial District/City/Municipal Canvass Service is Interrupted.**	
	1. Provincial Security personnel gives instructions for leaving the Provincial Center.
	Recovery:
	2. All the personnel must leave the place following the instructions of the Provincial/Municipal Security personnel.
	3. Check with the COMELEC Project Manager for instructions related with the Provincial Center.
	4. COMELEC will inform about the action to be taken for the Provincial/Municipal Center.
E. **There is sabotage, equipment robbery and other similar circumstances, and the Provincial/ District/ City/Municipal Canvass Service is Interrupted.**	
	1. Provincial/District/City/Municipal Security personnel will inform about any concern related with physical security.
	Recovery:
	2. If the Center is safe, ask the Provincial/District/ City/ Municipal personnel to stay in the Center, and the canvassing procedure continues.
	3. If the Center isn't safe, the Provincial/District/ City/Municipal personnel must leave the place, and the canvassing procedure stops.
	4. Check all the network devices, and servers. If one of the equipment is missing, call the NTSC, and inform about the missing equipment. For the replacement procedure, check the corresponding

	recovery procedure.
F. During consolidation, the canvass reports yield zero votes for all candidates in all positions.	
G. The CCS does not transmit consolidated canvassed results to the next level.	

III. **Contingency Procedures Applicable to the Vote Counting Machine (VCM)**

A. **The BEI PIN is unavailable.**	1. BEI Chairman will inform the VCM Technician.
	2. VCM Technician will inform the VCM Technical Coordinator.
	3. VCM Technical Coordinator will inform the NTSC.
	4. NTSC will authorize and provide the issuance of the PINs to the BEI.
	5. BEI members will use the PINs.
	6. VCM Technical Coordinator will inform NTSC on the acceptance of the PINs provided.
B. **There is a ballot jam.**	1. If the ballot is visible, the BEI, in the presence of watchers and the public, will gently pull out the ballot from the roller.
	2. If the ballot is not visible, BEI will call the VCM Technician who will remove the VCM from the ballot box, and retrieve the ballot causing the jam.
	3.BEI Chairman, after the VCM has been cleared of the ballot jam and installed again the VCM on the ballot box, will re-feed the ballot to the VCM.
	4. If the ballot is previously scanned, ballot will be returned.
	5. If the ballot was rejected for other causes (e.g., invalid, ambiguous, misread), BEI will follow the provisions as stated in the General Instructions for BEIs for rejected ballots.
	6. In case when the ballot jam is caused by the improper stacking of the ballots inside the ballot box, the BEI should shake the ballot box so that the ballots can adjust and allow feeding of new ballots.
	7. If there is a need to open the ballot box in order to make room for additional ballots, the BEI Chairman, in the presence of watchers, will open the ballot box, press the ballots in order to make room for additional ballots, and thereafter, close the ballot box.

C. **There is a printer jam.**	1. BEI will call the VCM Technician.
	2. VCM Technician will open printer cover and remove the jam gently pulling the paper.
	3. VCM Technician will reload the paper or add new paper roll if required, once the jam has been removed.
D. **The BEIs' passwords are unavailable.**	1. BEI Chairman will inform the VCM Technician.
	2. VCM Technician will inform the VCM Technical Coordinator who in turn will call the NTSC.
	3. NTSC will authorize and provide the issuance of the passwords to the BEIs.
	4. BEI members will use the passwords.
	5. VCM Technical Coordinator will inform the NTSC of the acceptance of the passwords provided.
E. **VCM malfunctions.**	1. BEI will call the VCM Technician assigned in the polling center.
	2. VCM Technician will look for the root of the failure and solve it.
	3. If the VCM Technician cannot solve the failure, he/she will report the incident to the VCM Technical Coordinator to request help from the NTSC.
	4. If the VCM Technical Coordinator cannot solve the failure, he/she will contact the NTSC to ask for proper solution.
	5. VCM Technician will attempt to repair the machine with the help of NTSC support personnel.
	6. After 60 continuous minutes of failure and non - operation of the VCM, the NTSC will authorize the deployment of a contingency VCM kit for replacement.
	7. VCM Technical Coordinator must get the new VCM kit bring it to the Polling Center and conduct the replacement procedure of the VCM.
F. **Any of the two SD cards (main/primary and back-up SD cards) failed.**	1. BEI will call the VCM Technician assigned in the polling center.
	2. VCM Technician will look for the root of the failure and solve it.
	3. If the VCM Technician cannot solve the failure, he/she will report the incident to the VCM Technical Coordinator to request help from the NTSC.
	4. If the VCM Technical Coordinator cannot solve

	the failure, he/she will contact the NTSC to ask for proper solution.
	5. VCM Technician will attempt to repair the machine with the help of the NTSC support personnel.
	6. After 60 continuous minutes of failure and non - operation of the VCM, the NTSC will authorize the deployment of a contingency VCM kit for replacement.
	7. VCM Technical Coordinator must get the new VCM kit, bring it to the Polling Center and conduct the replacement procedure of the SD card.
G. **The WORM SD card failed.**	1. BEI will call the VCM Technician assigned in the polling center.
	2. VCM Technician will look for the root of the failure and solve it.
	3. If the VCM Technician cannot solve the failure, he/she will report the incident to the VCM Technical Coordinator to request help from the NTSC.
	4. If the VCM Technical Coordinator cannot solve the failure, he/she will contact the NTSC to ask for proper solution.
	5. VCM Technician will attempt to repair the machine with the help of NTSC support personnel.
	6. After 60 continuous minutes of failure and non- operation of the VCM, the NTSC will authorize the deployment of a contingency VCM kit for replacement.
	7. VCM Technical Coordinator must get the new VCM kit, bring it to the Polling Center and conduct the replacement procedure of the back-up SD card (WORM).
H. **Power failure on election day.**	Review and check the VCM connection to the battery after the VCM is connected to a power outlet. The battery is capable to operate for 14 hours straight and the VCM is capable of charging the battery.
I. **The battery has been discharged after FTS.**	If there is power in the Polling Center, connect the battery to the VCM to charge it.
J. **One of the iButtons failed to register.**	The VCM kit has 3 iButtons assigned, 1 for Chairman, 1 for BEI member and 1 for BEI Poll Clerk. The VCM can be activated with a

	combination of 2 out of the 3 iButtons.
K. **The three (3) iButtons are unavailable**.	1. If iButtons are present, the BEIs must verify that the ibuttons are being used in the right VCM and with the correct PINs and passwords.
	2. If the iButtons are not presentin the kit or got lost by the BEIs, follow General Instructions regarding manual voting activation.
L. **Transmission failed after three (3) attempts.**	1. The BEI will call the VCM Technician assigned in the polling center.
	2. The VCM Technician will look for the root of the failure and solve it depending on the transmission media available.
	3. If the VCM Technician cannot solve the failure, he/she will report the incident to the VCM Technical Coordinator to request help from the NTSC.
	4. If the VCM Technical Coordinator cannot solve the failure, he/she will contact the NTSC to ask for the proper solution.
	5. The VCM Technician will attempt to repair the transmission failure with the help of NTSC support personnel.
	6. If the problem is the transmission device, the BEI can request a transmission device from any of the other precincts nearby and attempt to re-transmit.
	7. If the failure is still consistent, the BEI will Transport VCM to nearest Municipal Voting Center and attempt to re-transmit.
	8. If the transmission is still failing the BEI must follow General Instructions regarding manual upload of data from WORM SD card to the CCS laptops.
M. **The date of the elections is incorrect on the ERs and other reports.**	1. The BEIs need to enter to the main menu of the VCM.
	2. Select on utilities > Change system date and time.
	3. Proceed to change the date and or time according to the requirement and press apply.
N. **VCM does not write protect the data**.	1. The BEIs must follow the steps to conduct the write protect procedure.
	2. Check that the SD card is inserted in the Slot A and that the Backup SD card (WORM) in inserted in the Slot B.
	3. Once the write protect is done, the VCM shuts

	down and will not operate any more.
O. **VCM does not shutdown.**	1. BEI will call the VCM Technician assigned in the polling center.
	2. VCM Technician will look for the root of the failure and solve it depending on the transmission media available.
	3.If VCM Technician cannot solve the failure, he/she will report the incident to the VCM Technical Coordinator to request help from the NTSC.
	4. If the VCM Technical Coordinator cannot solve the failure, he/she will contact the NTSC to ask for the proper solution.
	5. VCM Technician will attempt to repair the transmission failure with the help of NTSC support personnel.
P. **Transmitted ERs yield zero votes for all candidates in all positions.**	1. BEI needs to verify the printed ERs to confirm the quantity of voters who actually voted, and the valid ballots cast.
	2. If the quantity of voters who actually voted is zero, that means that no ballots were cast.
	3. If the quantity of valid ballots cast is the same as the quantity of voters who actually voted, that means that none of the ballots casted was valid due to errors on the ballot shading and the VCM interpreted over votes or abstentions.
Q. **The VCM Technician cannot communicate with the NTSC, or the NTSC cannot be reached.**	1. The VCM technician can contact the VCM technical Coordinator.
	2. The VCM Technical Coordinator can contact the NTSC on behalf of the VCM Technician.
	3. The NTSC will contact the VCM Technician or any of the BEIs in place.
R. **There is no VCM technician in place.**	1.BEI can inform the Command Center about the issue.
	2. The Command Center will inform the NTSC about the lack of field support personnel in place.
	3. The VCM Technical Coordinator will inform the name and time of arrival of the new VCM technician assigned to the BEIs.
S. **The VCM kit has missing items.**	1. BEI will call the VCM Technician assigned in the polling center.
	2. VCM Technician will confirm what the missing item/s is/are.
	3. If the VCM Technician cannot find the missing item, he/she will report the incident to the VCM

	Technical Coordinator to request help from the NTSC.
	4. If the VCM Technical Coordinator finds the missing item, he/she will contact the NTSC.
	5. NTSC will authorize the deployment of a contingency VCM kit to get the missing item.
	7. VCM Technical Coordinator must get the new VCM kit, bring it to the Polling Center and get the required item.
T. **The VCM kit has not been delivered.**	1. The BEIs will call the Command Center to verify the arrival of the VCM kits.
	2. The Logistics provider will inform if there is a delay and when the VCM kit will be delivered in place.
	3. The Command Center will inform the BEIs the expected time of arrival of the VCM kit.
U. **The Ballots have not been delivered.**	1. The BEIs will call the Command Center to verify the arrival of the Ballots.
	2. The Command Center will verify with the EOs the location of the Ballots.
	3. If the Ballots are still on the Logistics provider's hands, it will inform if there is a delay and when the Ballots will be delivered in place.
	4. If the Ballots are still on the EO's hands, it will inform if there is a delay and when the Ballots will be delivered in place.