VoTeR Center

UConn Voting Technology Research Center

PI : A. Shvartsman, Ph.D.
Co-PIs : A. Kiayias, Ph.D., L. Michel, Ph.D., A. Russell, Ph.D.
Staff: T. Antonyan, S. Davtyan, S. Kentros, N. Nicolaou

Post-Election Audit of Memory Cards for the November 2008 Elections

Version 1.0, May 12, 2009

Summary

The UConn VoTeR Center performed a post-election audit of the memory cards for the AccuVote Optical Scan tabulators that were used and to be used in the November 2008 Elections. The cards were programmed by LHS Associates of Methuen, Massachusetts, and shipped to Connecticut districts for use in the elections. The VoTeR Center received in total 462 memory cards from a number of districts after the elections. This document reports on the findings obtained during the audit. Among these cards, 279 were used in the elections, the rest remained unused, serving as back-up cards. The 279 cards represent over 30% of all districts, thus the audit is broad enough to draw meaningful conclusions. We note that in a few cases, districts apparently had problems with one tabulator and had to complete the election using another tabulator.

Among the 462 cards received and tested, 421 cards (91%) were found to have been properly programmed for election. These cards contained valid ballot data and the executable code on these cards was the expected code, with no extraneous data or code on the cards. The remaining cards, 41 or 9% were found to contain "junk" data, that is, they were unreadable, which is easily detected by the tabulators as such, and could not have been used in the election. We are currently performing additional analysis to determine the cause of this. A separate report will document our findings.

Among the 279 cards actually used in the elections, all cards were properly programmed. Three cards contained a few unexpected data characters beyond the range of memory used by the tabulators; these characters do not affect the operation of the tabulator. Three additional cards did not match the pre-election baseline, and all such cases we found a valid reason for these discrepancies.

There are a number of cards that, although not presenting an immediate security concern, were found in unexpected states or contained unexpected timing of events. For example, a number of cards were duplicated prior to the election. We note that the adherence to the election procedures by the districts is improving, however additional effort is needed to ensure that the established procedures are followed and that any exceptions are documented and communicated to the SOTS Office.

In summary, (1) all cards used in the election were properly programmed, (2) cards with junk data continues to be a problem, and additional analysis is in progress to determine the cause, (3) a number of cards show that the pre-election procedures are not followed uniformly and that cards continue to be duplicated; we recommend that a stronger policy statement is needed on handling the cards before and during the election and disallowing memory card duplication.

The audit was performed on request of the Office of the Secretary of the State.

1 Preface

The Voting Technology Research (VoTeR) Center at the University of Connecticut conducted a post-election audit of the memory cards used in the AccuVote Optical Scan (AV-OS) tabulators in the November 2008 elections. The audit was performed on request of the Office of the Secretary of the State of Connecticut.

The memory cards were programmed by LHS Associates of Methuen, Massachusetts, and provided by LHS to the districts in Connecticut. The audit was performed on all memory cards that were shipped by the districts after the elections to the VoTeR Center at the University of Connecticut in Storrs.

The memory cards were subject to several integrity tests. A comprehensive overview of the procedures followed by the VoTeR Center personnel in conducting such audits is presented in a prior report[1]. We do not repeat here the description of the engineering that was performed to enable the audit and the technical setup used in the tests.

In this report, we present the objectives of the post-election audit and the audit results. The audit process included testing, comparison, and analysis of the data collected during the audit. The procedures followed in this audit include a strict chain of custody policy with regard to handling the cards, maintaining a log of all transactions and activities, and safekeeping (both physical and electro-magnetic) of the memory cards.

We conclude the report with several observations based on what was learned during the post-election audit process. We believe that technological audits are crucial in providing valuable feedback and maintaining the integrity of the electoral process.

This report is a high-level, non-technical presentation of the audit results and it omits all technical details. We also note that we had no access to, and we did not use any vendor documentation regarding the design and the internals of the AV-OS terminal.

About the UConn VoTeR Center

Following our participation in the Connecticut Voting Technology Standards Board in 2005, the Voting Technology Research (VoTeR) Center was established in 2006 to advise state government in the use of voting technologies, to research, investigate and evaluate voting technology and voting equipment, and to develop and recommend safe use procedures for the computerized voting technology in elections. The personnel of the Center includes several faculty members, graduate students, and staff of the Computer Science and Engineering Department at the University Of Connecticut.

The work of VoTeR Center in the State of Connecticut is funded by the Office of the Connecticut Secretary of the State (SOTS), and we function in close contact with the SOTS Office personnel. We offer the State an independent, objective analysis of the voting technologies offered by several vendors, we advise the State on selecting and administering the voting equipment for its election needs, and we are not associated with any of the voting technology vendors. The evaluations of the voting technology are performed at the VoTeR Center Lab at the University of Connecticut. These include hands-on evaluations, exploration of possible attack vectors, physical integrity checks of the terminals and memory cards, and mitigation strategies. The VoTeR Center is not involved in establishing State's policies for procuring the voting technology, but limited to providing technical expertise on, and evaluating these technologies before deployment and during the use by the State. In this sense the VoTeR Center is a third party independent technical consulting resource for the State of Connecticut.

[1] Pre-Election Audit of Memory Cards for the November 2007 Connecticut Elections. UConn VoTeR Center, Version 1.0, January 24, 2008. Available online at http://voter.engr.uconn.edu/voter/Reports.html.

VoTeR Center personnel assisted the State in developing safe use procedures for the Optical Scan terminals. The procedures in place for the election include strict physical custody policy, tamper-resistant protection of the equipment, and audits. The Center provides ongoing recommendations to strengthen and improve the security of elections based upon our findings in evaluating the voting equipment and conducting pre- and post-election technological audits.

2 Introduction

We start by overviewing the AV-OS based election system used in Connecticut, the goals of the post-election memory card audit, and a preview of the audit results.

2.1 Brief Description of the AV-OS

The AV-OS election system consists of two components: the AccuVote Optical Scan voting terminal (AV-OS terminal) and the ballot design and central tabulation system, GEMS, for Global Election Management System. See our report at URL http://voter.engr.uconn.edu/voter/Report-OS.html for details on this election system. We point out the following characteristics of these components:

- The AV-OS systems currently in use in the State of Connecticut contain the firmware version 1.96.6. It is equipped with an optical scanner, a paper-tape dot-matrix printer, a LCD display, a serial communication port, and telephone jacks leading to a built-in modem.
- The GEMS software is installed on a conventional PC (or a laptop). It includes a ballot design system and a tabulation system.
- Once the election data is entered into the GEMS system, the specifications of the election are downloaded into a memory card via an AV-OS system connected to GEMS by a serial line cable.

  In the State of Connecticut, GEMS is not used for central tabulation of election results.
- The memory cards are the 40-pin 128KB Epson cards. The memory card is installed into to the 40-pin card slot (J40 connector) of the AV-OS. It is worth mentioning that Epson has discontinued this memory card some time ago, and reader/writers for this memory card are not readily available.

For election deployment the system is secured within a ballot box so that no sensitive controls or connectors are exposed to the voter. Each memory card contains executable code that is used for printing the reports. The code is written in a proprietary symbolic language. Such executable files are identified as *.abo (AccuBasic Object) bytecode. The installation of the GEMS software on the PC contains several databases that include the data and ballot layout corresponding to the districts of the State of Connecticut, as well as the bytecode for AV-OS.

2.2 Goals of the Post-Election Memory Card Audit

The VoTeR Center was asked by the CT SOTS Office to prepare for and implement memory card audits. The primary goal of the post-election audit was to perform an integrity check of the contents of the memory cards that were used in the elections.

The memory cards contain the data and the ballot layout for the elections. The memory cards used in the AV-OS terminals also store the tally of the ballots cast and report the results of the election. In this sense the memory cards are the electronic analogue of a physical ballot box. The data, layout and the functionality on the memory cards are loaded on to the memory card using

the AV-OS terminal from the GEMS database. The GEMS database to be used as the baseline for the election data was provided by LHS Associates prior to the election. The total of 462 cards were shipped to the VoTeR Center by the districts for the purposes of the audit. The contents of the cards were then extracted and compared with the intended contents using the GEMS database as the reference. The audit process was automated to the extent possible. Any discrepancies or deviations from the baseline that were inconsistent with the use of the cards in the election were then logged and analyzed. Specifically, the memory cards were audited for any deviations in the ballot data/layout, bytecode, the state of the counters and the audit logs on the memory cards. We note that this is the first post-election audit where we performed a comprehensive analysis of the audit logs.

2.3 Preview of the Audit Results

The total of 462 cards, were received and tested by the VoTeR Center. Among these 462 cards, 415 cards (89.8%) were found to have been properly programmed for election. These cards contained valid ballot data and the executable code on these cards was the expected code, with no extraneous data or code on the cards. 0.6% of the cards (3 cards) contained a few bytes of noise (or "specks") that apparently do not interfere with electoral process; these cards were otherwise properly programmed.

One card (0.2%) contained a different candidate name. This was due to a very late replacement of a candidate.

One card (0.2%) contained a single letter difference in the district designation (Enfield District 4B-58 vs. 4A-58). Follow up with SOTS personnel determined that this is due to the different naming of otherwise identical cards for a specific district.

One card (0.2%) contained a different ballot identifier relative to the expected pre-election baseline. This identifier has no effect on the programming and usage of the card.

41 cards, or 8.9%, were found to contain "junk" data, these cards are unreadable by the tabulators, and easily detected as such. These cards not have been used in the election. Although this does not present a security risk, this is a high percentage of faulty cards. We also note that this is consistent with the percentage reported for the pre-election audit of November 2008 elections. The percentage is lower than detected in the post-election audit for the August 2008 primary (15%), but higher than detected in the pre-election audit for the August 2008 primary (5%), post-election audit for the February 2008 primary (5%), post-election audit for the November 2007 elections (8%), and pre-election audit for the November 2007 elections (4%).

There are a number of cards that, although not presenting an immediate security concern, were found in unexpected states or contained unexpected timing of events. We note that the adherence to the election procedures by the districts is improving, however additional effort is needed to ensure that the established procedures are followed and that any exceptions are documented and communicated to the SOTS Office.

3 Audit Results

We now present the results of the post-election audit in more detail. For the November 2008 elections we received and examined 462 cards. These cards were programmed by LHS. The cards were shipped by the districts to the VoTeR Center for the purposes of the post-election audit. The high level breakdown of the 462 cards is as follows.

- 279 were used in the elections,
- 142 were not used in the elections (in effect serving as back-up cards),
- 41 contained junk data.

3.1 Memory Card Data Audit Results: 279 Cards Used in the Election

Table 1 shows the frequency of various states observed on the audited memory cards for the 279 cards used in the election. The data is presented in two parts:

(a) Card Format: 273 cards (97.8%) were properly formatted and contained good data.

Three cards (1.1%) were properly formatted and contained good data, but also included a few "specks", that is a few isolated bytes with unexpected values. The specks are located beyond the data used by AV-OS, they are not detected by AV-OS, and it does not appear that they interfere with normal AV-OS operation. Given that the specks are located beyond the first 32K of memory used by AV-OS this does not represent a security/integrity risk (the situation would have been different if the specks were found within the first 32K of memory).

One card (0.4%) contained a different candidate name. This was due to a very late replacement of a candidate.

One card (0.4%) contained a single letter difference in the district designation (Enfield District 4B-58 vs. 4A-58). This discrepancy has been explained: it is due to different naming of otherwise identical cards when multiple cards are programmed for the same district.

One card (0.4%) contained a different ballot identifier relative to the expected pre-election baseline. This identifier has no effect on the programming and usage of the card.

(b) Card & Counter Status: 259 cards (92.8%) were in Election Closed state and had Non-Zero counters. This is the intended state for memory cards that had been used in the election.

20 cards (7.2%) were in Results Print aborted state with Non-Zero counters. Such cards are expected to have non-zero counters. However this is an undesired state, indicating that poll workers shut the machine during the printing of the results after the election was closed (perhaps unintentional additional printing of the results). This is not the intended procedure. Clearly these cards were used in the actual election. The results must eventually be printed and signed by the poll officials, according to election procedures, which suggests that the results were printed and signed, but election officials did not wait for the (final) printing to complete, and turned-off the machine prematurely. It should be recommended that the poll workers must allow the printing of results to complete, before turning off the AV-OS machines.

No cards with uploaded results were found. No cards with audit report printed were found. These are the expected results.

3.2 Memory Card Data Audit Results: All 462 cards

Table 2 shows the frequency of various states observed on the audited memory cards for the 462 cards examined. The data is presented in three parts:

(a) Card Format: 415 cards (89.8%) were properly formatted and contained good data.

Three cards (0.6%) contained a few bytes of noise (or "specks") that apparently do not interfere with electoral process; these card were otherwise properly programmed.

One card (0.2%) contained a different candidate name. This was due to a very late replacement of a candidate.

One card (0.2%) contained a single letter difference in the district designation (Enfield District 4B-58 vs. 4A-58). This discrepancy has been explained: it is due to different naming of otherwise identical cards when multiple cards are programmed for the same district.

	Cards Used in the Election	
	Number	% Total
(a) Card Format		
Good Data, Clean Card	273	97.8%
Good Data, Some "Specks"	3	1.1%
Good Data, Different Candidate Name	1	0.4%
Good Data, Different District Number	1	0.4%
Good Data, Different Ballot Id	1	0.4%
Totals:	279	100%
(b) Card &Counter Status		
Election Closed, Non-Zero Counters	259	92.8%
Election Closed, Zero Counters	0	0%
Results Print aborted, Non-Zero Counters	20	7.2%
Results Sent/Uploaded	0	0.0%
Audit Report Printed	0	0.0%
Totals:	279	100%

Table 1: Memory card analysis summary for cards used in the election: (a) card format, (b) card & counter status.

One card (0.2%) contained a different ballot identifier relative to the expected pre-election baseline. This identifier has no effect on the programming and usage of the card.

41 cards (8.9%) contained "junk" data, that is the card format is unrecognizable and appears to contain arbitrary noise. Such cards are not readable by AV-OS and they are readily detected through pre-election testing by poll workers, thus they could not have been used in the election.

In the rest of the analysis the percentages are computed for the 421 cards (91.1%) that were properly formatted, i.e., the cards that did not contain junk data.

(b) Card Status: This refers to the current state of the memory card, such as loaded with an election, set for election, running an election, or closed election, and others.

259 cards (about 61.5%) were in the Election Closed state, which is the desired memory card state for cards that were used in the elections.

20 cards (4.7%) were found to be in the Results Print Aborted state (this was discussed in the previous section).

90 cards (21.4%) were in Set For Election state. Such cards were not used in the election. They were back-up cards. This is the intended state for such cards.

Finally, 52 cards (12.4%) were in Not Set for Election state. This is not the intended state. All cards going into the election date should be in the Set for Election state, following pre-election testing. This does not present a safety issue: however this suggests that the pre-election procedures were not following uniformly by the districts.

(c) Card & Counter Status: 88 cards (20.9%) were in Set For Election state and had Zero counters. This is the intended state for memory cards that were not used in the elections.

259 cards (61.5%) were in Election Closed state and had non-Zero counters. This is the intended state for memory cards that had been used in the election.

20 cards (4.7%) were in Results Print aborted state, with non-Zero counters. (This was discussed above.)

Two cards (0.5%) were in Set For Election state and had non-Zero counters. Further investigation revealed that these cards were used in an election and at some point there was a switch from the first machine used in the election to the second (back-up) machine. The cards are: RIDGEFIELD-DISTRICT_1-0001928 and GREENWICH-DISTRICT_5-0002508. It is appropriate for these cards to not be in Results Print aborted or Election Closed state, since this indicates that there was no report of partial election results.

41 cards (9.8%) were in Not Set state with non-Zero counters. This is not the expected state, still it is not problematic as discussed above.

11 cards (2.6%) were in Not Set state with Zero counters. This is not the expected state. Presumably if these cards were to be used in the election, they would have been set to the Set for Election state.

The fact that roughly one third of the cards that were not used in the election were not in the expected state indicates that poll workers did not uniformly follow the proper pre-election procedures.

3.3 Log Analysis of the 421 Readable Cards

We examined the audit log of the 421 readable (i.e., non-junk) memory cards against a set of proper-use rules that we defined for memory cards depending on whether or not there were used in an election. Here we summarize our findings.

(a) 15 cards (3.6%) had more than 10 "session start" events. This refers to machine restarts. Some cards had as many as four restarts in one minute.

Among these cards, 10 cards (2.4%) additionally had a Count Restarted event during the election day.

This indicates that in some districts there were difficulties with the machines, perhaps ballot jams. It is suggested that records be made at the districts in all cases where the machines are restarted to help diagnose any problems that may have occurred.

(b) 41 cards (9.7%) contained duplication events in their logs, with 5 cards indicating more than one duplication. There should be no reason to duplicate the cards. One possibility is that duplication was performed when cards containing junk data were discovered during testing. It is strongly recommended that duplication not be performed at districts and that all improperly programmed cards are reported to SOTS Office as soon as this is discovered.

(c) 29 cards (6.9%) had a "zero totals report" printed before the date of the election. This can happen if one starts a machine before the date of the election after setting it for elections.

(d) 24 cards (5.7%) were programmed from 10/27/2008 to 10/30/2008. While this is not necessarily problematic in the election, these cards were not subject to pre-election audit.

(e) 2 cards had an additional Zero Totals Report event during the Election day. This happens if you restart the machine after finishing printing the Zero Totals Report.

(f) 1 card had the election close at 22:08.

	All Cards	
	Number	% Total
(a) Card Format		
Good Data, Clean Card	415	89.8%
Good Data, Some "Specks"	3	0.6%
Good Data, Different Candidate Name	1	0.2%
Good Data, Different District Number	1	0.2%
Good Data, Different Ballot Id	1	0.2%
Not Programmed	0	0%
Unusable Cards, "Junk Data"	41	8.9%
Totals:	462	100%
(b) Card Status		
Not Programmed (Blank)	0	0%
Not Set for Election	52	12.4%
Set for Election	90	21.4%
Results Print Aborted	20	4.7%
Election Closed	259	61.5%
Totals:	421	100%
(c) Card &Counter Status		
Not Programmed, Zero Counters	0	0%
Not Set for Election, Non-Zero Counters	41	9.8%
Not Set for Election, Zero Counters	11	2.6%
Set for Election, Non-Zero Counters	2	0.5%
Set for Election, Zero Counters	88	20.9%
Results Print aborted, Non-Zero Counters	20	4.7%
Election Closed, Non-Zero Counters	0	0.0%
Election Closed, Zero Counters	259	61.5%
Totals:	421	100%

Table 2: Memory card analysis summary for all cards: (a) card format, (b) card status, (c) card & counter status.

(g) 6 cards had the "prep for election" event on the day of the election. Such event should have taken place some days before the election and not on the election day. This suggests that pre-election testing procedures were not followed.

(h) 4 cards had an "Memory Card Reset" event. Resetting the cards clears the counters after the tabulator is placed in the election mode. All 4 cards were reset before the election date, thus no actual votes were lost. Nevertheless, this indicates a deviation from standard procedures.

(i) 1 card had an Upload Started event. This indicates deviation form standard procedures (apparently upload was attempted, but of course there was no receiving system). The card was not used in the election and otherwise its log appears normal.

(j) 2 cards had test elections on 10/31/08. We expected test elections to happen earlier.

(k) 1 card has a test election on 11/03/08. We expected test elections to happen earlier.

(l) 1 card has a test election on 11/26/08 and an election executed on 12/04/08. This suggests that the clock of the machine was 1 month ahead. The card was used in the election and had 1436 votes. The card is FARMINGTON-DISTRICT_1-3-0004962.

None of the observations made in our analysis of the audit logs indicate a security problem or malicious intent. However, it appears that proper procedures are not followed uniformly. We discuss this in more detail in the last section.

3.4 Bytecode Analysis Result on the Readable Cards

We have analyzed the Accu-Basic bytecode that is loaded into each programmed memory card. Based on the analysis we conclude that the bytecode provided by LHS Associates for the elections is safe to use. The bytecode performs the expected reporting functions. Note that it is not possible to overwrite the contents of the card with the Accu-Basic bytecode.

4 Discussion and Recommendations

Having performed and completed the audit, we believe that memory card audits are crucial in providing valuable information necessary to ensure the integrity of our electoral system. There are several noteworthy observations that emerge from the audit analysis. We now discuss the the observations in terms of their procedural and technological significance.

4.1 Procedural Observations

- Preparation for elections: Among the cards that were not used in the election, there are still many cards (about 12%) that are not set for election. This is about the same percentage as observed in the post-election audit for November 2007 elections. All cards need to undergo pre-election testing and be set for election by the election day.

  It is possible that test elections were performed, however, the cards were not set for election by the districts. In any case, this indicates that pre-election procedures were not followed. All cards not used in the election should be in "Set For Election" status with zero counters.

- Card duplication: The CT SOTS Office instructed the municipalities to not duplicate cards. If there is any perceived reason for cards to be duplicated, the CT SOTS Office must be promptly informed. Duplicating cards creates cards that have not been directly produced from

the election database (GEMS at LHS), and should not be allowed to be used in the elections until proper procedures are developed. It is recommended that SOTS Office offer training through ROVAC to reinforce that stated no-duplication policy.

- Aborted prints of election reports: There are a number of cards that indicate that printing of the election results report was aborted. The districts need to be advised to wait for the complete printout of the reports before shutting the machines down. Presumably at least one complete copy of the report is always printed as it needs to be signed by the election officials. Perhaps the results were printed until the signature space started appearing and then the machines were reset or shut off, or perhaps a duplicate results were printed unintentionally, and then the machine was shut off at that point. This amplifies the need for the election moderators to ensure that end-of-night procedures are strictly followed and that any problems are reported to the SOTS Office.

  However we note an improvement from August 2008, when the post-election audit reported about 7.3% of the cards with print aborted status, vs. 4.7% reported in the current audit.

- In once case the election was closed very late according to the audit log. This could indicate a problem with the machine, or incorrect clock settings, or a simple oversight.

- There were a few other single instances of cards that indicated somewhat unexpected timing of events (2 cards), memory card reset events (4 cards) before the date of the election, and one instance of attempted upload of election results (1 card). While these observations indicate deviations from the standard procedures, there is no negative impact on the use of such cards in the election.

The audit indicates that we have still a large number of cards not in the expected state. None of these cards were in the state that would be an immediate security concern. However, it may be the case that the instructions to poll workers were unclear, or that the poll workers were unable to follow the instructions. We recommend holding additional training sessions explaining to poll workers exactly what needs to be done to prevent this situation in the future.

4.2 Technological Observations

- All readable cards were found to be properly programmed.

- Larger than acceptable number of cards were unreadable and thus unusable because they contained what we describe as "junk" data. By saying that the card is "junk" we understand that the card was not programmed correctly. When one puts the card containing the "junk" data into the AV-OS terminal it issues a prompt requesting to format the card.

  This is clearly a technological issue. We do know that LHS is encountering these issues as well during their testing of the cards, and it would be helpful if LHS reported on how many unreadable cards they detect in their testing.

  Among the audited cards 8.9% of the cards contained junk data. This percentage is high and this issue has to be resolved in the future. We are continuing to investigate the exact causes for the cards to become unreadable. Since the previous election we have established that cards are not damaged in shipping/mailing (unless a card is physically damaged). We have also established that junk data is not due to "hot" (machine turned on) or "cold" (machine turned off) insertion of the cards. We will document our latest findings in a separate report.

- Among the cards examined we found 41 duplicated cards. We note that there is an increase in the duplication of cards. Duplication of cards is done both by the districts and by LHS (based on the timestamps of the duplication events in the memory card audit logs). We assume that the cards were duplicated, apparently to replace bad/unusable card.

  The CT SOTS instructions to municipalities clearly do not allow for cards to be duplicated.

  Our recommendation is that card duplication should not happen in adherence to SOTS instructions.

- No detected ballot data or bytecode corruption.

  During the data analysis we have not detected any corruption of the ballot data or the bytecode. The ballot layout of the audit cards were identical to the ballot layout of the corresponding baseline data.

In conclusion,

(1) all cards used in the election were properly programmed,

(2) cards with junk data continues to be a problem, and additional analysis is in progress to determine the cause,

(3) a number of cards show that the pre-election procedures are not followed uniformly and that cards continue to be duplicated; we recommend that a stronger policy statement is needed on handling the cards before and during the election and disallowing memory card duplication.

Reiterating on our recommendations in more detail, it is vital that established pre-election testing procedures be followed. The SOTS Office should re-issue procedures and offer training. The procedures should provide direction to local election officials not to abort print. Moderators logs must record machine restarts and perceived causes. All moves to back-up machines must be reported to SOTS at the time of the occurrence. The cards must not be duplicated by municipalities. Municipalities should be instructed to report pre-election testing results (and any card problems) to SOTS immediately upon completion of tests. It is worth repeating that any unexpected behavior of machines that necessitates a restart or a memory card reset must be immediately reported to the SOTS Office.

[End]