FREEMAN, CRAFT, MCGREGOR GROUP

California Secretary of State Consultant's Report on:

Functional Testing of the ES&S Unity 3.0.1.1 Voting System

Prepared for the California Secretary of State by:

Steven V. Freeman
Senior Partner

February 15, 2008

Election Systems & Software's
Unity 3.0.1.1 System
Consisting of Application Modules:

- **Audit Manager (AM) version 7.3.0.0**
- **Election Data Manager (EDM) version 7.4.4.0**
- **ES&S Image Manager (ESSIM) version 7.4.2.0**
- **Ballot On Demand version 7.4.2.0**
- **Hardware Manager (HPM) version 5.2.4.0**
- **Election Report Manager (ERM) version 7.1.2.1**
- **M100 Optical Scan Precinct Counter HW 1.3/FW 5.2.1.0**
- **M650 Optical Scan Central Counter HW 1.1/FW 2.1.0.0 (both visual infrared and visual green sensors)**
- **AutoMARK Technical Systems, LLC's**
- **AutoMARK Information Management System (AIMS) version 1.2.18**
- **AutoMARK Voter Assist Terminal (VAT) HW A100/FW 1.1.2258**
- **AutoMARK Voter Assist Terminal (VAT) HW A200/FW 1.1.2258**

Scope of Work and Reporting

State certification testing for the Unity 3.0.1.1 System with the AutoMARK voter assistance terminal consisted of a series of test events:

a. Phase I, System installation and generation of the election definition, CA SOS offices, Sacramento CA
b. Accessibility Testing, CA SOS offices, Sacramento CA
c. "Red Team" Security Testing, CA SOS offices, Sacramento CA
d. Source Code Review, atsec information security offices, Austin, TX
e. Phase II, Functional Testing, ES&S offices, Omaha, NE
f. Volume Testing

This report covers work completed in Phase I and Phase II testing. Narratives describing the Accessibility testing, Volume testing and Security testing ("Red Team" and Source Code Review) are prepared as separate reports.

We are not attorneys and do not offer legal advice. We have assisted the California Secretary of State in the collection of facts and evidence that she will use in reaching certification decisions. However, to advise the Secretary of State (SOS) on the determination of whether the system complies with California's certification requirements would require an interpretation of law. Accordingly we do not provide recommendations or any opinion as to whether the system can be certified.

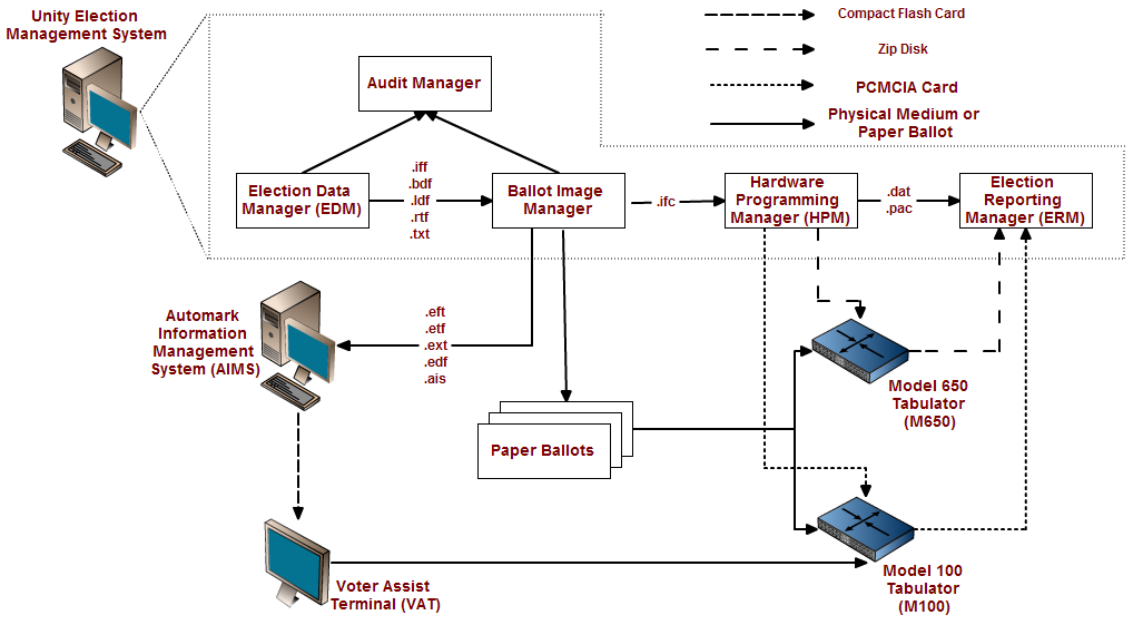
The work that we have performed and our findings are strictly limited to the specific serial numbered hardware elements and specific software elements tested during the examination. An inventory of those items is included as Attachment A to this report. The results described in this report should be reliable and repeatable for those specific items. The decision to apply those

results to decisions about other items is solely at the discretion of and risk of the Secretary of State and the purchasers of the system. Although Attachment A of this report can be used as part of a baseline for reaching conclusions about compliance of other items, users of this report who wish to arrive at such conclusions about compliance of purchased systems or the compliance of a system in use should conduct appropriate acceptance testing or system validation analysis to support those conclusions.

Description of the System Submitted for Certification

The ES&S Unity 3.0.1.1 (Unity) System is a paper ballot based system, but it is marketed in other states with a Direct Recording Electronic (DRE) component and is capable of supporting other balloting options. Specific components excluded for this California certification are:

- iVotronic, a DRE voting machine
- iVotronic Image Manager, a Unity component that supports DRE screen layouts
- Ballot On Line, a Unity component supporting iVotronic operations
- Optech Eagle III-P, an optical scan precinct counter
- Optech IV-C, an optical scan central counter
- Optech Image Manager, a Unity component supporting Optech style ballots
- M150/550, Optical Scan Central Counters (older models)
- Data Acquisition Manager, a Unity component that supports remote collection of voting results using telecommunications
- Compact Flash Multi-Card Reader/Writer, aka CF Duplicator



The Unity system is a suite of software applications which provides election definition (EDM), ballot layout (ESSIM – Shown as "Ballot Image Manager" in the diagram), voting machine programming (HPM), voting result collection (ERM), consolidated reporting (ERM), and access controls and audit logging. Applications that are not required do not need to be installed (such as the iVotronic Image Manager excluded above). In general, the separate applications may be installed and exercised on separate workstations (with the exception of the Audit Manager, which is needed for EDM and ESSIM). The application's design and access controls on the EDM and ESSIM use different standards, programming languages, audit log controls, third party utilities, and databases than the HPM or the ERM with AutoMARK adding yet another set. Data transfers

between the applications and those used for installation to the voting machines are based on different file formats and data transfer technology rather than a shared database system or common data exchange interfaces.

The Unity paper ballots are Australian Ballots, which are defined as "A printed ballot that bears the names of all candidates and the texts of propositions and is distributed to the voter at the polls and marked in secret." The ballots also include machine readable identification information which identifies the ballot style (contest choices and layout) needed to correctly recognize and tally the ballot. They are tallied using devices that read optical marks (the M100 and M650) but may be manually counted or reviewed in an election audit process such as recounts or ballot resolution boards. The M100 optical scanning device uses a continuous scan technology to sense marks, identified by ES&S as Intelligent Mark Recognition visible light technology which allows the ballot to be read in any orientation. The M650 uses discrete light sensors to detect markings in discrete channels (timing mark, code channel, and multiple data channels) that require the ballots to be read in only one orientation. The M650 is available with two different sensor sets: an older model used in some California counties is sensitive to infra-red light and a newer version sensitive to visible green light.

The initial election definition resulting from EDM contains no ballot formatting information. It creates a ballot definition file (.bdf) that will be imported to the ESSIM applications. ESSIM supports text formatting, ballot style information (size and positioning of information labels and voting positions for candidates and other voting choices), and other support to meet state and local requirements for ballot layout of contests, instructions, and ballot features. Alternative language translations (both visual and audio) may also be loaded and linked to the election definition in ESSIM. The Ballot On Demand (BOD) feature allows ballots to be printed directly (appropriate for small numbers of ballots) or the creation of Portable Document Files (.pdf) to be used by printing services provided by ES&S or through printing partners for bulk printing of ballots. Because of problems encountered during testing with differences between the election definition and the ballots, we did not test BOD. The .ifc file produced by ESSIM may be imported to HPM (along with necessary audio files) to provide election definition and ballot layout information for programming the ballot scanners. The local printing agents who are contracted to print the ballots may not be able to use the ESSIM ballot images directly. Once ballots are printed for an election, any shifts or changes in position for individual candidates resulting from manual layout procedures, original election definition errors, or late election changes will lead to incorrect tabulations if the election definition used for tallying the votes is not changed to reflect these alterations. (This is a problem which actually occurred in this certification testing.) However, the expense and timing can be prohibitive to go back and reprint an entire ballot run for minor errors. The HPM application design includes provisions for adjusting the election and ballot information to recognize such changes. The HPM data definitions are created and maintained separately from the EDM election definition files and do not update the ballot definition files prepared by EDM or ESSIM. The HPM election definition, rather than EDM's .bdf files, is used to import the election definition to the ERM to convert and report voting results from the ballot scanners. Note that a change made through HPM due to ballot changes may make the Ballot On Demand functionality risky as the ballot produced may not match the ballot scanner programming. A capability also exists to create subset elections that allow election definitions with different tabulation conditions that may then be merged back into the ERM reports.

The AutoMARK application is a separate development by AutoMARK Technical Systems, LLC, which has been adapted to process ES&S ballots. (ES&S recently announced its acquisition of AutoMARK Technical Systems, LLC.) The AutoMARK Voter Assist Terminal (VAT) system is categorized under the Federal election standards and guidelines as a ballot marking device. The VAT accepts ES&S unvoted ballots and, through a DRE style touch screen, supports the voter in selecting, reviewing, and correcting the voter's choices before the ballot is actually marked. Once the ballot has been accepted by the voter after a review, the ballot is printed and is hand carried

to a precinct ballot scanner (the M100) or deposited directly in a ballot box for central tallying operations (using M100 or M650 ballot scanners). The VAT specifically includes support for voters with disabilities under the Help America Vote Act (HAVA) and Americans with Disabilities Act (ADA) provisions. The VAT provides visual, enhanced visual, and audio presentations of the ballots and touch screen, accessible control buttons, and support for alternative assistive devices for voters requiring assistance in responding to choices in viewing the ballot and making voting choices. The capability also exists to insert an already marked ballot and verify how the ballot is marked under the election definition loaded to the VAT through the visual screen or audio ballot playback. The VAT does not record the votes electronically nor perform any vote tallying operation. The paper ballot is the sole record of the voter's actions on the VAT. The AutoMARK Information Management System (AIMS) application, which runs on an IBM compatible PC, can accept the .ifc file (plus some other files in the same directory as the .ifc) or other text files to create the election definition that is to be programmed in the VAT. Editing of the election definition is needed to add alternative language labels and all audio files. During testing, we also encountered problems that requiring careful editing in AIMS due to issues in importing the Unity election definitions. Like HPM, the capability exists to reprogram the imported election definition to make corrections and adjustments so that VAT will recognize, display/report and mark the voter's choices in the correct positions.

Qualifications

NASED Qualification

1. N-2-02-22-22-006 (Voting System Standard-2002), 31 Aug 2006 includes:
    a. Unity 3.0.1.1
        i. Audit Manager v. 7.3.0.0
        ii. Election Data Manager v.7.4.4.0
        iii. ESS Ballot Image Manager 7.4.2.0.
        iv. Hardware Programming Manager v. 5.2.4.0,
        v. Election Reporting Manager v. 7.1.2.1
    b. Model 100 Optical Scan Precinct Ballot Counter Firmware v. 5.2.1.0
    c. Model 650 v. 2.1.0.0 (Visible Red and Visible Green)
    d. AutoMARK Information Management System v. 1.2.18
    e. AutoMARK Voter Assistance Terminal HW 1.0 & 1.1/v 1.1.2258\

    Note: the NASED certification and ITA report do not identify Ballot On Demand nor report testing of Ballot On Demand ballots.

    Note: All components have changes from the prior certified versions under the prior California certification for Unity 2.4.3. The Model 650 with Visible Green sensors and the AutoMARK A200 components are new with this certification.

Findings

We used standardized benchmarked test elections based on a subset of the San Diego 2002 Primary and General elections updated with changes based on 2004 and 2006 elections to include the addition of the Presidential race in seven political parties. Three parties, American Independent, Democratic, and Republican, were defined as allowing Decline to State (DTS) voter participation and reporting with the Republican DTS not permitting participation in Presidential nominations. A third test, the Special Election, was based on the Governor's Recall election and is used to test special conditions requiring a large contest.

Phase I: Installation and Election Definition

The Unity 3.0.1.1 and AIMS applications were installed on desktop workstations located at the California SOS office in Sacramento. The desktops were reformatted and fresh installations of the Windows XP SP2 and up to date security critical updates and patches were completed. ES&S provided copies of some of the required Commercial Off the Shelf (COTS) software and other COTS components were added as part of the Trusted Build installation disks sent directly from SysTest, the Independent Testing Authority (ITA) who performed the NASED certification testing for these releases. The Trusted Install disk placed portions of Unity in directories in a directory one level down from what the actual programs required. . It is not known at this time if that was an error in the setup of the Trusted Install disk or a change in the new version of the system. The misplaced files were moved to the correct directory before the system could be used. Instructions for the installation were missing details including correctly identifying the COTS supporting software that needed to be installed (some listed software was not needed for the components to be installed in California). A set of installation instructions used in an older certification test were found that provided some of the missing instructions and the Unity 3.0.1.1 applications were finally installed so the election could be defined. The AIMS installation CD had not been created correctly and, again, the detailed instructions proved to be missing details needed for complete installation, in particular for the installation of MS .NET Framework and the MS SQL Server components that were part of the Trusted Build installation. The AIMS CD was replaced with a corrected CD from SysTest that installed without apparent problems with the information gained from the first install. We noted in the process of verifying the installed versions that three different versions of MS Office files were present (MS Office XP, 2003, and MS Access 2002). The scope of testing did not cover determining if this is a source of errors we encountered or whether this was part of the problem with the bad Trusted Install disk.

As part of creating the election definition, ES&S provided a copy of their proposed California Use Procedures. The Unity suite contains many options and features that are inappropriate and should not be used in California as well as others which are needed but were not immediately obvious to the user. The draft Use Procedures did not provide adequate guidance for California clients to anticipate and correctly select the necessary options. Later, this proved to be even more serious, when the transfer of the election definition to AIMS resulted in problems which required going back and making changes to the election definition. Among these problems were:

Device driver installation issues:

a. The Omni Drive used for write and read PCMCIA cards for the M100. The driver has to be <u>disabled</u> in the Windows XP Control Panel/System/Hardware/Device Manager in order to function properly.
b. The Omni Drive, once installed, has to be connected to the same USB port each time. (Note: The PCMCIA card driver in HPM does not use the standard Windows protocol but does a direct write to that port).

Election Definition Manager (EDM)

c. The “vote for two” contest was not identified as a “vote for two”. Although this was a testing data entry error, the initial error triggered other errors that proved hard to correct in HPM and AIMS such as missing write-ins and vote ovals.
d. The report of the Ballots Counted was not included in initial reports on the M100 and ERM reports. The EDM user manual warns that creating a new election from an old one does not reset the statistical counters that provide the required total ballots counted and ballots counted in each party. We discovered that this option also needs to be turned on in HPM.

ESS Image Manager (ESSIM)

e. One of the contests had a different spacing between candidates on one of the printed ballots than the others. This resulted in the position of the candidates below that position on that ballot being one position lower in AIMS than was defined in the imported definition. The offset applied only to voting positions lower in that column of the ballot where the offset occurred.

Hardware Programming Manager (HPM)

f. In HPM, we found we could create multiple election definitions for the same election (see earlier comment about sub elections) and needed care to correctly identify which election we were using. This will be more of a problem if multiple users are given access to the election definition.
g. In the Change Control File, the default entry for state was FL. Changing the default to CA did not reset all the options correctly. For this certification, the use procedures need to indicate that Modems and Data Acquisition Manager (DAM) are not activated. Note: California requires modems to be disabled. It is not clear to us and we did not have time to test whether this modem option would allow the modem to be re-enabled in the client jurisdiction.
h. Because of the potential of an election definition being modified, reports in HPM need to be identified as part of the official audit files to show if or where changes have been made from the EDM and ESSIM audit reports.
i. The sequence number for the Natural Law (NL) party was ten but needed to be input in hexadecimal (also known as base 16 math) Hexadecimal uses the numbers 0 to 9 and a to f. In base 10 math the value for ten is expressed as “10”. In Hexadecimal the value for ten is expressed as ‘A’. The sequence number was input as “10” which in hexadecimal is the value of sixteen. The error resulted in the two races between the NL and Peace and Freedom (PF) being switched. The field had no edit restriction to ensure that only hexadecimal values would be entered.

AutoMARK Information Manager (AIMS)

j. When trying to complete the Translation file (an Excel table showing which labels need translations that may be exported to a translation program or service) we had to manually create a folder where the Excel file would be written.
k. The tri-language labels in English, Spanish, and Chinese for the contest title and “Vote for” label were transferred from ESSIM to AIMS as a block text field and had to be deleted and manually entered to pick up the specific language translation needed. (A known problem with this version of AIMS.)
l. The AIMS application cannot mix double sided and single sided ballots. A dummy contest had to be added to AIMS in the Primary Election to ensure that both sides would be “read” on those ballots that only used one side. On a non-partisan ballot with only the measures on the back, all the oval positions had to be deleted to allow the dummy oval to be defined as the first oval and then vote ovals had to be replaced for the rest of the ballot. Although this could have been alleviated by a more intelligent ballot layout, the example shows an issue with inserting missing oval positions.
m. The indexing of the contests/candidates between ESSIM and AIMS was one off, requiring adjustments in AIMS. The first contest in AIMS begins with ‘101’, not ‘100.’ (A known problem with this version of AIMS.)
n. The AIMS Validate Data step warned that the count of target ovals defined did not match the expected number of target ovals for the contests on the ballot We found we had to manually add write-in ovals in three contests to complete the definition.

These problems also required unexpected changes in HPM since, once the ballots were printed, we could not go back and wait for the ballots to be reprinted. In the last week of testing, we did go back and step through the election setup a third time in sequence because of conflicts

in the election definition needed to read the ballots that these changes created between EDM, ESSIM, HPM, and AIMS

.

Security Controls

As part of the California Use Procedures, instructions for securing the system are required. In the draft Use Procedure provided by ES&S for this testing, a copy of the Center for Internet Security's (CIS) Windows XP Professional Operating System Specialized Security-Limited Functionality Benchmark Consensus Baseline Security Settings guideline was given as the recommended operating system "lock-down" setup to be applied to the Unity and AIMS workstation. Although that high level of "lock-down" of the operating system would be desirable in an election system, the actual use of the guideline recommended by CIS assumes careful testing by application developers or information security personnel to determine what portions of the checklist could safely be applied or adapted without denying the services and resources needed for the application to function. The level of effort to test the settings in the guideline and determine which settings may be applied is outside the scope and time allotted for this certification testing project. There was no evidence in the form of adjustments or instructions that ES&S had performed the necessary testing to apply the guideline at the level presented. As a result, we declined to setup the test environment to that level and instead applied only basic elements of the Legacy level of the CIS checklist, terminating only services that were known to be vulnerable and recommended by the Microsoft Security Program office.

ES&S largely depends on the basic Windows login accounts and physical and procedural security provided by the local client's Information Systems staff or equivalent to protect the Unity operations. The EDM/ESSIM, HPM, and ERM applications have separate access login options that use different designs. By default, they are not installed or enabled unless the client sets them. Audit Manager is designed to be the standard mechanism for the set up and management of the application login user IDs and passwords and audit logs. It must be installed and activated to provide application level user login and audit logging. Anyone with administrator privileges may enable or disable the use of the login user IDs or audit log in. The user IDs and audit logs are stored in a password protected Access database. Only EDM and ESSIM currently use Audit Manager in the system submitted for certification. The user account passwords are similar in complexity to the default Windows login passwords, which is considered a weak password scheme. See the Red Team and the Source Code Review report for more details on the effectiveness of this application.

HPM and ERM have different programs, UHPMMNGR.COB and UERMMNGR.COB respectively. Both require administrative passwords which are reset on entry to new passwords. These passwords cannot be blank but may be 1-16 letters, digits, or special symbols. In HPM, only a user id is created. The user id may be 1-3 characters, including leading blanks. There is no authentication to show the user id is used by authorized individual. The user id used to login is recorded in the audit log and printed in audit log reports to show who implemented the reported action. The user ids may also be disabled in the UHPMMNGR.COB utility. ERM user ids are set up just the same as the HPM user ids but also may be assigned limited rights to implement the least privilege needed to perform the task. Again, there is no authentication of the user's right to use that id and the entailed access rights. For the HPM (critical because it can be used to change the election definition) and ERM (critical because it has the functionality to change votes in the reports) the only protection from malicious attacks is restricting physical access to the workstation. See the Red Team and Source Code Reviews for further information on the effectiveness of the user id access control.

Phase II: Functional Tests

The elections defined in Phase I were installed to the ballot counting devices and a Logic and Accuracy test was run to verify the machines were operational and the test ballot decks were being read consistently. The test runs identified two of the problems reported above: (1) the switch between the NL and PF party contests, and (2) the lack of the total ballot count on the M100 precinct counter. Both these problems were errors made in the creation of the election definition that were not found until the machine count.

For the Primary, all the test decks were tallied on each of the three voting machines to detect differences in which votes were recognized on one machine and not necessarily on the others.

In the General Election, we scanned ballots that were marked by the AutoMARK VAT, the hand marked ballots, and a subset of the hand marked ballots that had been folded as if they were vote-by-mail ballots. Although the folded ballots were more difficult to scan and sometimes had to be rescanned, no errors in the vote count were found. Machine level, precinct, and consolidated summary reports from all machines were collected and checked against the known counts of the test deck. No errors were reported from the review.

Attachment A:

Test Equipment Inventory

	Category		
1.	Server/Workstation	**Unity 3.0.1.1. workstation**	**AIMS 1.2 workstation**
a.	Model	Cosair Orbit	Cosair Orbit
	Serial Number (S/N)#	1116598	1116602
b.	Processor	2.8 GHz Intel Pentium 4	2.8 GHz Intel Pentium 4
c.	Memory	1025 MBytes	1025 MBytes
d.	Hard Drive	Western Digital Caviar SE 40GB	Western Digital Caviar SE 80GB (partioned for 40GB)
	S/N#	WCAMA1775084	WCAM9H352265
e.	Other Drives	CD R/W	CD R/W
f.	Keyboard	Standard	Standard
g.	Mouse	HID/USB	HID/USB
h.	Other Peripherals	Iomega ZIP 250 OmniDrive USB Ver 1.0.0.1	ImageMate USB 2.0 Reader/Writer
i	Operating System	Windows XP Pro, SP2	Windows XP Pro, SP2
	Critical/SecurityHotfixes	As of 11/7/07	Only SP2
j.	COTS Software	Adobe Acrobat 7.0	MS Application Error Reporting Version 11.0.6560
		Adobe Distiller 7.0.0	
		Adobe Type Manager 4.1	
		Norton AntiVirus 2005	
		11.02 Virus update	
		RM/COBOL 7.50.1	
		COBOL WOW 3.12	
		PC Card Manager 1.3.0.0	
		Omni Drive Prof 1.72	MS Office XP Pro
		Crystal Reports 9.2.745	MS Office 2003
		MS Data Access Comp 3.525.22227	MS Data Access Comp 3.525.22227
		MS Internet Explorer 6.00.2900.2180	MS Internet Explorer 6.00.2900.2180
			MS Access 2002
			MS .NET Framework 1.1.4322
			MS SQL Server 8.00.760
k.	Application Software	ESS AM 7.00.0002	AIMS 1.2
		ESS EDM 7.4.4.0	
		ESS ESSIM 1.3.0.0	
		ESS HPM 5.2.4.0	
		ESS HPM User ID Manager	
		ESS ERM 7.1.2.1	
		ESS ERM User ID Manager	

2.	Voter Assistance Terminal (VAT)		
a	Model	ATS VAT A100	ATS VAT A200
b	S/N#: unit 1	AM0106430636	AM0206442639
	unit 2	AM0105491061	AM0206446128
i	Operating System	Windows CE 5.0.1400	Windows CE 5.0.1400
3.	Ballot Scannes	Precinct Counter	Central Counter
a.	Model	ESS M100	ESS M650
b.	S/N#: unit 1	201984	39077650 (Visual Green)
	unit 2	204283	31047138 (Infra-Red)
h.	Other peripherals		Two Okidata printers
i.	Operating System	QNX 4.2.2	QNX 4.2.5

The test workstation units used in Omaha were similar models but we removed and used the hard-drives from the Sacramento test units in the Omaha units to preserve the controlled install results.

The operating system and some COTS installs were default installs from commercial disks. We attempted to install under custom options with the intent to just install the components needed for the Unity and AIMS based on available install directions from ES&S . The Unity workstation Office install was a custom install but the AIMS unit was reinstalled later with a full default Windows install.. After the software installs were completed, some additional applications were found along with other components typically added from MS commercial install disks, The AIMS Trusted Build installations included other COTS files which were not part of the COTS installed files.