The Use of COTS
in the
EAC Voting System Certification Program

A White Paper Prepared for the
US Election Assistance Commission

By
H. Stephen Berger

I. Summary

Recent experience has called for a reexamination of the treatment of COTS, particularly COTS PC's under the EAC's certification program. In particular, three issues have arisen:

1. Vendor recommended specification of what may be considered equivalent COTS is often to broad and exposes the election system to undue risk. One example is a laptop that was submitted as part of a recently certified system. The laptop can be purchased with or without wireless capability. The version without wireless was submitted and so no testing was done of the version with wireless to determine its security. However, the verndor's specification for its customers did not specify that only the version without wireless should be used in the certified system.
2. It is not clear under the current VVSG when COTS is sufficiently changed so that it should be evaluated as a modification to the system before being accepted for use as part of a certified system. It was recently discovered that one of the first users of a newly certified system intended to run the system with a combination of server and operating system that the server vendor had never evaluated but when asked advised it believe would be unstable.
3. COTS currently accepted, pretty much as face value, without qualification as to its truly meeting the intention of COTS and particularly without alertness to the potential for interoperability issues between different COTS components. In a recent voting system submitted for certification a combination of server and operating system was submitted, similar to the one described above. The server vendor later advised that the combination was likely to be unstable. However, the VSTL, not being directed to be alert for interoperability issues, incorrectly diagnosed the repeated problems with the machine as being "the machine from Hell", replaced it but did not report the combination as problematic and no action was taken to warn election officials not to use that specific combination. Note that both products are reliable in other combinations but did not work well together. The vendor in question knew of the issue and advised its customers against using the troublesome combination but this information was not found by the VSTL primarily because they are currently not directed to be alert for such information.

This paper will evaluate the current state of COTS under the EAC's certification program and recommend mitigating steps that can be taken to minimize the risk to elections which retaining the significant value of using COTS components in voting systems.

II. Contents

III. History and Current Provisions

Under the NASED voting system certification program limited exemption from testing was provided for COTS products. For hardware, COTS was exempted from environmental and EMC testing. For software, COTS was exempted from source code review. Other than these exemptions COTS was required to undergo testing and evaluation as part of a voting system. These exemptions were documented in the 2002 Voting System Standard and were incorporated into the EAC program when it adopted that standard.

There is widespread belief that under the NASED and now EAC programs COTS was provided much wider exemption from testing but this is not correct. Of particular concern is the relatively common practice by vendors of not including COTS under their configuration management process, as they would for any other component of a voting system. This has lead to a wide variability in the COTS used with voting systems. This range of variability and the lack of version control over COTS creates risk for the election process and is generally unevaluated and unmitigated.

IV. Theory for COTS Exemption

This section sets forth the theory supporting COTS Exemption and then analyzes the practical realization of that theory.

IV.1. Basis

There are two reasons why it is believed that COTS may be exempted from some testing:

1. COTS is believed to undergo extensive testing, making additional testing redundant and unnecessary.
2. COTS is believed to have widespread usage, providing evidence from field experience of its adequacy.

Based upon these beliefs it is argued that an exemption from some testing is justified.

IV.2. Varieties of COTS

There are varieties of COTS, with very significant differences in their characteristics. This discussion will be restricted to COTS PC's but there are parallels and similarities with other types of COTS products. There are four categories of COTS that can be identified:

1. Special Qualification COTS

   Some products are qualified to higher standards or tested more thoroughly because they are marketed to programs that impose additional requirements. An example would be PC's sold to federal agencies. These PC's come under the Section 508 requirements for disability access and will be evaluated to those requirements. PC's that are not sold to federal agencies will not be required to be evaluated to these requirements.

2. Internationally Marketed COTS

   Internationally marketed COTS is the category that is usually thought of when speaking of COTS. These PC's are sold around the world and must comply with a variety of national and international standards and regulations. Additionally, they are used widely. Information from field data can be used to further validate the adequacy of a model.

3. Special Market COTS

   Special market COTS is developed and sold to a limited niche market. Accordingly there may be less testing and certainly will be less field data. An example of special market COTS would be a PC that is only sold in the US. There are not mandatory EMC immunity requirements in the US and so such a PC may not have been tested for its RF or power line immunity and therefore may be vulnerable to such disturbances. In contrast the European CE Marking requirements make EMC immunity mandatory and PC's that are CE marked will have been tested to requirements which are very similar to those in the VSS and VVSG.

4. Semi-Custom COTS

   It is very possible to have companies provide semi-custom COTS PC's. Many companies will allow the selection of a variety of components and will assemble those into a PC for their customers. While the individual components may be excellent and may have been tested, the resulting PC, built from those components will not have been tested. Further, such semi-custom will not be widely used and so field experience will not provide data based on widespread use.

V. Causes of COTS Failures

This section sets forth the theory supporting COTS Exemption and then analyzes the practical realization of that theory.

V.1. Wide Use

A key assumption with COTS is that it is commercially offered, widely marketed and used. Unfortunately some items are represented to be COTS when they are simply commercially offered. Some products may be commercially offered but only have actually been sold to a very few customers. In some cases equipment or software may

have been sold to only a handful of customers. In these cases the safety provided by wide use and a depth of field experience with the product does not exist.

V.2. Uniqueness of Voting Systems

Voting systems are required to meet demanding expectations for accuracy, reliability, security, accessibility and usability. Because of this they require somewhat unique specifications. Some products may be perfectly suited for use in many applications but fail to meet the expectations for use in voting systems. In these cases additional qualification may be necessary to determine that a component meets the needs of a voting system.

V.3. Interoperability

While many PC's, operating systems and software work together without problem, there is a long history of specific combinations that do not work together. A challenge when accepting COTS is that while the specific products and versions tested may work very well together not all versions may. The challenge for certification is to allow as much flexibility as possible but not so much as to expose the election process to problems that can occur when different versions are not interoperable.

Of particular concern is the possibility of combinations being used that the vendors do not recommend due to known issues. Recently it was discovered that the operating tested with one system was intended for use with a PC server. The server was not designed for use with a consumer grade operating system and its vendor recommended against use of that particular combination. In this case, two pieces of COTS, a widely used operating system and a server from a major computer manufacturer, each of which were fine products, in combination would very potentially have caused significant problems if used in an election.

Communication with the vendors can be a helpful source of information about these kinds of issues. Communication with COTS programs at other agencies is another source of information. When problematic combinations are identified there needs to be a mechanism for preventing its use in a voting system.

V.4. Modifications

Changes to COTS, both hardware and software, are an ongoing fact-of-life. There is relatively wide variability under the same model and version number but even greater variability between new models and versions compared to those submitted for testing. The modification process of the certification program offers a method by which there can be some independent assessment of new models and versions, to protect the election system from excessive risk, due to untested COTS being introduced into voting systems.

VI. Recommendations

The use of COTS provides valuable benefits for voting systems. COTS products offer lower cost and high quality than could be provided by custom products designed for exclusive use in voting systems. The reason this is true is that COTS products provide economies of scale and with that efficiency in pricing. Manufacturers of COTS serve the combined needs of many uses and spread the cost of research, product development and

manufacturing over a much larger number of units than could ever be the case for custom products used only in voting systems.

However, COTS can fail to meet the specific needs of voting systems. The following recommendations are offered as a means of mitigating this risk, while retaining the benefit brought through the use of COTS.

VI.1. COTS Qualification

COTS should be qualified to assure that it meets the assumptions of the COTS definition. Specifically information should be provided that:

1. The COTS equipment is not only commercially available but in wide use. Some quantification should be placed on what is meant by general availability
2. The assumption that the COTS has already been tested to requirements similar to the VVSG should be required. As an example the European CE mark requirements include specifications that are generally similar to the EMC and safety requirements of the VVSG. A copy of the Suppliers Declaration of Conformity for CE Mark would be evidence that the product has been tested to similar standards to the VVSG.

VI.2. Qualification of Field Data

A missing element in the VVSG is the ability to disqualify COTS that has a history of poor field performance. While this would not be used often, it is needed in order to allow the VSTL's and certification program to disqualify a component that has a poor performance history. Currently if a product is accepted as COTS it cannot be rejected, even if there is evidence that it has a history of problems.

VI.3. Similarity of Use

In some respects voting systems require levels of accuracy, reliability and security that exceed those for general use products. An example would be the computer operating system that must be hardened to a greater extent than most home users would apply. NIST has developed recommended security hardening procedures for the most commonly used operating systems. When these systems are used in voting systems they provide the required level of security only when properly configured and hardened. Hence, the use of

VI.4. Interoperability

When a system is certified there should be as much freedom for exchange of comparable components as can be allowed without exposing the election process to undue risk. Where the potential for interoperability problems exist, new versions, and combinations of new versions should be qualified before being allowed as modifications to the certified voting system.

Vendors of various hardware and software components can be very helpful in this regard. They often know what combinations may be troublesome and be willing to help the EAC protect election officials from introducing combinations of COTS that are not interoperable.

VI.5. Limits to Modification

The degree of variation within COTS components, software and hardware, should be clearly specified with each certified system. Changes that exceed these limits, should be considered modifications and receive an appropriate level of review by a VSTL.

VI.6. Communications with Vendors

COTS vendors have the potential to be valuable partners to the certification program. Establishing points of contact and a periodic dialogue with key vendors offers the potential for a rich variety of benefits. Vendors and notify the EAC of their product roadmap, allowing planning for evaluation of new models and versions, accepting them as approved modifications to the voting system, after appropriate review by a VSTL. Vendors can also assist in alerting the EAC to interoperability issues or other field data that may affect elections. A healthy partnership and two way communication offers many possibilities.

VI.7. Communication with other Agencies

There are a variety of COTS programs, particularly in the DoD. Establishing liaison with these programs and regular dialogue and exchange of information is another vehicle to help mitigate the risk of using COTS while retaining the benefits of its use.

VI.8. Reduction of Costs

The recommendations made above will require additional effort, increasing the cost of certification. It is therefore recommended that concurrent with the introduction of these measures there be a counterbalancing reduction of testing requirements that are proving to provide relatively lower value. An example of such a reduction might be allowing a voting system vendor to provide a declaration of conformance for certain low-risk environmental requirements, similar to the process allowed by the FCC for PC's and under the European CE Marking program. Requirement that would be candidates for inclusion under a vendor declaration of conformance would be those that have a history of seldom failing AND where the risk to an election of a failure would be minimal.