Testimony of Brian J. Hancock

EAC Public Meeting December 2, 2010

An Update on EAC Work Related to COTS Products as Used in Electronic Voting Systems

Introduction

Madam Chair, Commissioners, Executive Director Wilkey, General Counsel
Robbins: Thank you once again for allowing me to testify this morning. As
we all know, the use of Commercial Off The Shelf (COTS) products and
components in voting systems has been a concern almost since the
introduction of electronic voting systems 30 or so years ago. As voting
system manufacturers continue to integrate more and more COTS products
into their systems, these concerns have only increased. While we have taken
numerous steps forward in the voting system arena since the passage of the
Help America Vote Act, COTS remains an unresolved and frankly neglected
issue. I believe that we all feel it is high time to address COTS issues in a
systematic, inclusive and transparent manner. In the remainder of my
testimony I will outline some of the COTS issues and risks and propose a
solution for moving forward.

Review of COTS Risks

The good news, if there is any, for the voting system industry is that COTS issues, risks and mitigations are well known by other government agencies and industry, so we do not need to reinvent the wheel, as the saying goes. A few of the major risks that all COTS integrators and users face are worth discussing to get an idea of the magnitude of the work ahead of us. The following COTS risks were noted by the Federal Aviation Administration:

1. Rapid Change: The rapid rate of change in technologies and products, a direct consequence of the competition within the commercial market, means that new commercial products are released at a pace based on the speed of technology evolution, not necessarily on their continued usefulness to the acquiring entity. As a result, they are characterized by diminishing levels of product support.

To compound the challenge of managing rapid change, various types of products (e.g., processors, displays, power supplies, memory, etc.) have different market cycles. The products tend to be introduced at different times with varied service lives and are therefore out of phase or asynchronous with each other.

2. Different Obsolescence Impacts. When a COTS product is projected to be nearing end-of-life (EOL) (i.e., out of production) or end-of-service (EOS) (i.e., no longer supported by the manufacturer), the effects of these projected changes of state on the product and on systems using the product must be examined to determine what action if any is needed. It is not a foregone conclusion that all products declared to be EOL or EOS need to be replaced immediately. Obsolescence impacts vary along a wide spectrum all

the way from no impact – when a COTS product is considered reliable and there are sufficient spares (at acceptable prices, within the market or on-hand) to support the projected failure-driven demand over a pre-determined timeframe.

However, a major or high impact situation exists if there are no compatible replacement products or technologies available on the market. This situation typically calls for a major redesign or an integrated system change.

3. Higher life-cycle Costs. The fact that COTS product development costs have already been assumed by the manufacturer consequently lowers the front-end development costs of a COTS-based system acquisition for the acquiring activity. However, unless a risk management program includes proactive mitigation strategies specifically oriented towards COTS-unique risks, the initial cost benefits can be offset by the often more costly fixes of the risks that weren't effectively managed.

Cost considerations for a COTS-based acquisition strategy that need to be included as part of a total cost of ownership analysis include:

- **Inadequate planning costs** (Must adequately plan and budget for COTS)
- **Test and integration costs** (Testing, integrating and deploying COTS may be greater over a system lifetime than custom approaches)
- **Modification costs** (In some cases COTS products may need to be modified, which would void product warranty and support provisions)
- **Configuration management costs** (Acquisitions of COTS products are likely to have multiple configurations of the COTS product requiring rigorous CM process)

- **Continuous system engineering costs** (Constant need to perform market surveillance/investigation and to analyze obsolescence projections to determine options and limit impacts)

4. Multiple Configurations. During the course of developing and producing a COTS product, the manufacturer is subjected to constantly changing market availability of components and subassemblies. For example, one production lot of a COTS product can be functionally equivalent to the next lot but contain different components and subassemblies. If a COTS product contains firmware or if it is a software product, revisions can be made to subsequent product releases to correct deficiencies or to add unique features to enhance product marketability. A COTS product manufacturer **may or may not** elect to identify these configuration changes to its customers.

5. Different Quality Practices. Not all COTS products are created equal. While many individual COTS products from different manufacturers might satisfy a particular set of functional requirements, there can be marked differences from one product to the next. Differences in the components manufacturers choose to use, quality assurance practices, manufacturing processes, labor force composition, market share, product support, upward/downward compatibility, corporate longevity, etc. can all affect the quality and therefore desirability of the products that are offered for sale. The "buyer beware" maxim applies when choosing among apparently similar products.

These are only a few examples of the risk factors associated with COTS products as determined by the FAA. All of these and more are relevant to COTS in the voting systems arena.

Where do we go from Here?

So we know some of the risk factors associated with COTS. The question is how will the EAC go about the task of working with the election community to address these issues?

As a first step, I would propose that the Commission facilitate the first in what might be a series of COTS forums or roundtable discussions with all interested parties as early as possible in 2011. This initial meeting should include not only by election officials and voting system manufacturers, but we need to move outside our little elections box and also invite others to participate who have already moved well down the road to effective handling of COTS issues. These additional participants might include COTS manufacturers including folks like Dell, HP, perhaps even Microsoft or other software companies. More importantly, we should seek participation from other government agencies such as the FAA, FCC and perhaps some representatives from the Navy or from the Air Force. The purpose of the meeting should be threefold:

1. To develop a workable specific definition of COTS for the voting systems industry.
2. To discuss and expand upon the known risk factors related to COTS with a particular emphasis on specific risk factors that may be unique to the voting systems industry.

3. To ultimately work on the development of a series of workable COTS risk mitigation strategies.

This task will be neither quick nor easy. I am however confident that as a community we can work together to develop workable solutions to the issues presented by the use of COTS products in voting systems.