

## **Voting Systems Innovations Class (DRAFT)**

Prepared at the direction of the STS Subcommittee of the TGDC

June 26, 2007

This paper has been prepared by the National Institute of Standards and Technology at the direction of the STS subcommittee of the Technical Guidelines Development Committee (TGDC). It may represent preliminary research findings and does not necessarily represent any policy positions of NIST or the TGDC.

The Technical Guidelines Development Committee is an advisory group to the Election Assistance Commission (EAC), which produces Voluntary Voting System Guidelines (VVSg). Both the TGDC and EAC were established by the Help America Vote Act of 2002. NIST serves as a technical adviser to the TGDC.

## Voting Systems Innovations Class

This document is in support of the following TGDC resolution:

**Resolution # 03-06: Offered by Dr. Rivest**

**Title: The Innovation Class in VVSG 2007**

*To spur development of new and innovative secure voting systems, the Technical Guidelines Development Committee (TGDC) directs the Security and Transparency Subcommittee (STS) to include in the next iteration VVSG a new class of voting systems, referred to here as the “Innovation Class.” The TGDC directs STS to investigate high-level, guiding requirements for systems in this class for the purpose of providing system implementers with a path towards achieving certification to the next iteration of the VVSG. STS should also investigate approaches for reviewing, testing, and certifying systems in this class. These approaches could include convening a review board to review submissions and performing expanded open-ended vulnerability testing on systems submitted for certification.*

### 1. High-Level Requirements for Innovation Class Technologies

Since this is a call for research, the TGDC must be careful not to harm innovation by issuing entry requirements that might eventually prove inadequate, constraining, or irrelevant to a specific new technology. Hence the TGDC proposes the following minimal set of requirements:

- I. Technologies in the innovation class must be different enough to other technologies so as to justify expanded review, conformance testing, and open-ended vulnerability testing. In particular, it should be clear that the “standard” path towards achieving conformance is not appropriate for the proposed technology;
- II. A reasonable case must be made that deployment of the new technology does not present excessive logistical complexities. In particular, if the proposed technology is based on multiple interacting components (e.g. cryptographic key certification authorities, public electronic bulletin boards, smart witness devices, multiple holders of shared keys, etc.), then deployment of these components, interoperability testing, and control and maintenance of the various communication paths should not present insurmountable problems.
- III. A reasonable case must be made that the new technology does not present an excessive burden on election administration. More generally, the technology should help rather than hinder election administrators in their goal of producing timely, accurate, and trustable election results.

This paper has been prepared at the direction of the STS subcommittee. It does not necessarily represent any policy positions of NIST or the TGDC.

The above requirements are intended to allow early discarding of technologies that fall *outside* the intent of the innovation class. The TGDC also needs to issue positive guidance. That is, help researchers and developers understand what should be *in* the innovation class. This is the purpose of the following two requirements:

- IV. Technologies in the innovation class must meet the relevant requirements of the 2007 VVSG as well as further the general goals of holding fair, accurate, transparent, secure, accessible, timely, and verifiable elections;

The TGDC recognizes that these goals present conflicting challenges. For example, design choices that enhance security might adversely affect accessibility and timeliness. Thus the evaluation process leading to conformance should not be guided by excessively narrow criteria nor dominated by experts from a single field of expertise. On the other hand, safeguarding the legitimacy of the election process requires special consideration be given to security and transparency (both actual and perceived). Since there is no universal measure of security, the TGDC defines the following security requirement relative to existing voting technologies.

- V. A reasonable case must be made that the new system is, when taken as a whole, approximately as secure, transparent, and auditable as existing systems permitted by the 2007 VVSG.

In particular, the innovation process is not a back door by which vendors can get systems approved that are less secure than what is approvable through the ordinary process.

Requirements I-V are not “testable” requirements. Rather, they are guiding requirements to be used when evaluating new technologies. The proposed evaluation process for the innovation class is discussed later in this document.

## **2. Component Submissions**

The innovation class is designed to permit a wide variety of new types of voting systems -- some of which may already have been anticipated or currently be under development and some of which may be truly new and unanticipated. There are a number of voting technologies, at varying stages in the research and development cycle that would appear to fall under the innovation class. A common feature of these is that they enhance security by avoiding single vulnerability points. Since the threat model for voting systems often includes insider fraud or sabotage, technologies based on multiple (mutually distrusting) components have been considered. For example, there are products already in the market that purport to enhance security of voting systems by adding a hardware “witness” device to a DRE. The general idea is that fraud can go undetected only if all (or a significant portion of) components in the system are compromised. Even more tantalizing is the prospect that voters in the future may be able to verify that their votes are included in the final election tally. So called “end-to-end” voting systems aim to

This paper has been prepared at the direction of the STS subcommittee. It does not necessarily represent any policy positions of NIST or the TGDC.

provide this feature without causing the system to be vulnerable to voter coercion, or vote buying and selling.

These new directions in voting technology raise issues of

- interoperability of components; and of
- component certification.

Components in the innovation class might be an auditing device, a witness device, an on-line bulletin board, a mix-net, and so on. The TGDC proposes that the review process outlined below apply not only to full voting systems but, on an optional basis, also to functionality and interoperability of components thereof. Component certification shall not be enough for the component to be used in an actual voting system. Conformance of the complete system (e.g. a DRE plus a witness device) is still necessary. However, allowing component certification may help innovations obtain market access and encourage vendors to make their systems interoperable. Interoperability of data (perhaps through the use of a standard like the election markup language EML) and devices is important for any voting technology. It should not be acceptable, for example, that a DRE outputs audit data in proprietary format. Interoperability is expected to play an important role in the innovation class. This is because the TGDC expects most technologies in this class to be based on multiple mutually auditing components.

### **3. Innovation Class Review Panel**

The first question to consider in forming an innovation class program is, how will submissions be reviewed? It is unlikely that a submitter would submit a complete, innovative voting system to a test lab, with all VVSG requirements satisfied as appropriate. More likely, a submitter would submit a proposal that would have to be reviewed and approved before proceeding onto production of the innovative voting system. Thus, some form of review panel consisting of experts in voting, IT technology, usability, accessibility, etc., will need to be formed.

The TGDC also supports an open process. Reasons for this are the need to show transparency and to develop trust. Another reason is that the innovation class is likely to include technologies that are difficult to analyze. A considerable time is required in such an open process to find the right security assumptions and criteria, to allow full, detailed cryptanalysis of the proposals, to make a well-considered selection, and to carefully document the rationale of the selection(s).

### **4. Basic Entry Criteria**

The idea of an innovation class arose out of the TGDC's concern that adoption of a "software independence" requirement (TGDC resolution #06-06) could stifle innovation in the pursuit of voting technologies that do not necessarily use voter-verified paper records.

This paper has been prepared at the direction of the STS subcommittee. It does not necessarily represent any policy positions of NIST or the TGDC.

The TGDC recognizes that security is a proximate rather than an ultimate goal of voting technology. Ultimate goals are fairness, privacy, autonomy, accuracy, accessibility, timeliness, legitimacy and finality. Constraints on voting systems imposed by security goals are justifiable only to the extent they promote ultimate goals. Therefore it is recommended that the process of “reviewing, testing, and certifying” technologies for the innovation class be open to all proposals that satisfy the following:

- i) the proposed technology must be different enough to other technologies so as to justify expanded review, testing, conformance, and open-ended vulnerability testing. In particular, a reasonable case should be made that the “standard” path towards achieving conformance is not appropriate for the proposed technology;
- ii) the proposed technology offers prima facie evidence of supporting the ultimate goals of voting technologies.

## **5. Steps in Reviewing Submissions**

While there are many potential strategies for reviewing submissions, it would seem as if several stages of review would be likely, and the stages may vary depending on the technology submitted. The initial submission of a proposal would be the first round, then followed by one or more rounds of review.

The initial review is akin to any initial review of proposals in that it is designed to help filter out clearly flawed proposals, and offer guidance to the submitter regarding the rest of the process. At this preliminary stage the proposal would likely be a high-level description of the technology.

Subsequent rounds of review could be designed to become progressively more stringent and require more detailed information from the submitter. Multiple rounds of review would likely assist smaller or first-time vendors who may not have the resources to go directly from an initial proposal to immediate implementation. A public review of the technology should be considered, especially if the technology involves cryptography as used in an end-end cryptographic voting system. Particularly with cryptography, a public review would be highly beneficial in obtaining additional scrutiny and in developing public confidence in the approach.

Two likely final rounds of review would be (a) development of a prototype, and (b) submission to a test lab for conformance testing. Review of the prototype may involve expanding the review to include various security and usability expertise.

The criteria for lab testing should be the same as for voting systems falling outside the innovation class except that it should be complemented as follows: (a) the review panel or submitter should issue testing requirements, and (b) system documentation should inform labs of testing protocols that are appropriate to the new technology. These sets of testing protocols should relate to aspects of the technology that require testing not sufficiently covered by the general testing regime of the VVSG. It is anticipated that OEVT will be significantly augmented by these testing protocols.

This paper has been prepared at the direction of the STS subcommittee. It does not necessarily represent any policy positions of NIST or the TGDC.