# Voting systems innovations class.
# (DRAFT)

Prepared at the direction of the STS Subcommittee of the TGDC

March 10, 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.

# The innovation 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.

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, testing, certification, and open-ended vulnerability testing. In particular, it should be clear that the "standard" path towards achieving certification 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.

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 certification 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.

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 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 may be things like 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. Certification 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.

## Review Process

The idea of an innovation class arose out of the TGDC's concern that adoption of a stringent "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.

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

**Basic entry criteria**

i) the proposed technology must be different enough to other technologies so as to justify expanded review, testing, certification, and open-ended vulnerability testing. In particular, a reasonable case should be made that the "standard" path towards achieving certification is not appropriate for the proposed technology;

ii) the proposed technology offers prima facie evidence of supporting the ultimate goals of voting technologies.

The TGDC also strongly 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. An open process, with a series of open meetings and publications seems the right way to standardize a technology that the TGDC expects will contain complex security algorithms. 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). But the objective of voting systems where voters can know that their votes were properly counted is well worth the time, trouble and cost.

## *First stage in the review process:*

A proposal must make the case that the above basic entry criteria are satisfied. A decision as to whether a proposal passes this first hurdle is to be made by a FACA panel established by the EAC. This step will i) help filter out clearly flawed proposals, and ii) offer guidance to the proponent regarding the rest of the process. The latter task is more demanding in expert resources, but the TGDC finds this justified in that it is likely to make further evaluation easier/less costly. The panel may choose to contract out expert opinions (on security, usability, accessibility, etcetera) as part of this task. Additionally, expert opinions may be submitted as part of the proposal itself. The TGDC notes that the latter documentation may be used by industry to help make decisions regarding R&D funding.

At this preliminary stage the proposal is expected to be a high-level description of the technology. The panel need not evaluate complex mathematical proofs or statements of technical feasibility and may take such claims at face value. Similarly, the panel's report (for those proposals that are given the go-ahead) is expected to be a set of high-level statements (of the sort "it looks like the technology offers x and y, but we don't see how you plan to solve z").

## *Second stage in the review process (preliminary security assessment):*

The second step in the review process starts by submission of a detailed proposal to the review board. This proposal must

i) address all issues raised by the review board in the first stage;

ii) provide enough documentation and specificity to make a security evaluation possible. The TGDC singles out security as the critical component to be evaluated at this step because i) of all necessary properties of voting technologies security is the hardest to evaluate; and ii) market forces do not select for security properties with the necessary rigor (it does not pay to invest heavily in security analysis of software) and timeliness (the way the market is likely to operate is to filter out bad technology after it fails).

The review board shall commission a security report on the proposed technology. The report shall spell out the set of detected vulnerabilities in the form of threat scenarios (e.g. statements such as "this technology would allow voter coercion in the following manner"). The TGDC recognizes that security experts may not have the full range of expertise necessary to weight benefits (with respect to ultimate goals) against the danger posed by the threat scenarios identified in the security report. Analysis of risk, cost, and benefits shall include people with expertise in the social sciences, law enforcement (e.g. the Election Crimes Branch of the Department of Justice), election administration, and policy makers. Thus the review board shall include, or be able to obtain, expertise in these areas.

## *Third stage in the review process (public review):*

After passing the second stage of the review process, it is expected that the proposed technology be mature enough to be turned into a commercial product put forth by a specific vendor. In this stage the vendor shall provide a working prototype of the voting technology.

In recognition that the end "client" for voting technology is the voting population at large, a one year review period shall be allotted for public comment on and testing of the proposed technology. Granting appropriate public access to the technology is the responsibility of the vendor. All aspects of the technology shall be offered for public scrutiny and testing by specialists. These include usability, accessibility, and security. Small-scale pilot runs are particularly encouraged. Full performance data from these experiments should be made available to the review board as part of the proposal's documentation.

Requirements for public release of technologic specifications should be compatible with rules regarding protection of trade secrets. However, in cases where applicability of existing rules is unclear, public confidence should take precedence over protection of trade secrets.

Publicly available information shall include full specification of any new cryptographic algorithms and multi-party protocols. Security and correctness of such algorithms and protocols are extremely difficult to establish. Public review by the cryptographic community is currently the best evaluation method we have. To aid in this review, the vendor shall provide a high-level description of all algorithms and protocols, along with a precise description of their functionalities.

The review board shall have access to proprietary source code. The review board shall certify that the code implements only publicly available algorithms and protocols.

Public review can at any point in time result in a petition for the review board to discontinue consideration of the technology on the grounds that a serious enough security flaw has been found. A process for handling such petitions should be put in place.

## *Fourth stage in the review process (testing by labs):*

A proposal that passes the first three stages can be submitted for testing by EAC-accredited labs. The criteria for testing at this stage shall be the same as for proposals falling outside the innovation class except that it is to be complemented as follows: i) the review board shall issue testing requirements at each of the stages in the review process; ii) system documentation, as produced by the vendor, shall 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 VVSG07. It is anticipated that OEVT will be significantly augmented by these testing protocols.

## *Timing of stages in the review process:*

There are a number of possible ways to implement the four stages above. The first stage enforces entry criteria and offers guidance to developers. Guidance can arguably be offered outside a formal review process. In this case we can fold enforcing of entry criteria into the second stage, thereby collapsing stages I and II.

Stages III and IV can be performed in parallel with the proviso that accreditation requires both stages to be completed.

During public review (stage III) it may become apparent that minor fixes to a design are necessary. Full disclosure and documentation of any design change shall be provided to the review board. The review board shall extend the duration of public review according to the nature of the design changes. Whereas small fixes need not delay review, a radical re-design of the system shall cause the public review process to be extended for up to one year.