March 31, 2017

Mr. Brian Hancock
Director, Voting System Testing and Certification
U.S. Election Assistance Commission
1335 East West Highway, Suite 4300
Silver Spring, MD 20910

Dear Mr. Hancock:

We, the EAC registered manufacturers, are writing to you in response to several concerns about FIPS implementations and new systems that we have recently shared at both the Manufacturers Meeting and Department of Homeland Security meeting in March 2017. As you requested, we have considered the EAC's positions and have prepared a consensus response for your consideration.

In response to the EAC's position on the required use of a NIST-approved cryptography suite within the FIPS 140-2 program, we request that the EAC consider the following points.

Revise RFI 2012-05 by removing the applicability of requirement 7.5.1.b to private networked solutions.
A private network by nature does not share the same vulnerabilities as a public network and so the same protections necessitated by a public network are not warranted for a private one. The private network is controlled from end-to-end by facility and administrative procedures.

Reconsider the EAC's position requiring that the approved algorithm be implemented on an Operating Environment (i.e., Operating System and processor) that is listed on the FIPS 140-2 module certificate.
As we currently understand the EAC's position, a manufacturer would be required to implement a FIPS-approved cryptography module that is certified by the Cryptographic Module Validation Program (CMVP). This includes deploying the suite in both the exact software version and hardware environment as specified on the FIPS 140-2 module certificate, which would include specific operating system version, specific microprocessors, and if tested in that manner, specific hardware make, model, and version. If the manufacturer is unable to do so, then we would be required to have our solution tested by a FIPS certification lab at our expense or contract the originating FIPS 140-2 vendor to perform a maintenance release of their FIPS module to be inclusive of our Operating Environment. NIST has clearly stated in their "Implementation Guidance" a means for allowing level 1 FIPS cryptographic modules to be used in non-certified hardware and software configurations. This is commonly referred to as the "Portability Argument". All FIPS validated cryptographic modules provide a "Security Policy" as part of their certificate. This Security Policy clearly describes the FIPS configuration and operation of the cryptographic module. Such information should be readily reviewable by a VSTL. We request the EAC continue to recognize the FIPS 140-2 portability argument of commercially available cryptographic modules. Denying the FIPS 140-2 allowance to port

cryptographic modules onto platforms not specified on the FIPS 140-2 validation certificates will result in disproportionate maintenance and oversight costs for manufacturers and the EAC. Without the advantage of the portability argument, an inevitable security update to the Operating Environment would invalidate compliance, regardless of whether a cryptographic module was developed by a third party or by the manufacturers. If the EAC's intent is to reject the portability argument, then EAC guidance is required to understand how compliance is to be preserved when patches are necessary for manufacturers to maintain a secure posture. Operating Systems, microprocessors, and installed hardware are driven by a number of organizations (Microsoft, Canonical, Red Hat, Dell, HP, Intel, ARM – to name but a few) and these organizations development cycles are measured in months and are not (or may not ever be) reflected on a FIPS 140-2 certificate. Thus, configurations on the CMVP will exist for a few months at best, if they are not obsoleted during the proposed FIPS testing campaigns, which will be months in duration. In addition, we believe that the use of these crypto suites in this manner would not significantly improve the security of our solutions, especially when weighed against the cost. By removing the applicability of the FIPS requirement on private networks, we would be allowed to continue testing solutions as we previously have before the release of RFI 2012-05. Alternatively, by not requiring a full FIPS Validation, this would allow the manufacturers the flexibility to design solutions that are maintainable and cost effective for our customers. We would also caution that the vulnerability announcements surrounding FIPS cryptographic modules, which are public announcements, will need to be managed, and may have the unintended consequence of eroding the public's confidence in the voting process.

In response to the EAC's criteria for "New Systems" as communicated in email correspondence on October 24, 2016, we request that the EAC consider the following options (presented in the order of preference):

Retract the currently documented criteria for determining new systems and replace the determinations with a minimum set of criteria for all modifications, irrespective of the VVSG standard to which the system will be tested for conformance.

Continue to allow modifications and new systems to be tested for conformance against VVSG 1.0.
Instead of forcing new systems to comply only with the newer VVSG 1.1, require that when a system exceeds the threshold for "modification" and becomes a "new" system that it be subject to a full testing campaign – and allow such testing to be conducted against a VVSG version that is of the Manufacturer's choosing (either VVSG 1.0, or VVSG 1.1). ***Any previous certification testing (including hardware) would be evaluated to determine if it could be reused in the current certification campaign to eliminate redundancy.***

In the "Determinations," strike the line: "*any single instance resulting in greater than 20% new functional source code change*".

We believe that this threshold is arbitrary and does not provide a proper identification of the scope of potential modifications.

In the "Determinations," strike ambiguous language such as, "*Criteria for determining NEW systems include, but are not necessarily limited to…*"
Language that purports to name or identify essential items of concern that in fact remain *un-named* and *un-identified* do not serve the collective need for clarity in determining what constitutes a "new" versus a "modified" system; on the contrary, such ambiguity is effectively a blank check that invites subjective and potentially inconsistent decision-making, as well as inefficient planning for future designs.

In the "Determinations," strike the language allowing "States" to make decision on the classification of a system.
The authority to make decisions on the certification and thereby the testing of voting system resides solely with the EAC. We do not believe that it is in the best interest of the testing and certification program to have actors outside of the testing program make determination on how the voting systems should be tested.

Since the issuance of the new system criteria, the manufacturer's ability to effectively plan testing campaigns has been greatly diminished. In addition, these criteria, from our perspective, are likely to cause repetitive, costly, and un-necessary hardware testing. We understand and respect the need for the EAC to manage risk as it tests and certifies voting systems. However, the current determinations on "new systems" are counterproductive to the EAC's and the manufacturers' joint goals of supporting jurisdiction needs and their ability to conduct elections ***in a nimble, cost-effective manner***. And, most importantly, the parties that ultimately bear the adverse costs of these conditions are the very jurisdictions that purchase election technology, and that are supposed to ultimately be the beneficiaries of the EAC's election assistance.

It can be simply stated that systems that were designed and deployed to the 2005 VVSG are, in most cases, unable to meet the VVSG 1.1 requirements without substantial and costly re-designs and subsequent hardware update at the jurisdiction.

We are concerned that if the EAC makes it effectively impossible to modify older systems designed to earlier standards, the outcomes are likely to simply re-create most of the challenges of the past decade, namely: these policies will leave election administrators with old technology that has a bridge to nowhere; they will slow down the flow of new innovations, by creating disincentives to modify otherwise serviceable platforms; and they will raise costs for purchasing jurisdictions, by leaving them only with the option to buy all-new systems that can meet the new standards – *and* jurisdictions will also have to wait months or years while the manufacturers design systems to a "one-size-fits-all" single VVSG.

In contrast, by pursuing an alternative, more flexible course and retracting (or modifying) the determinations, in the specific ways described above, the EAC can return the testing and

certification process to a condition that will be less disruptive to the jurisdictions and election administrators that we serve. It will allow the manufacturers to continue to support our customers who may not have the funding to invest in a new solution, while still allowing manufacturers to design their platforms for the future, at a methodical pace. We are confident that by diligently working together, the goals of the manufacturers, the administering jurisdictions, and the EAC can be accommodated under a mutually acceptable solution.

We appreciate your considered deliberation on these proposals. If you have any questions or wish to have a follow-up conversation please do not hesitate to contact us.

Sincerely

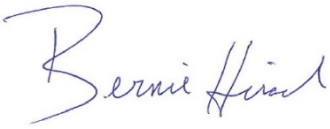
Ed Smith
Vice President, Product
Clear Ballot

Ian Piper
Director, Federal Certification
Dominion Voting Systems

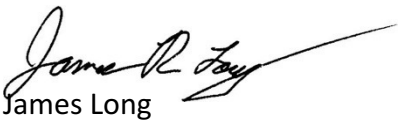
Steve Pearson
Vice President, Voting Systems
Election Systems and Software

David Wallick
Director of Certification
Everyone Counts

Pamela Cardenas
Certification Manager
Hart InterCivic



Bernie Hirsch
Director of Software Development and
Quality Assurance
MicroVote



James Long
Director of Certification
Smartmatic

Chris Ortiz
Director of Certification
Unisyn Voting Solutions

CC: Brian Newby, Executive Director
Cliff Tatum, General Counsel