Date	Commentor	Section	Comment
1/18/18	Kevin Skoglund	10.2-B	10.2-B – Indirect Voter Associations I think there needs to be a requirement for the proper generation of an indirect association identifier. The identifier must be: 1) unique (obvious but critical) 2) random 3) not derived using voter identity, ballot contents, voting order, or any date or time 4) generated by the voting system, not by pollworkers On #4, this could be generated either at runtime or pre-generated for activation devices. The main point being that humans are bad a picking random numbers and may be tempted to use a numbering system. There could be additional requirements to prevent human errors, such as "Must be alphanumeric," or "Must avoid ambiguous characters (0 vs. O, 1 vs. l)".
1/18/18	Kevin Skoglund	10.2-B.4	10.2.B.4: Encrypt uncast ballots "Ballots that are not cast, and contain an indirect association, must be encrypted." Should become: "Ballots that are not cast, and contain an indirect association, must be encrypted and must not be decrypted while an indirect association exists." Discussion: There should be no point in time, even fleeting, where a decrypted ballot has an association. * A ballot must be encrypted before a indirect association is recorded. * An indirect association must be accessible and removable without decrypting the ballot. A system should not need to decrypt data to locate the identifier. * When transitioning from an uncast ballot with an indirect association to an cast ballot with no association, the indirect association must be removed prior to the ballot being decrypted.
1/18/18	Kevin Skoglund	Under 10.2-B	I think there needs to be a requirement under 10.2-B for Indirect Voter Associations requiring that stored, but still-uncast ballots are signed. This requirement exists in 10.2-A.2 ("The voting system must digitally sign CVRs and ballot images.") but it is a requirement under Direct Voter Associations. It is not clear that the requirement also applies to Indirect Voter Associations. In this new requirement, it may be worth specifying whether it should be sign-then-encrypt or encrypt-then-sign. I would think "sign first", because it will be decrypted when the ballot is cast. The signature should guarantee the integrity of the original contents more than the integrity of the ciphertext. An attempt to re-sign it after decryption could present subtle vulnerabilities. It could be sign-encrypt-sign but that seems like overkill.

1/18/18	Bernie H.		I would submit that we should clearly define the following terms: Cast Recorded How would a paper ballot that is directly associated with an enclosing envelope containing voter information (name, address, etc.) that has not yet been cast be encrypted and decrypted? Are you suggesting some type of encryption technique is used to generate the paper ballot at home in order to meet this requirement? There can be no indirect association identifier generated by the voting system because the voting system doesn't know the identity of the voter.
1/19/18	Neal McBurnett		This whole concept of "indirect voter association" seems to be misguided for the reasons I wrote back in september: (Re: [VVSG-cybersecurity] Ballot secrecy), and adds complications.
1/19/18	Neal McBurnett	10.2-B.1	10.2-B.1 – System-wide Support of Indirect Associations All voting system components that capture ballot selections from a voter must be able to support indirect associations. means that the complications are mandatory, despite the "may" language in 10.2-B. It would be one thing to try to make these associations safe enough for consenting adults, despite the many risks and complications of bad implementations or even good ones. But it seems to me that to require all voting systems to support this is a tax on good practices to support the minority that need this for some purposes, and adds risk (even if very small) and complication (more substantial) for everyone.
1/19/18	David Wagner	Kevin's Comments	Agreed with Kevin's comments.
1/19/18	Bernie Hirsch	Indirect Associations	Thank you, David, for your comments. I would like to add to this discussion in one respect. I would suggest that "indirect associations" not be changed to "provisional ballots." If an alternate name needs to be picked I'd suggest coming up with something new like "non-verified ballots" or "delayed verification ballots." Provisional ballots have a legal meaning and would preclude other scenarios involving a delayed verification process. It's precisely because this is a commonly understood election term that some other more precise wording should be considered. Some examples, in addition to provisional, requiring indirect or direct voter association:
	Bernie Hirsch	Continued	1. Mail-in ballots (also called "Absentee"). Ballots cast via mailbox by the voter have not yet been verified and direct or indirect information must be allowed to be associated with the ballot until it's verified at some later date. Envelope obscuration (not encryption) during the days or weeks that the ballot is in transit and then in storage may or may not be an adequate method of guaranteeing absolute voter secrecy. Requirements and testing assertions related to security and secrecy should apply agnostically to this technology as well as any other technologies employed by the voting system. Future voting systems may require much better protections for paper technology. Examples could include a randomly generated number being assigned to each ballot envelope enclosure mailed out by the jurisdiction rather than requiring the voter to put their personally identifiable information on the obscuring envelope. Perhaps a future voting system would have a method for the voter to biometrically authenticate themselves and be issued a number at home. We just don't know at this time what may be required or advisable. The U.S. Postal Service itself may not always be in existence 5-10 years from now or considered a reliable ballot delivery method depending on voting system security and secrecy requirements.
	Bernie Hirsch	Continued	2. Absentee ballots. Overseas military, election workers and others may use other means of casting their vote (fax, email, etc). These must also be verified at some later date.

	Bernie Hirsch	Continued	3. Early ballots (called Absentee in some jurisdictions). Some jurisdictions require that the voter live continuously in their jurisdiction during the 30 days leading up to Election Day. Anyone casting a ballot before Election Day in these jurisdictions has not been verified until the actual Election Day and their ballot is subject to retraction. Other eligibility requirements may be in place applicable to vote retraction or acceptance for non-verified early ballots.
1/19/18	Jon Luning	Indirect Associations	I noticed that Kevin used the term "uncast ballots", possibly to mean the common (not legal) meaning of "provisional." That is, ballots which are subject to some delay before being included in those that produce a result. I don't see how the requirements I proposed pose any problems for mail-in ballots. I think the requirements that I proposed already allow the current standard practice for mail-in ballots (where the name is on an external envelope). I don't see any requirement that this practice would violate. If you see one, please point it out, so we can adjust the requirements. The intent of the proposal I made today is to allow the existing standard practice for mail-in ballots, where the voter's name is on an external envelope and isn't on the ballot itself.
1/19/18	David Wagner	Indirect Associations	My proposed approach does prohibit printing voter identity or voter IDs directly on the ballot itself. Are you suggesting that the federal standards should allow that? If so, I'd like to hear the argument for why that should be allowed.
	David Wagner	Continued	> 2. Absentee ballots. Overseas military, election workers and others may > use other means of casting their vote (fax, email, etc). These must > also be verified at some later date. I don't see the problem here. Jurisdictions that are using fax and email aren't using voting systems that undergo certification to the federal standards. If we're talking about building electronic systems to support overseas voters and the like (e.g., Internet voting), it seems like those systems could determine the eligibility of thevoter before accepting the vote, so I don't see why they'd need to retain an indirect association between the voter's choices and the voter's identity. So I think I'd need to hear a more specific use case that is prohibited by my approach and that you think shouldn't be prohibited, before I personally can perceive a problem with the current approach.
		Continued	>3.) Can we get some more specifics here, to talk about specific jurisdictions? Which jurisdictions are we talking about? Can you identify the jurisdictions that you are aware of that do early voting by checking eligibility only after the ballot is submitted, and that *don't* treat those ballots as provisional voting? Are you aware of any? I think many of us were surprised to learn of any jurisdictions that support retraction, and I understand there aren't many of them. At the same time I am aware that in many places that do early voting, those early votes are technically actually provisional ballots (e.g., because the state law has no explicit authorization for early balloting). In the few places that support retraction, are their ballots already technically treated as provisional ballots? Would there be any serious problems if for the purposes of the standards we considered those to be provisional ballots? What problem would that cause?

1/19/18	Bernie Hirsch	Mail In Absentee	No, I am not suggesting that the federal standards should allow voter identity to be printed directly onto the ballot itself. In answer to your first query, if the intent is to allow the existing standard practice for mail-in ballots, the following requirements will need to be adjusted: 10.1-A – System Use of Voter Information The voting system must be incapable of accepting, processing, storing, and reporting identifying information about a specific voter. 10.2-A – Direct Voter Associations The voting system must not create or store direct associations between a voter's identity and their ballot. 10.2-B.4 – Confidentiality for Indirect Associations Ballots that are not cast, and contain an indirect association, must be encrypted.
1/19/18	Bernie Hirsch	Continued	A paper based mail-in system accepts, processes and stores envelopes containing identifying voter information (name, address, etc.) directly associated with the voter's ballot (contained within the envelope). The process begins when the ballot is mailed to the voter, continues as the voter drops the ballot into a mailbox and it winds its way through a fairly insecure, uncontrolled environment (post office, drivers, storage locations, etc.) and usually ends when the ballot is verified and identifying information scrubbed (the ballot is irretrievably separated from the envelope many days later). The reason you identify the envelope as "external" is because it has an "internal," namely - the ballot. Think of it as the metadata encapsulating the data. There is a direct one-to-one relationship between the two sets of data. This would not meet two requirements (10.1-A and 10.2-A) as currently written.
		continued	The paper ballot is printed in plain text and has not yet been "cast." The term "cast" has yet to be clearly defined but "not yet been cast" might include the time it travels through public transportation systems (post office) and sits in storage in multiple places. My position is that "cast" takes place the moment the voter loses control of the ballot. Regardless, a paper ballot would not meet the encryption requirement (10.2-B.4). "Contain an indirect association" can be interpreted different ways, but I would submit that having one piece of paper "contained" within a second would establish a direct association with the voter's personal information written on the second piece of paper. Are you exempting a specific technology (paper device) from some of these requirements, and if so, on what basis? We have many "current standard practices" that haven't seemed to have made their way into the proposed requirements up to this point. That doesn't seem to be generally accepted as a valid reason.
		continued	The most obvious abuse of voter secrecy involves simply opening the envelopes and looking. If one wanted to be sneaky about it the envelopes could be steamed open and then resealed. We have been told that electronic databases stored in completely separate systems (voter registration vs. voting system) can't be trusted because a diabolical election worker could link the two together and "unmask" the identity of voters and their ballot selections. Well couldn't the same diabolical person simply open and reseal a few hundred envelopes? Couldn't a postal worker simply "accidentally on purpose" lose a few hundred from certain neighborhoods?
1/19/18	Bernie Hirsch	Absentee Ballots	OK, let's get specific. I can speak authoritatively regarding Indiana Statutory Code since our company presently supplies the voting system for 50 of the state's 92 counties. Indiana by law must use a system that has been tested to federal certification standards. No overseas, internet, electronic voting system could legally meet the requirement for determining eligibility in Indiana prior to Election Day. The following statute has been interpreted by members of the Indiana Election Commission to require an absentee ballot to be rejected if the voter hasn't continuously lived in their precinct during the 30 days preceding the Election Day.

		continued	IC 3-7-13-1Persons eligible to vote Sec. 1. A person who: (1) will be at least eighteen (18) years of age at the next general, municipal, or special election; (2) is a United States citizen; and (3) resides in a precinct continuously before a general, municipal, or special election for at least thirty (30) days; may, upon making a proper application under this article, register to vote in that precinct. As added by P.L.12-1995, SEC.22 Indiana also has a law requiring living early or absentee voters to remain living all the way through Election Day, although the state Senate has just passed a measure repealing that provision, which could very well become law in the near future.
1/19/18	Bernie Hirsch	Early Ballots	It would cause the problem of "confusion." A provisional ballot has been defined in Indiana code. § 3-11.7-1-2 (b) A provisional ballot must indicate that the ballot is a provisional ballot and not an absentee ballot. There are numerous laws covering what a provisional ballot is and how it is to be handled. This is completely separate from an "absentee" ballot, which has its own exhaustive rules and regulations.
1/20/18	David Wagner		> Discussion of the processing of mailed absentee > ballots represents a substantial expansion of scope that I believe most > states would object to. Agreed. Election processes and procedures are beyond our scope. Thank you for helping to keep us focused on our scope and mission. > If you want to capture the concept > without the legal entanglement, you could call them "conditional" > ballots. OK, thank you for the explanation of why using the term "provisional" is not a good idea. That makes sense, and that sounds like a good solution to me.
1/20/18	Bernie Hirsch		Calling them "conditional" makes perfect sense to me as well. It's great to hear that election processes and procedures are beyond the scope of requirements! We certainly had numerous requirements related to processes and procedures when going through our V1.0 certification, some related to security and secrecy. In addition to electronic DRE's, our system uses a paper-based absentee ballot scanning system. Here are just a few of the many hundreds of these "discrepancies" that we needed to address related to functional processes and procedures. Note: sometimes the testing lab would combine several requirements which when taken individually do not require enumerated processes or procedures, but when taken together do.

1/20/18	Nelson Rosario		This may be a dumb question, but who is the intended main beneficiary group of the standards? Voters, government agencies, or vendors? That is, in the event of a conflict of interests who should win out?
1/20/18	Kevin Skoglund		We all agree (I think) that cast votes should be 100% anonymous. However, there is also a common category of ballots which: * have left the voter's control * are either in transit or being held by election officials * are not yet irrevocably cast votes * require eligibility determination * include identifying information about the voter This category includes provisional, absentee, vote-by-mail, drop-off, early, and military ballots. It may include some cryptographic E2E systems. It includes all ballots in jurisdictions where law requires that a ballot can be revoked if the voter's eligibility changes before the polls close.
		continued	I think of these ballots as being in purgatory: standing at the gates, awaiting judgement. In our search for a common terminology, we might refer to them as "uncast ballots", "conditional ballots", "provisional ballots", "delayed ballots", or "un-adjudicated ballots". There is a security trade-off in allowing this category of ballot, regardless of whether they are physical or electronic. We do not get to choose whether to allow them--state laws have already decided they must be allowed. So our goal should be to assess the potential risks and thoughtfully mitigate against them. We must also recognize that we can not eliminate the risks entirely. Some level of risk is inherent.
		continued	One solution, proposed on our call, is to disallow any electronic storage of these ballots. The argument is that human-supervised procedures are better at protecting the confidentiality, integrity, and availability of these ballots before, during, and after adjudication than an electronic machine. Instead, these ballots would be stored in security envelopes with the voter information attached. Additionally, by moving the ballot out of the "voting system", a system can more easily comply with Guideline 10.2 (Never associate the voter's identity with the voter's selections.). Human-supervised procedures are not inherently better. The risks are just different. Encrypting an electronic ballot is similar to putting a physical ballot in a security envelope. Both are concealed from view. Both have voter identities attached. Both have a risk of being mishandled, revealed, altered, or destroyed.

		continued	Personally, I prefer electronic storage. Encryption is better at protecting the confidentiality and integrity of the ballot than a security envelope. Electronic storage can offer better access controls. A machine can decrypt and cast the ballot without any temptation to peek at the selections. And our governing body has much more control over the security of the machine than we do over local administration and procedures. Both have risks but I think the risks of electronic storage are less. It is reasonable to ask if associating a voter's identity with a chunk of encrypted data via an indirect identifier (a foreign key) violates Guideline 10.2. I would argue that it does not as long as the indirect identifier is not attached until the ballot is encrypted and is removed before the ballot is decrypted. I can also see why others might disagree. But as many noted yesterday, it is less of security risk than a vote-by-mail system, which we allow and which associates a voter's identity with the ballot in an even more direct way.
		continued	I disagree with the notion that physical ballots better comply with Guideline 10.2 than electronic ballots. Cybersecurity is not well served if we push security issues outside of our purview so that we do not have to address them. The risks are still there, and are possibly worse. The overarching goal of the guidelines is to increase security in the voting system. Pushing them out of the system does not do that.
		continued	I am not naive about the risks of ballots being decrypted. However it is not a trivial hack and I am comfortable with the indirect association in the most recent draft as a way to "air gap" the voter identity. Suppose a hacker can access the machine, bypass access controls, obtain the private key, and decrypt the ballot. They would also need to exfiltrate the ballot through a display or data port and then be able to match a random identifier (e.g. "H5F978V2M7") to a voter's identity outside the system, such as in the pollbook or written down in the polling place. Someone noted the possibility of keeping a database of identifiers. We can and should disallow any such database from ever interfacing with the voting system to maintain the "air gap". We have not removed all risk, but we have mitigated it.
1/20/18	Jon Luning		This is well-stated, and for purposes of risk understanding, this class of "intended to be cast"/"purgatory" ballots should be explicitly defined, and treated distinctly. From a security and risk mitigation perspective, a recommended (required?) practice might be to ensure that ballots in this class are fully isolated from cast ballots (i.e. are not included within the same system/storage), and that the transition of these ballots into cast ballots is performed in a manner that irrevocably removes any direct or indirect link between the ballot and the voter.
1/20/18	Bernie Hirsch		We configure our system in Indiana to have “absentee” DREs that are used prior to Election Day. Either the activation device or the poll worker creates an indirect association identifier with the voter (could be a randomly generated number used by the voter registration system). It would not be unusual for tens of thousands of conditional ballots to be “cast” on these machines over the weeks leading up to Election Day in each county, which are completely separate from the Election Day DREs (and each other). These conditional ballots are extracted from the individual absentee machines and then election officials retract any ballots (using the foreign key lookup) based on state law. Typically they have a printout or some other completely “air gapped” report telling them which ballot foreign keys out of the thousands recorded must be retracted. Once that operation is complete we insert the eligible ballots anonymously into the data containing the Election Day ballots while scrubbing out the foreign keys. Our paper based absentee ballots are essentially handled the identical way, but instead of an electronic foreign key we use an obscuring envelope which is separated from the ballots prior to the ballots being scanned into the final anonymous Election Day database.

		continued	So initially these ballots (whether paper, electronic, or some other medium) are fully isolated from cast ballots. At some point they must be “transitioned” into the anonymous data. Perhaps you could suggest some of the possible methods for mitigating risk while doing this with electronic records that must at some point cross over to their anonymous Election Day brethren? For our system we have avoided using any network connected devices or removable storage and instead physically connect each absentee DRE to a single standalone server using a short data cable specifically for this purpose. Would keeping the ballots encrypted until after the identifier has been scrubbed be sufficient? Would we be able to store these encrypted conditional ballots with the foreign key for possible use in an audit or should they be deleted permanently once scrubbed, decrypted and posted? Keep in mind that state law might dictate some of these storage requirements (where and how).
		continued	Currently in our other states we don’t need to create these foreign keys for early voting (other than for paper-based absentee ballots which have a direct association to each voter) but that doesn’t mean some state law won’t be amended or revised to require it at some point.
1/21/18	Carl Hage	10.2-D	Note, as a highlight (in case you don't want to read my long message. I disagree with "10.2-D – Prohibition on Voter Record Order Information". It should be allowed to have a voting system that has ordered ballot and CVR data (with restrictions on recording order of voter appearance).
		Ron Rivest Principles	R.E. Ron Rivest's base principles, #3 *[privacy]: The system shall lose track of the association between a voter's choices and a voter's identity. This really leads to 2 sub-principles: a) It is not possible to determine the votes of a specific person b) It is not possible for a specific person to prove the way they voted [Both are required by law, depending on the state-- your vote must remain anonymous, and you can't prove (sell) your vote.]
		Definitions	There seems to be a basic problem of definitions, e.g. "voting system", "access", "indirect association". Maybe they are defined elsewhere, but in this context there are some problems. The discussion here on the "indirect association" has been good. These words need to be defined and only referenced in the context of "uncast ballot" or "deferred cast ballot" or similar. [It would seem that the term cast is better than "delayed verification ballots."] I'm not certain of the definition of "cast", but I assume that is a point where votes are irretrievably submitted and association with a voter is lost. The term "voting system" is ambiguous. I would assume system means the whole process-- both validating voters to collecting and processing cast ballots. So section 10.1-A seems contradictory. I presume this should mean, the parts of the voting system that records, stores, or processes cast ballots cannot record voter identification.

Cast Ballot Order	There are several sections related to cast ballot order. I presume the issue is privacy. The issue is not being able to determine voter identity in a cast ballot by associating voter order with ballot order. If you are going to restrict electronic CVR order, then paper pallot order should also be randomized, e.g. there must also be a requirement to shuffle ballots in a ballot box. I think restricting ballot order limits security, reliability, and auditability, and is incompatible with existing voting systems, e.g. paper audit trails printed on a roll of paper. Another approach is to insure the time and order of appearance of voters is not recorded. It would be best to state order restrictions in terms of a privacy requirement explicitly, e.g. "It should not be possible to associate a voter's identify with cast ballot by order-- either the time and/or order of appearance by voters must not be recorded, or cast ballot order must be randomized. Randomizing cast ballot order means paper ballot order must be physically shuffled, and there must not be any means to determine the ordering of electronic CVRs, including time-stamps, file naming, ID, physical storage location, or file system IDs (e.g. inodes).
continued	The rules in the current BallotSecrecyRequirements only address some of the issues involved with recording CVR order-- better to eliminate them and apply a more general rule, listing the individual methods as examples. With some extra software complications it is possible to create cast ballot IDs and record CVRs in a random order, but it is not trivial, and there may be some reliability issues, e.g. the CVRs might need to be stored temporarily in backup storage in case the machine fails. I think cast ballot order should not be restricted-- it significantly impacts security, e.g. by prohibiting chained cryptographic bashes, and complicating the audit process.
Metadata	There seems to be incompatible restrictions on encryption, e.g. 10.2-A.1 says cannot and 10.2-G says must be. Also, 10.2-G says "metadata" which is ambiguous. I would think metadata must be public and also digitally signed. It is as important as CVR and image data. But maybe what I think of as metadata is different.
10.2-F	"10.2-F – Non-Memorable Identifiers & Associations" seems incompatible with end-to-end verification. I don't think it should be a requirement.

1/21/18	Lynn Garland	10.2-B.4 Carl	10.2-B.4 requiring encryption presumably applies only to deferred cast ballots submitted electronically. The wording probably should be: Ballots that are not cast, and contain an indirect association, must be encrypted or physically cloaked, e.g. in a vote-by-mail envelope. Electronic submission of provisional ballots is complex, and might need a whole set of restrictions. Probably, there should be an assumption that uncast encrypted ballots can be stored indefinitely, therefore to maintain privacy, the key used to decrypt and cast a ballot should be destroyed afterwards. It's not clear to me how to insure the integrity of decrypted anonymous cast ballots as being derived from the cloaked uncast ballots with indirect voter association. How can "the recording order of voter appearance" be restricted, since that information is generally within the poll books and outside the voting system, right?
1/21/18	Carl Hage	lynn	Are poll books outside the voting system? The non-electronic poll books I've seen have paper listings marked with a pen. The time the voter is checked off isn't recorded-- it's just a mark with a pen through the name. I suppose one could have a video camera to record a person entering, but then you could have a video camera above the poll booth too. The issue is if voter order can be correlated to ballot order. An electronic poll book would need to record if a voter has cast a ballot and/or entered the voting system, but without a time-stamp.
1/26/18	David Wagner		Well said. I think we should make the irrevocable transition required rather than recommended. Can we think about what requirements we need, to ensure that the transition is irrevocable and does not allow to later reconstruct the linkage to voter identity? Kevin's suggestions seem like a good start, but I suspect we might need some more requirements, to make sure that after the transition occurs it is not possible to subsequently obtain both the encrypted ballot and the decryption key and the indirect eligibility identifier even if the system is later breached. Can anyone suggest requirements that would ensure this?

1/26/18	Carl Hage	continued	Perhaps we can create two requirements: 1. All copies of the encrypted ballot and indirect identifier must be securely erased at the time when its status is determined (and it either transitions into a cast ballot, or is rejected as ineligible). 2. After all such conditional ballots have been processed and their status has been determined, all copies of the decryption key must be securely erased at that time. We'd probably add some other requirements. We should require that a separate public/private key be created for each election and used solely for encrypting conditional ballots. The private decryption key should be stored only on the central equipment that is used to process conditional ballots (and not on all voting devices). Before the election processing is finished / closed / before the election is certified, the private decryption key must be securely deleted. The voter should be made aware that they are casting a conditional ballot. What other requirements do we need to make this approach work well? Any thoughts? > 1. All copies of the encrypted ballot and indirect identifier > must be securely erased at the time when its status is determined > (and it either transitions into a cast ballot, or is rejected > as ineligible). It doesn't seem feasible to erase an encrypted indirectly identified ballot. [People have tried to destroy digital evidence, only to have it recovered from a backup somewhere.] I think you'd need to rely on the decryption key being destroyed. With a key stored in hardware (chip), the hardware can be physically destroyed as well as stored securely. But then there is the issue of validation. How do we know the decryption software doesn't insert fake ballots? If it's extracting paper from an envelope it's an observable process. Electronic-only seems like it would require some sort of voter verification or collective hash.

1/29/18	Kevin Skoglund		As Bernie, Carl, and David noted, the transition from a provisional uncast ballot to an anonymous cast vote is a particularly vulnerable point in the process that deserves attention. I would offer two thoughts: 1. The indirect association must be removed before the ballot is decrypted. This removal must be complete and irrevocable. No copies may be kept. I do not think it is our role to engineer a perfect system or provide detailed specifications. For example, I don't think we need to specify that the private key must be handled or destroyed in a particular way. The guidelines can leave room for different implementations, as long as they meet the goal that the removal of indirect associations is complete and irrevocable.
		Continued	2. The system must generate a digital signature of the ballot contents before encryption. The signature should be attached to the data or stored in a structure like a hash chain where it can't be altered (or both). After decryption, the signature should be verified before the vote is cast. This prevents software from inserting a fake ballot. It does not prevent a total hijack of the software, but that's true for all ballots in the system and is the reason for VVPT and audits.
		Continued	To me, the trickiest bit is how to handle integrity failures. If the system must confirm the integrity of the data against the digital signature, then it must be prepared to handle a negative result as well as a positive one. What happens to the ballot? The system can't let it be cast but can't just silently reject it. Does the system notify administrators? What does an admin do with the ballot? What do they do with a machine that just failed a ballot-integrity check? Maybe the folks who have worked on cryptographic systems have thought decryption-integrity error handling through already... it seems like a common problem with encryption.
1/31/18	John McCarthy		I understand that some vendors are pushing BMD's (and Hart is even still selling DRE's), but it seems to me that relying on BMD's rather than old-fashioned voter-marked paper ballots (with envelopes for conditional ballots like mail-in and provisionals) are an unnecessary expense as well as another potential threat to election security. As Rebecca Wilson has pointed out very well, Maryland's "local election directors rebelled at the idea (of all BMD's) because they realized that it takes each voter much longer to use the ExpressVote than to mark a paper ballot and they feared long lines in the polling places, which they have not seen since we switched to hand-marked paper ballots -- EXCEPT at the ExpressVote machines. Not to mention the expense of owning and maintaining so many machines, which they did not bring up."

1/31/18	Bernie Hirsch	Continued	I'm concern that some members of our VVSG cybersecurity working group are arguing that electronic voting systems need to be able to maintain "indirect" associations of voters with "conditional" ballots (e.g., provisional, signature mismatch, and perhaps end-to-end internet voting systems), despite the TGDC principles and guidelines adopted at the Sept 2017 TGDC meeting that clearly prohibit such associations, as follows: "10. Ballot Secrecy The voting system protects the secrecy of voters' ballot selections. 10.1 Ballot secrecy is maintained throughout the voting process. 10.2 The voting system does not contain nor produce records, notifications, information about the voter or other election artifacts that can be used to associate the voter’s identity with the voter’s intent, choices, or selections." There seem to be two main drivers for Indirect associations: (1) BMD vendors who want sell all electronic (i.e., DRE) systems, and claim that such system must be "equal" to systems that can easily protect ballot anonymity of conditional ballots using envelopes and paper ballots. and (2) future end-to-end internet voting systems It seems to me that (2) is far enough out in the future that the TGDC could reconsider the high level Ballot Secrecy principals and guidelines at such time such end-to-end systems begin to look likely for practical use, and that it is not worth opening the pandora's box of "indirect associations" to accommodate a few vendors who want to sell all electronic systems rather than using paper ballots and envelopes for conditional ballots. This doesn't seem likely for compromise The TGDC Principles and Guidelines adopted in September would appear to disallow paper ballots being stored with direct voter information in an enclosing envelope. 10.2 The voting system does not contain nor produce records, notifications, information about the voter or other election artifacts that can be used to associate the voter’s identity with the voter’s intent, choices, or selections." The enclosing envelope contains information about the voter (name, address, etc.). The ballot inside the envelope contains the voter’s intent, choices, and selections, and is physically associated with the enclosing envelope. If direct (or indirect) associations for paper ballots are not allowed, how would a paper-based system handle conditional ballots (like an absentee mail-in system)? I’m curious. How are paper ballots, voter verified paper audit trails, etc. going to meet accessibility requirements? How would people with vision, dexterity or other disabilities vote unassisted using “old-fashioned voter-marked paper?”
1/31/18	Whitney Quesenberry		Surely you are not talking about disallowing ballots marking devices. First, this would be in conflict with the ability to provide accessible voting systems for people who need them — including the many people for whom “old-fashioned” voter marked paper ballots are a return to days when they could not vote privately and independently. Second, it ignores the real value of being able to use a computer system to mark and print a ballot, including error correction, the possibility of a meaningful review before casting, support for languages without the cost of printing ballots in advance, support for people with low reading literacy, the cost of printing non-standard (and somewhat ineffective) large-print ballots, and fewer opportunities for the many ways that paper ballot design can fool voters into marking a ballot in a way that does not match their intent.

1/31/18	John McCarthy		No Whitney, I certainly was not arguing against Ballot Marking Devices in general. I was arguing (1) against all electronic BMD's that do not produce any paper whatsoever and (2) against BMD's that only produce light weight paper with voter choices as text but bar codes that are used for tabulation and defined to be the ballot of record. and (3) in favor of BMD's that produce ballots that look like vote by mail ballots with circles or rectangles filled in that can be read by scanning tabulation equipment and scanning equipment that can read back voter choices via an audio device for visually-impaired voters. (3) is preferable not only because it can be "read back" to visually impaired voters in privacy, but also because it preserves ballot anonymity much better if all ballots look the same, it makes it easier for all voters to confirm their selections in context (see Marilyn Marks examples), and it is much more secure than all electronic systems.
	Whitney Quesenberry		1. I don't understand what a "BMD that doesn't produce any paper" is. The definition of a BMD is that it's an electronic interface for making selections and then casting a ballot. 2. I think you are talking about VVPATs - a good example of how even good goals can produce terrible design. 3. The only devices I know of that read voter choices back from a hand- or machine-marked ballot are another BMD. OK, but not ideal. And it means that to create a device-independent voting experience, there must be 2 of them in the polling place or vote center. We're going to have to agree to disagree about whether producing something that looks like an optical scan ballot is really more readable. I take your point about not having ballots look different, and I understand your interest in this for auditing, but I think it's equally important to make sure that people can actually mark their ballot to reflect their intent. There are so many ways that people can misread a poorly designed optical scan ballot. We do our best over in the HFP requirements, but since the ballot design is out of scope for the VVSG - we can only require the capability to produce a ballot with certain characteristics - it's hard to use the VVSG to ensure that they are well designed. How I wish that we could simply point to the EAC's best practice paper ballot designs and say "make it look like that!"

Comment Status	Udpate By

The main beneficiaries are the local and state jurisdictions that are eligible to purchase certified voting systems using federal tax money. This means their state and local tax revenues can be reduced or used for other purposes which presumably benefits citizens. The other beneficiaries are the federal agencies that manage the certification program and grants, vendors who receive contracts for election products and services and voters who use these “upgraded” systems.	Bernie Hirsch

Epollbooks are mostly outside the certified voting system. The only part of epollbooks that are included is ballot activation. For instance, the Diebold Expresspoll 5000s create a voter access card, which is provided to a voter, which they then inserted into a Diebold touchscreen unit.	Josh	