No.	*Issue*	*Counterpoint 1*	
1	Browsers are not interested in distinguishing OV/DV as they don't see any relevance	Browsers aren't the only constituency. This would assist those that report on cert data and other relying parties that want to distinguish	
2	There would need to be a new OID every time the BRs were revised	The section of the BRs that deals with this is rarely (if ever) changed. If this were relevant, then it would be equally applicable to EV Certificates. Plus, because of the infrequent changes to this section, approximating issuance date by notBefore yields sufficiently reliable results.	
3	CAs would need to re-do their certificate hierarchy as policy OIDs are inherited	Yes, some CAs would have to do this. No one is saying we need to implement this intermediate change today but starting now and asking CAs to re-do their intermediates when they expire or are updated would put things in place for the change. In addition, many CAs use an anyPolicy OID or omit policy OIDs in their intermediate, significantly reducing the number of certificates requiring reissuance.	
4	We've established that there's no 'uniform' definition of what constitutes OV, only that the BR requires certain vetting steps for certain subject fields that are OPTIONAL.	One of the purposes of the BRs was to declare a homogeneous method which all CAs could adhere and be audited against. OV/DV certs are now done using the same principles at all CAs. OV certs contain validated org information which DV certs do not. The optional component is a non-issue since the OID indicates the optional fields are included.	
5	Interested Parties can already tell the difference between and OV and DV cert by looking at the O field	Because of the large number of 5-10 year certificates, determining what constitutes OV v. DV is very difficult. Many of the older OV certs included O	

		information. An interested party can't use the notBefore date to determine whether the certificate was OV/DV when issued since the notBefore date does not reflect the actual issuance date. Depending on how CAs operate, CAs not present for the previous CAB Forum discussion may still reissue certificates after the effective date of the BRs with the same error as previously issued certs. Certs issued by CAs outside of the BRs (with an O field, but not BR compliant) are not readily detectable.	
6	Validation of the O field is inconsistent between CAs, making the information in the O field unreliable	The BRs unified the procedures that required all CAs to use government records or ID document to verify the O field. The differences that still exist are primarily in implementation of the requirements, similar to how differences exist in implementing the options in the EV Guidelines.	
7			