# Notes for completion - 101: (and apologies if this appears to be teaching Granny to suck eggs)

# This document uses custom Properties fields. To see your corporate or personal reviewer id., go to File - Properties – Custom, select ‘ReviewerId’, change the text to your own corporate and/or personal name and then Modify. Do the same to set ‘Date completed’. Then open the headers, select the line commencing ‘Reviewer’ and update the field (‘F9’).

# Each review comment in the following table will be automatically numbered but you need to set your own abbreviated ‘RevId’. To set your corporate or personal reviewer id., go to Format – Bullets and Numbering – Customize, in the ‘Number format’ field change ‘RevId’ to your own corporate and/or personal id and then ‘OK’ back out. Please use a max of four characters (two or three is better) – all we need to be able to do is identify your comments among others’.

# Severity (Svrt) should be one of the following, accepting that these are somewhat subjective determinations:

# F – Fatal or Major problem which will have a seriously adverse effect on the validity of the document and its ability to fulfill its purpose or be widely accepted as being authoritative. This might be a single item or a systemic problem if there are many instances of a problem which would be of lesser import if it were to occur singularly;

# S – Significant problem which could have a notable adverse effect on the validity of the document and its ability to fulfill its purpose or be widely accepted as being authoritative, but would not be so severe as to leave it fundamentally flawed;

# C – Cosmetic problem, e.g. typos, grammatical enhancements, layout, style and consistency, which whilst not being unlikely to hinder comprehension of the document might give an impression of inattention to its preparation.

# If the document is Word, be cautious of installation-specific variances which may cause line or page numbering to be inconsistent between different reviewers’ copies of the doc. Other formats (e.g. Excel, Adobe) tend to be more reliable in terms of their structure. Use something more permanent e.g. the section number, a title or a unique sample of text.

# Please be brief and to the point – no offence will be taken. Proposed resolutions will speed the review and disposition of comments, which will lead to the agreed resolution.

# Feel free to delete these notes once you’re familiar with them. Problems? Pls either call or email KI (Joni Brennan) or Zygma and we’ll get back to you as soon as we can.

| Ref# | Svrt | Section/Line/Unique ref. | Current wording/Question/Definitional issue | Reviewer’s proposed resolution | Editor’s resolution |
| --- | --- | --- | --- | --- | --- |
|  |  |  | Blue highlights are Ann; green are Susan, maroon are Jeff Stollman, orange is David Simonsen |  |  |
|  | S | 36-40 | 3) specify the types of information about the identity subject that will be collected from or verified by a third party; and  4) disclose the types of information that may be disclosed to a Relying Party; | I would remove “types of” so that the statement requires the specification of the specific information to be collected, not merely the category of information. Categories leave too much vagueness as to what is being collected. One man’s generic information is another man’s identify. | Agree |
|  | S | 46-48 | c) not use or disclose [identification or transaction] information about the identity subject for [1) marketing]; or [2) any purpose not permitted under [the No Activity Tracking standard]]; | or 'for any third party or purpose not described in the purpose description of the service' without the users' consent? BTW: the service purpose description should be part of the consent dialogue. | Is this really part of informed consent? I believe it should be part of Section 1.5, No Activity Tracking |
|  | S | 50-55 | d) disclose to an identity subject [immediately] prior to each authentication transaction each element of information about the identity subject that will be disclosed to a third party, including a specification of each data element not required by the authentication transaction, [unless the identity subject has indicated that the disclosure is not necessary and the information to be disclosed has not materially changed]; | The actual attribute values in question should be presented to the identity subject (user) - hence this should happen after authentication (at the IdP), but before sending the information to the service. |  |
|  | S | 78 - 91 | 1.1 Informed Consent  A CSP must:  a) provide to the identity subject a copy of the CSP’s terms of service, which must:  1) be clear and concise;  2) describe how the CSP operates;  3) specify the types of information about the identity subject that will be collected from or verified by a third party; and  4) disclose the types of information that may be disclosed to a Relying Party; | 1) be clear and concise; and written to clearly communicate to a consumer the following information:  Suggest making 1)--- be part of the lead in sentence.  2) describe how the CSP operates; Perhaps add “precisely in non-technical language”. | A CSP must:  provide the identity subject a clear and concisely written copy of the CSP’s terms of service, which must:  a) describe in non-technical terms how the CSP operates;  b) specify the information about the identity subject that will be collected from or verified by a third party; and  c) disclose the information that may be disclosed to a Relying Party |
|  | S | 97-99 | c) not use or disclose [identification or transaction] information about the identity subject for [1) marketing]; or [2) any purpose not permitted under [the No Activity Tracking standard]]; | Ann Geyer: There seems to be an assumption that identity providers cannot bundle services. This is counter to the way IdP is developing in the e-commerce space and I believe limits the leveraging factor. Many consumers will obtain identity credentials because of their internet based activities. We should be encouraging this type of development while ensuring reasonable privacy protections are incorporated into service offerings and agreements.  Susan Landau: I’m not sure of the purpose of [1] given 2. I would recommend skipping the marketing point as it is subsumed by No Activity Tracking. | c) must not disclose information on End User activities  with the government to any party, or use the information for any purpose other than federated authentication. |
|  | S | 101-106 | d) disclose to an identity subject [immediately] prior to each authentication transaction each element of information about the identity subject that will be disclosed to a third party, including a specification of each data element not required by the authentication transaction, [unless the identity subject has indicated that the disclosure is not necessary and the information to be disclosed has not materially changed]; | May be leading to information overload for the typical consumer. Sounds very bureaucratic as well. Simplicity should be a watchword for this type of activity. Consumers should not be bombarded with lots of information that don’t know how to process. | Agree. d) disclose to an identity subject prior to each authentication transaction, or as part of the credential issuance process, examples of the elements of information about the identity subject required by the authentication transaction that will be disclosed to a third party. Identity subjects may indicatet hat the disclosure is not necessary; |
|  |  | 121-129 | h) provide an easy-to-follow identification of changes to previously agreed-to disclosures  i) minimize changes to disclosures  j) provide evidence of the identity of the CSP  k) provide evidence that the CSP is “authorized” to provide CSP services by the federal government | We don’t want to burden people with having to read the entire new document when only a small section has changed. As stated, this may not be enforceable. The point is to compel service providers to develop well-thought-out policies in the first place to minimize subsequent changes | Having looked at the many comments regarding this I am concerned that this consent dialog is becoming War and Peace. There are now 11 separate requirements that are part of informed consent. I believe that as this section continues to grow, it will become nothing more than another of those annoying things a user has to check thru but never reads – how many people actually read 40 page privacy statements on websites. This document is laying so many requirements it runs the risk of becoming irrelevant. |
|  |  | 150-153 | 3. There are two levels of notice. First is the CSP’s notice of its terms, which requires affirmative consent. This notice is presumably given once with occasional renewals. Then there are notices for each transaction. If a user opts-in to the service and then asks for a specific verification, there is another opt-in. | It would be extremely helpful to consumers to have an industry standard CSP that consumer groups can vet and endorse. Then each credential provider can communicate its variance to that standard. | A good idea. The FICAM certification process more or less provides this in its Trust Framework Provider Adoption Process that includes the requirements against which a TFP (and subsequently IdP/CSPs) are certified. The Privacy Criteria are but one of many reuqirements that are assessed. |
|  |  | 155-156 | 4. At AL-1, can/should there be a different policy because data is self-asserted, unverified, not complete, and not as sensitive as at higher levels? Could AL-1 allow opt-out for some or all data elements, with opt-in at higher levels for some or all data elements? Should an identity subject of an AL-1 activity be allowed to say that the consent is good forever, for a year, until cancelled, or otherwise? It would be annoying for an identity subject to be obliged to opt-in all the time for a basic (and non-PII based) activity used multiple times a day. ICAM would allow a “don’t show me this message again” option. Should there be different consent standards for AL-1, AL-2, etc? | Usability is critical for security and privacy. That would argue against different consent standards. I’d go one step further and suggest including an affirmative statement that as usability is critical for security and privacy to be properly applied, keeping the consent the same for all levels is best. | Agree |
|  |  | 161-162 | Should there be different consent standards for AL-1, AL-2, etc? | I would recommend to implement to the widest degree the same rules and interfaces for different LoA's - and also emphazise that consent applications should support 'remember my consent' functionality. This is BTW closely related to the fact that users must be able to later withdraw stored consents, one technical solution is described at http://wayf.dk/wayfweb/users'\_consent\_to\_data\_exchange.html | Agree with the comment to use the same standards as much as possible.  Another requirement levied in the last sentence |
|  |  | 173-183 | Proposed 1.1 c) here would ban uses and disclosures for any marketing and all secondary purposes. But an alternate formulation could allow processing with affirmative consent. For example, the requirement could be that *a CSP must obtain affirmative consent from* an identity subject *[immediately] before using or disclosing information about that* *identity subject for 1) marketing; or 2) any purpose not previously disclosed to the identity subject*. The activity tracking framework seems to prohibit secondary uses, but it does not address whether secondary uses can proceed with affirmative consent. It would be appropriate to provide a clear answer one way or the other. If secondary uses/disclosures are allowed with consent, the process could be controlled with procedural requirements, including time limits. | I do favor allowing secondary use with affirmative consent. I see a number of opportunities for citizen-acquired credentials to be issued as part of a broader marketing program. Sign up for my X service and get your AL1-2-3 credential suitable for purposes a-b-c. This a vibrant developing area and we should be embracing these trends.  In response to Ann, the No Activity Tracking applies to usage on federal sites, not elsewhere. So that doesn’t prevent using the credential elsewhere. Re Bob’s question, that is the heart of the matter. Once one can allow activity tracking with affirmative consent, there will be all sorts of incentives developed by CSP for the users to do so, and the No Activity policy would have no practical effect.  This is important. There should be one consent for the minimum information necessary to process a transaction. But there can be optional consents for additional user information, the provision of which may have benefits to the party providing the information. | Agree with both comments. The consent, at this time, only applies to activities with Federal sites; does not apply for other business purposes, e.g., Facebook, et al. yet |
|  |  | 189-191 | 8. There is a defined term for *attribute*. The term *information* is not defined. Should *attribute* be used instead? Instead of *data element* too? The corresponding term in the minimalism standard is *attribute* not *data element*. | I prefer the term attribute as used to include any information that is intended to identify or convey privilege in this space we are working with.  One possible way to clarify the distinction between attribute and data element is that a data element may be a person’s age. But the attribute could variously be is the person “over 21”, “under 12”, etc. depending on context. | Agree |
|  | F | 196-203 | 1.2 Optional Participation  A CSP should, if it provides identity services as part of its business processes [or activities] to its own employees, faculty, students, or other affiliated individuals, allow the individuals to opt-out of using the CSP’s identity services to gain access to a Federal [and state] government application if access is not required by the [individual’s] [CSP’s] organizational responsibilities or there is an alternate means of access to the government application. | Not sure of the intent of this provision. Does it mean that an employer cannot require its constituents to use the employer mandated credential when engaging with feds for employer related business? If so, I do not support this provision. It is too intrusive into the employer-employee relationship. | Editor does not believe the proposed wording intrudes on the employer-employee relationship. The key phrasing is: “if access is not required by the individual’s organizational responsibilitites”  However, editor also suggests the inclusion of the phrase [and state] significantly expands the intent of this document beyond that of the FICAM.  Further, editor suggests expanding this clause to allow it to apply to any entity that uses the services of the CSP, i.e., business partners, as part of its business activities with the Federal government.  Suggested wording is:  1.2 Optional Participation  A CSP should, if it provides identity services as part of its business processes [or activities] to its own, or business partners’ employees, faculty, students, or other affiliated individuals, allow the individuals to opt-out of using the CSP’s identity services to gain access to a Federal government application if access is not required by the individual’s organizational responsibilities. |
|  | C | 214 | 2. The term *business process* is not clear. Does a non-profit organization have *business processes*? Adding the word *activities* might be clearer and more encompassing. *Business process* is not a defined term. | Yes, business process is a generally used and understood term in the Non-profit sector.  Business process may need definition, but the general usage of the term can certainly apply to non-profits. It commonly refers to any routine process to accomplish a task. The term “business” does implies neither commerciality nor profit motive any more than the term “work” is limited to paid employment. | Agree |
|  | C | 217-220 | The term *organizational responsibilities* is not clear If the organizational responsibilities being referred to are those of the *individual*, the meaning is something like *for the individual to function within the organization*. It cannot be tied to a job requirement, especially if students are possible users in a school setting. | It can be tied to one’s organizational role and responsibility set. At my university (UC Berkeley) we do this routinely. | Agree |
|  |  | 227-228 | A CSP must transmit only those attributes [about an identity subject] that are a) explicitly requested by the Federal Relying Party application; | Should there be some additional description here to emphasize that query responses should not only limit themselves to the scope of the query, but also transform data elements (such as age) to transmit only “older than 21” if that is sufficient to address the query?  This is where the 'minimal disclosure' principle should be observed: Only the minimal amount of information needed to perform a transaction / grant access must be supplied to the service. Hands-on experience show that often services request too much information - so, considering what mechanism ensures that the attribute release profile only lists the minimal information needed for each service would be worth while? | Agree with both |
|  | S | 224-229 | 1.3 Minimalism  A CSP must transmit only those attributes [about an identity subject] that are a) explicitly requested by the Federal Relying Party application; or b) required by the Federal identity assertion profile. | And for which affirmative consent to release the attributes has been acquired from the information subject (or whatever this term ends up being). | Editor comment:  Believe that the addition of consent, again, is not needed. Consent is clearly covered in Section 1.1 |
|  | S | 239 | Other Kantara requirements may already address minimization | It may be worth querying FICAM to confirm that there is no data minimization requirement on the identity provider. That does seem to be the case however. If that’s so, then it might be worth calling out in the document.  I am not convinced that coverage in other documents is sufficient grounds for exclusion here. I think that collection minimization is important. I think each document needs to stand alone. They may not always be used in concert. | The FICAM Trust Framework Adoption Process says this about minimalism: **Minimalism** – Identity Provider must transmit only those attributes that were explicitly requested by the RP application or required by the Federal profile. RP Application attribute requests must be consistent with the data contemplated in their Privacy Impact Assessment (PIA) as required by the E-Government Act of 2002. |
|  | S | 241-244 | Minimization as discussed here applies to data disclosure to a relying party. Perhaps there should be an independent minimization requirement for data *collection* to prevent the creation of more comprehensive dossiers. It’s an important principle of Fair Information Practices. Collection needs would, of course, vary with the level of credential | I agree this needs serious discussion. Creating a large identity dataset creates significant privacy exposure. I would start with the idea that relying parties should have a standard attribute set that they require; industry can vet the standard over time; Privacy principles of minimization can be set as an expectation.  Then consumers can be informed about this process rather than having to individual vet for themselves how all this works.  Consumers will operate on a trust framework—naively accepting the conditions imposed if this is the path to get access to the services they want; so the trust has to be built into the process and this document can be the start of that process.  I support this. | Aagree, this needs discussion. |
|  |  | 250 | 4. Section 1.1d uses the term *data element* while this provision uses the term *attribute* | In my terminology, data elements refer to what is collected. Attributes refer to what is transmitted. Attributes are congruent with, but not equal to, data elements. | Attribute |
|  | F | 252-254 | 5. Should there be any possibility of sending additional information if requested by an identity subject? Suppose that a frequent flyer number is not a required element, but the identity subject wants to share it. | See comment immediately above. Your questions raises the issue of separating identity attribute transactions from information that the service may require after authentication. I suggest that this line not become too blurred, else we risk falling onto the slippery slope to the big identity database  As we restrict information collection, we need to allow for user provided data which a user volunteers to enhance his/her user experience.  Also data verification services might come into play: if you choose to apply for X, also legal age may be needed, or >21 years. Typically this kind of information MUST NOT be self asserted and further requests for info can be expected (these might work as standalone services, providing specific information). | If an authenticating party wishes to share additional data with an RP, suggest that this be considered a part of a post authentication transaction. Agree with Ann that we should not be looking to complicate things here. |
|  |  | 258 | 1.4 Unique Identity | or 'pseudonym' / 'service specific pseudonym' |  |
|  | S | 258-266 | 1.4 Unique Identity  A CSP must  a) give a persistent abstract identifier unique to an identity subject for any Federal application that does not require personally identifiable information; and | What does this term (abstract) imply? | If the Federal application does not require actual PII, the CSP must provide a unique identifier to ensure the same individual is attempting the authentication. This identifier may be any form of data, but must be unique to that given individual and be the same for every transaction |
|  | S | 265-266 | b) when allowed by the technology, create a unique identifier for an identity subject that is also unique to each Federal application. | Don’t immediately see why this provision is necessary. We risk proliferating identity and complicating authentication. The federated identity management scheme handles this issue much better.  Ann, isn’t this simply exactly doing what a federated system does in creating a pseudonymous identifier per SP? | Completely agree with Ann.  Not technical enough to address Susan’s comment. |
|  |  | 281-282 | (a) The Kantara original used the term *individual identity subject*, which is not a defined term. The superfluous modifier *individual* has been dropped. | Don’t forget that authentication transactions include non-person resources. The attributes will be different but the framework and workflow processes should be similar. | ok |
|  | S | 288-290 | c) The standard *when allowed by the technology* is not an especially clear standard. Something may be allowed by the technology but administratively or financially infeasible. Alternatives are: (a) *When feasible*; (b) *When practicable*; or (c) *When practical*. | Why can’t we use the policy verb “should” which typically means in SDO settings -- unless there is a good reason not to comply.  It is not clear to me that any of the alternatives provide an enforceable standard that can be audited. Perhaps it can be viewed as a recommendation only, in which case the wording becomes less crtical.  Alternatively, we could use the term “commercially acceptable” which has legal meaning – at least in the US. | The ICAM Trust Framework Provider Adoption Process includes the following requirement: The authentication process shall provide sufficient information to the Verifier to uniquely identify the appropriate registration information that was (i) provided by the Subscriber at the time of registration, and (ii) verified by the RA in the issuance of the token and credential.  The drafter of the PAC suggested in line 271 that there was no requirement to provide a unique identity. The preceding suggests that there is. However, the requirement does not specify the method for doing so.  Suggest this section (1.4) be rewritten along the following line:  The CSP should provide sufficient information to the RP to uniquely identify the authentication party. |
|  |  | 294-304 | 1.5 No Activity Tracking  A CSP may not disclose [identification or transaction] information about an identity subject’s activity regarding any [Federal] application to any other party; or use the information [for any purpose or activity] except  a) for proper operation of the identity service; or  b) as required by law. | Add Or as agreed to by the subject.  Ann, why are you suggesting “as agreed to by the subject”? That opens a can of worms that will eventually eviscerate the purpose of No Activity Tracking. | FICAM requirement re this is:  **Activity Tracking** – Commercial Identity Provider must not disclose information on End User activities with the government to any party, or use the information for any purpose other than federated authentication. RP Application use of PII must be consistent with RP PIA as required by the E-Government Act of 2002.  Why does Kantara need anything more?? |
|  |  | 308-310 | 1 The provision here is titled *no activity tracking*, but that is not what the text does. It regulates use and disclosure but not recording of information about transactions. That title is misleading. | That’s correct, but that’s the federal term, so we have to use it that way.  Could it be turned around?: Activity tracking: A CSP may only ... , and not ...' ? | Yup |
|  |  | 312-318 | 2. ICAM has a flat ban on disclosures. It employs a different standard for secondary use: *any purpose other than federated authentication*. That standard is not defined and may be unrealistically narrow. Fraud detection and subpoenas must be accommodated. NIST ties *use* to a Privacy Act of 1974 standard not directly relevant here, one that is interesting nevertheless – to employees *who have a need for the record in the performance of their duties*). NIST’s disclosure limit also tracks the Privacy Act, but the Act’s disclosure rules are too flexible to be relevant here. | Except for legal investigations the ban on secondary use “for any purpose other than federated authentication” seems exactly right.  This provision is problematic from a privacy perspective. It is too broad and effectively negates affirmative consent; since there is such a big loophole that no consumer would ever contemplate the set of needs in the performance of federal agency duties. Out, out out! | See above |
|  | S | 320-322 | 3. Can uses/disclosures be made with an identity subject’s consent? If so, what is the nature of the required consent? Disclosures can presumably be made to the identity subject, although that is not clear here. It is addressed later under dispute resolution. | Again privacy principles would require that the subjects be able to see and correct any information maintained about them.  As a privacy oriented profile, let’s fully engage with the FIPPs principles. | See previous. Let’s not get things so involved and spread that we tie things in knots. |
|  | S | 324-325 | 4. Should there be a different standard for identification information than for transaction information? The focus here seems to be on transactions (activities). | Attribute requirements could very easily be different, but the goal should be a consistent, replicable process for either. | Same here |
|  | S | 327-329 | 5. Some issues raised by permissible disclosures apply to uses. A large company that offers identity services along with its other activities may be tempted to use the wealth of data for marketing or other purposes. | No. This is exactly what No Activity Tracking prohibits. | Agree |
|  |  | 336-340 | 6. Will it always be possible to identify a federal application? What about government contractors and grantees? What about joint federal-state activities? If the document is tied expressly to federal agencies (not necessarily an inappropriate choice), it may require considerable change to use in other contexts. A state will not be able to use it because the policy here is too intertwined with the Privacy Act of 1974. | For the purposes of this document, such contractors function as if they were the federal government and are subject to the same rules.  Agree, this work should be useful outside the federal government. Perhaps we can think about a mechanism to allow localized substitutions.  Privacy Act of 1974 is used here, I believe, as enabling legislation. States will have different such legislation. | Agree with |
|  |  | 342-345 | 7. The original “information regarding Identity Subject activities with any Federal application” language is awkward. Substitute language proposed here is not much better. Would just plain “about an identity subject’s activity” work? Is *transactions* better than *activity*? Would *actual or proposed transactions* be clearer? | I would think we could create a definition of transaction that works for this purpose. I use the term quite broadly to include request, response, communication between two or more parties.  I don’t understand what information would exist for a “proposed” transaction. | I reiterate. Why does Kantara need anything more than what is specified by FICAM? |
|  |  | 347-356 | 8. The first exception is troublesome. *Problem resolutio*n in the original document is not that clear a term and may be too limiting. What about ordinary operation of the service, such as disclosing data to service providers, lawyers, accountants, cloud computing vendors, etc. The disclosures may not relate to the specific solving of any problems, and that language has been dropped from the original. Should any disclosures under this exception be controlled with respect to further use and disclosure by an authorized recipient? Perhaps with language that limits use/disclosure to those permitted under this provision, under contract with the CSP, or when required by law? The entire HIPAA *business associate* notion could be dragged in here, although the full thing would be overkill. A CSP could be left with the responsibility of addressing use and further disclosure of personal information by its service providers. | Perhaps we could use the second use principle? If the disclosure is for a different purpose, consent is required.  Begs the question about how to define the purpose; but I think it can be resolved.  Agree—this is not a HIPAA document.  Keep in mind that the CSP and the SP can and will be part of different entities and their relationship established by contract. CSP may not have much control over the actions of the SP. | See above |
|  |  | 365-368 | 10. Should the disclosure limits apply only to identifiable data? Or individual level data? Aggregate or de-identified data could be made available for research or other purposes if an identity subject’s privacy interest is adequately protected. Data use can be controlled with a data use agreement that limits how the recipient can use the data (or reidentify it). | No, no, no. No activity tracking is what is in order to protect privacy. And we really don’t know what identifiable data is; much that looks like it has been deidentified is possible to reidentify.  These days, it doesn’t take much to identify the subject of information. CSP are collecting information for identification purpose. The presumptions should be all this data can be re-identity and treat it as if it already is. |  |
|  |  | 371-379 | 11. Should there be a requirement to maintain a disclosure history even for ordinary service disclosures? Disclosure histories are a two edged sword. They are useful and probably essential for accountability. But if histories include credentialing activities, then the result is a history of all transactions. That history is a privacy flash point in a credentialing system, which could become a complete history of all user activities across the Net. However, without records, there may be no accountability. One potentially easier idea is to maintain histories of service disclosures but not transaction disclosures. Or to require destruction of transaction disclosures on a short and fixed schedule. There may be other approaches to the problem, some involving the use of encryption. | It probably should be agency dependent (e.g., yes for access to your IRS records, no to checking information on STDs at HHS). Therefore best if left to agency discretion (and therefore can be ignored here).  From healthcare experience, consumers rarely ask for disclosure-; but the information is extremely useful for incident management and of course for investigations, audits, and legal purposes.  I believe that some history will be necessary to provide evidence for enforcement of these guidelines. It may be appropriate to require that such logs be encrypted to a certain standard and be accessible only by certain roles under specific conditions. But without such records, how can a bad actor be held accountable? Retention limits likely also apply. | See above |
|  |  | 386-394 | 13. *Required by law* is a familiar standard, but a very loose one. An agency of a municipal government in a state can issue a regulation requiring disclosure of the mayor’s transactions to the local newspaper. That’s *law*. There are ways to slice the issue here. One could specify court orders as one category to deal with that aspect of compulsion. Thus, *order of a court of competent jurisdiction* helps and allows for fighting over what the limitation means. It might be read to exclude an order of an out-of-state court or a North Korean court. The term *law* is very broad. It could be limited to *statute*, *federal statute*, *federal or state statute*, *federal statute or regulation*, or in some other way. It helps some that these disclosures are allowed but not required by the provision. | Required by law means after all legal recourse has been exhausted should the disclosure be made. There are many jurisdictional issues, exceptions that can be exercised.  Because this profile is limited to federal government, it would seem that federal jurisdiction needs to be specified. | Again, why more than required by FICAM?  In any case, these apply only to transactions with Federal applications so the applicable law is US federal law. |
|  |  | 402-405 | 15. A broader question is what happens if an identity provider based in another country (Canada, EU, or others) provides credentials for access to U.S. government systems. | If the laws of the home country of the company conflict with U.S. requirements (e.g., No Activity Tracking), then perforce the company cannot provide identity services to the USG. So I think this is an non-issue. | This is not an issue. For authentication to US government applications and portals, the credentials used MUST be issued by an IdP that is certified by a FICAM certified trust framework. If the IdP is located in a foreign country it must operate according to the TFP requirements which will likely operate according to US law. |
|  |  | 409-449 | 1.6 Adequate Notice  A CSP must  a) at the time an identity subject initiates access to a Federal government application, display to the subject any text provided by the application, including:  1) a general description of the authentication event;  2) a description of any transaction with the Federal application;  3) the purpose of the transaction; and  4) a description of any disclosure or transmission of information about the identity subject that the application requested from the CSP;  b) allow the subject to cancel the transaction before any of the subject’s information is shared with the application; and  c) make available in a timely and effective fashion to each identity subject, each potential identity subject, and the public a clear and concise notice of its privacy practices, including a general description of:  1) the types of personal information collected, including whether each data element is required or voluntary;  2) all sources of personal information;  3) how the personal information is used and disclosed;  4) the manner in which an identity subject can exercise choice and express consent;  5) the procedures by which an identity subject can utilize the CSP’s dispute resolution process to complain about any CSP failure to comply with its terms of service or privacy policy; or to obtain access to or request correction of information about the identity subject; and  6) how personal information is stored and how and when it is disposed of when no longer required. | Should this be the responsibility of the CSP or of the Federal application? How will the CSP gain knowledge of all federal applications sufficient to provide this information – especially if it is a new application?  This requirement implies developing a standard for passing data from the application to the CSP sufficient to address this requirement. It may be better to impose this requirement on the application.  Reply to Jeff's question: It is the responsibility of the CSP because the notification / consent must happen \_before\_ the data release to the SP.  Federation metadata may be used for this purpose (eg. SAML2). Examples of existing systems could be http://www.incommonfederation.org/ or http://www.wayf.dk or http://www.refeds.org | This really appears to be overkill. We have Opt-in in Section 1.2 and as bad as those requirements are operationally, this levies even more unrealistic requirements on the CSP. I totally agree with Jeff’s comment. |
|  |  | 497-499 | 7. Should all assurance levels have the same privacy notice? All notice needs may be met by one common notice, but that notice may become more elaborate and harder to understand. | It seems to me that it would be useful to include in this document recommended forms for notices of AL1-4, with a short description that AL-1 does not contain PI (unless your identifier reveals such information), that AL-2 … , etc., but a warning that aggregating information may lead to identification | I think this may be getting confused. The FICAM Privacy Assessment Criteria say the following about Adequate Notice:  **Adequate Notice** – Identity Provider must provide End Users with adequate notice regarding federated authentication. Adequate Notice includes a general description of the authentication event, any transaction(s) with the RP, the purpose of the transaction(s), and a description of any disclosure or transmission of PII to any party. Adequate Notice should be incorporated into the Opt In process.  Nothing here about Privacy Notice. Again, why make this more restrictive than the Feds do? The current wording of this PAC requirements includes so much detail that I would suggest 99% of transactions never complete and the PAC becomes irrelevant. This is the current wording:  1.6 **Adequate Notice**  A CSP must  a) at the time an identity subject initiates access to a Federal government application, display to the subject any text provided by the application, including:  1) a general description of the authentication event;  2) a description of any transaction with the Federal application;  3) the purpose of the transaction; and  4) a description of any disclosure or transmission of information about the identity subject that the application requested from the CSP;  b) allow the subject to cancel the transaction before any of the subject’s information is shared with the application; and  c) make available in a timely and effective fashion to each identity subject, each potential identity subject, and the public a clear and concise notice of its privacy practices, including a general description of:  1) the types of personal information collected, including whether each data element is required or voluntary;  2) all sources of personal information;  3) how the personal information is used and disclosed;  4) the manner in which an identity subject can exercise choice and express consent;  5) the procedures by which an identity subject can utilize the CSP’s dispute resolution process to complain about any CSP failure to comply with its terms of service or privacy policy; or to obtain access to or request correction of information about the identity subject; and  6) how personal information is stored and how and when it is disposed of when no longer required.  This is an inordinate amount of information that effectively requires that the CSP privacy policy be presented to an authenticating party with each transaction. STRONGLY suggest that this be rewritten to mirror the FICAM requirement and NO MORE. |
|  |  | 515-516 | destroy personal information maintained for the identity service as soon as practicable; | For emphasis, it might be useful to say “destroy all copies of personal information retained for …” | There are very specific time frames for the retention of data that was used to verify identities which can extend to 7.5 years after the credential has expired or been revoked in the case of PKI credentials that are cross certified with the FBCA. Many non-PKI IdPs will operate according to similar policies.  Once again, this requirement adds significantly to the FICAM requirements which states:  In the event an Identity Provider ceases to provide this service, the Provider shall continue to protect any sensitive data including PII. |
|  |  | 544-551 | 5. This requirement suggests that, if transaction retention (as discussed in my comment on Item 1.5) is required to support enforcement, a CSP may shut down to circumvent log retention and potential penalties.  6. It may be advisable to provide an either/or choice here. Rather than merely requiring destruction of all information, adding an option for the CSP to offer its clientele the ability to securely transfer all of their data to a different CSP would preserve the existing accounts with federal agencies, rather than causing users to have to reestablish them with every application. | Inserted question from Jeff. |  |
|  |  | 529-532 | Security may be adequately addressed elsewhere in the Kantara set of requirements, in which case this language is unnecessary, as would, perhaps, be the requirement to maintain security after termination. Termination is addressed, e.g., at AL1\_CO\_ESM#055. Does security belong here rather than here? |  | Security and the steps used to protect PII re generally covered in specific sections of credential policies and other operational documents. Suggest that is the best place for it and not here. |
|  |  | 564-566 | 1.8 Changes in the Service  A CSP that changes the terms of use of its identity service must promptly inform each Identity Subject of what changed and the purpose of the changes.  **Drafter’s Notes and Questions**  1. There is no comparable provision from ICAM or NIST. The Privacy Act of 1974 requires agencies to publish notices in the Federal Register, with the type of notice depending on the type of change. |  | So why should Kantara insert this? |
|  |  | 571-572 | The language says *promptly*, but this is a weasel word that provide no real direction. Does it mean before or after the changes takes effect? | This weasel word issue concerns me. Is there a way we can strength things, e.g., by insisting that a requirement of the Kantara PAC is that the user must be informed prior to the change (I realize that the informing may occur moments before the change; still, that puts a delimiter on the action). | There is no requirement from FICAM for this so why add it? |
|  |  | 584-589 | Third, should the notice requirement differ depending whether a change is material or not? Suppose that a CSP changes the name or title of its privacy officer. Compare that to a change that would permit a CSP to use personal information for marketing when the previous policy did not allow marketing uses. Should the same notice obligation attach to each change? The best answer is probably not, and minor or immaterial changes might have a different notice procedure or perhaps none at all. | I believe that all changes should require notice. Trivial changes should not be burdensome to report. But the more burdensome they are, the more incentive a CSP will have not to change. This simplifies life for its many users – many of whom will have a proliferation of accounts and would prefer changes to be minimized | This statement sort of points to a very serious issue with this entire document:  But the more burdensome they are, the more incentive a CSP will have not to change.  As burdensome as the requirements in this document are, will CSPs really want to participate? |
|  |  | 621-642 | A CSP must  a) reserve in its terms of service the right to change the terms and to make the change effective for all information previously collected;  b) to the greatest extent practicable, provide effective advance notice of a material change that would affect the rights or interests of an Identity Subject, with individual notice to an Identity Subject required if a change would alter a choice make by the Identity Subject;  c) provide for a reasonable period before and after the effective date of a non-material change, notice of the change through a dated and highlighted posting on the CSP’s website at one or more places where an Identity Subject would be most likely to see the notice of change;  d) include a date and version number for its terms of service;  e) maintain as part of its terms of service a history showing the date and nature of all changes made previously;  f) if practicable, make a material change effective no sooner than 30 days after providing notice of a change. | Once you impact “information previously collected” it becomes necessary to require consent from the user. Otherwise the user’s initial consent becomes meaningless because it can be overridden by a subsequent change.  I agree  I think this is good. | Has anyone discussed with actual operational CSPs to determine the cost and resource implications of this? |
|  |  | 646-654 | 1.9 Dispute Resolution  A CSP must  a) promptly allow an identity subject to review and have a copy of any information about the identity subject maintained by the CSP, except for information specifically compiled in reasonable anticipation of a civil action or proceeding; | I don’t understand this exemption. Is this intended to cover the possibility that the CSP will bring civil action against its client? In such a limited circumstance, I would agree. But it might be worth being more explicit about who is bringing action against whom. | This is generally included in Privacy Policies. |
|  |  | 656-658 | b) promptly allow an identity subject to request an amendment of any information that the Identity Subject could review under paragraph a) that the identity subject believes is not accurate, relevant, timely, or complete; | I think what needs to be prompt is the CSP’s response.  The CSP should also be required to provide an effective mechanism to allow timely filing of a request. | Promptly – an hour, day, week, month…?? Suggest deletion of the word. Again, usually included in Privacy Policies. |
|  |  | 665-666 | d) establish a process for sharing any amendments with those recipients of the unamended information designed by the identity subject; | This will require the maintenance of a transaction history as discussed earlier. Otherwise the CSP would have no record of whom to update. | Agree with Jeff. This is an unrealistic requirement. Please delete |
|  |  | 668-670 | e) establish a fair dispute resolution process for any complaint made by an identity subject about a failure of the CSP to comply with its terms of service or any other applicable requirements.. | Isn’t this the process described under sub-item c)? | Don’t think this is the same as item c. However, this item should be item a in the is section and is generally included on Privacy Policies. |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  | 646-655 | 1.10 Technology Requirements  A CSP that engages in any identity transaction with a government application must comply with one or more of the ICAM-approved Authentication Schemes. (See <http://www.idmanagement.gov> for the current list of technology protocols from which to choose.)  **Drafter’s Notes and Questions**  • There is no comparable provision in ICAM or NIST. |  | There certainly is. See the following from the FICAM Trust Framework Provider Adoption Process:   1. Use an ICAM adopted authentication scheme.   This is included at all three levels of assurance in the Assertions section of requirements for certification. Suggest this section be deleted from the PAC. |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

# On completion of your commenting please observe the following requested process for submitting your comments by the requested date, for disposition along with all other comments received:

# save your comments in a Word file with the name ‘*«RevId»*’ (i.e. append with the ‘RevId’ you used in the table above);

# email your comments to the P3 list or directly to using the above filename as the Subject line.

Your adherence to these requests will facilitate the capture & processing of your comments.

**Comments not provided in the above format will not be processed**. Thank you for your time.