openIDL - System Requirements Table (DaleH @ Travelers)

Grouping	ID	Date	Requirement	Notes
Data and Data Integrity	D.1	5/23/22	Data contained in the carrier data store will conform to OpenIDL data model standards	
Data and Data Integrity	D.2	6/1/22	OpenIDL data model standards shall exist for all Property & Casualty lines of business except Workers Compensation (List out lines of business). Domestic business for now.	
Data and Data Integrity	D.3	5/23/22	Minimal data attributes to be available in carrier data store shall consist of the "Day 1" OpenIDL data model fields, other attributes in the OpenIDL data model are populated at the option of the carrier	
Data and Data Integrity	D.4	5/23/22	Data shall consist of policy and loss transactions over the course of the policy term and lifetime of any associated claims based on source system activity	
Data and Data Integrity	D.5	5/23/22	Data shall be current to the Prior Month + 45 days	
Data and Data Integrity	D.6	5/23/22	Companies shall maintain data in the carrier data store for 5 prior years plus current year	
Data and Data Integrity	D.7	6/1/22	All data contained in the carrier data store is soley owned and controlled by that carrier	
Data and Data Integrity	D.8	6/1/22	Data shall remain accurate as of a point in time and may be corrected over time if errors in the transmission of data occurs with no obligation to restate prior uses of the data. Once data leaves the carrier node, that data is assumed to be published/accepted.	
Data and Data Integrity	D.9	6/1/22	OpenIDL shall maintain (specification and implementation) an edit package to be available and used by carriers to test conformance to data model standards and data point interactions similar to the functioning of the AAIS SDMA portal. Implementation is part of HDS solution. OpenIDL will audit, certify and conformance of edit package implementation.	
Data and Data Integrity	D.10	5/23/22	Data must pass through OpenIDL edit package and be within 5% error tolerance per line and state based similarly to acceptance by AAIS through SDMA portal	
Data and Data Integrity	D.11	6/1/22	The OpenIDL data model standards will foster effective and efficient data extractions such that queries of data can be satisfied within 24 hours of commitment to participate in an information request	
Data and Data Integrity	D.12	6/1/22	Any changes NAIC required fields to the OpenIDL data model will require a minimum of 18 months notice for carriers to conform	
Information Requests	IR.1	6/1/22	Requests for information shall be specific in detail and communicated through a secured protocol	
Information Requests	IR.2	6/1/22	Forum shall be established for carriers and regulators to discuss and agree to intent and interpretation of information request	

Information Requests	IR.3	6/1/22	Request for information shall be for aggregated information only, no individual policy, claim, or personally identified information shall be requested or honored	Need for info @ a policy level or vehicle, obfuscation of VIN ways these requests are added to or validated? KS: exceptions known when extrax is requested JB: at policy level, info from policies CANT be extracted (they might be useful) or some level of aggregation. Data contributed from each carrier to prevent identification DH: requests - none ask for policy or claim info up until today JB: VIN & Insurance? Not just carrier only restrictions, address requirements across ecosystem DH: straight to regulator? fine w/ providing info. Analytics node others have access to and can pull? NO JB: only regulators would have access to information DH: person or group making reports for reg? Concerned. Controls so they cant do anything with data DR: blurring lines from compliance-style store to transaction processing, requires higher standards, conflating 2 systems, holding to other standard can make a lot of reqs messy JB: not matter of timeliness or responsiveness, matter of scope and level of aggregation, level by which info is agg or identified, only collected for purpose of sending to regulator, covenants needed DR: purely a regulator - not LE or Insurance Commissioners. Caveat - not bulk. PII should never be requested in Bulk. If a specific question, then yay/nay "coverage exists" but leery of "give me all VINs" just because DH: dont want to open up our books JB: PII in general not involved. ND is VIN not necessarily person involved. DR - policy effective date, VIN and address enough to correlate. Still protected by aggregation rules DH mentioned. 100k VINs "is someone in the state covered" not WHO. JB - another requirement applies to Data Requests
Information Requests	IR.4	6/1/22	information requests shall identify who has access to the ~~private analytics node~~ result data and interim data (anything coming out of the HDS)	DH - not naming people, data within the node. For specific info request KS: To the analytics node or to the specific report? Doesn't change from request to request. Dont add new user to analytics node DH: req from Reg, no interim body in between, just us and Reg have access to data. If AAIS has access to openIDL, and create extraction pattern, need to understand WHICH bodies will have access to that data - needs to be spelled out. Get to 3rd party: AAIS + Carpe Diem, wants to know ahead of time JB: access to the data, the results, the report DH: access to the data AND the report, outside of carrier node KS: aggregated, extracted data DH: Carrier, claim, policy, PII - I need to know who has access to it KS: anything you say is OK to be in the results, you want to know who JB - qual and credentialing DR: need for simple data lifecycle, provenance. For this request, this all lives in the extraction request, for this request - this raw data - the result shall be X and visible to Y folks for Duration Z. No unfettered access to HDS, only with some purpose. Even analuytics node shoulfn't be used for other purposes without consent KS: Definition of what data shoulf be used for JB: Categories: privileged, etc. DR: a lot may not be funct. but when we get to approval of extraction patterns, might be more implementation JB - term sheet of a request DR - adapters can see these X raw elements, can turn them into Z elements for ABC. Routine if useing same data, but shouldf be explicit KS: Nuance, part info request and part how it works. Who can see uncombined data should be part of system architecture. Refined results are what we are talking about. DR: System works well, only see results. Flaws, mistakes, exploits - what data at risk. Sanity check - looking at result data and asking for 20 fields of raw and only using 10, then spiking that request KS: When a carrier consents their data is run thru extrax, their data is recognizable UNTIL it is processed DR: 3 steps: RAW, Semi-Agg/not anonymized, Anonymized. Bake in now
Information Requests	IR.5	5/23/22	Information requests shall define timeframes for data to be included in the aggregation	JB: talkkng about lifetime use of info - historical or one purpose, number of uses, number of purposes DH: when you make a req for info, request must be specific (time parameters, types, etc.) for the request of the data - query range

Information Requests	IR.6	5/23/22	Information requests shall define the attributes to be used in aggregation	JB: Nature of the data call request? KS: shoudl be redundant - dont see people reading code JB: query, results in aggregated things, 2 parts of a request-report. Req will identify the things selected and need to be accessed. If you did this via Wizard or screen, those criteria included at that level. Translated into extraction KS: least big declarATIVE IS A HEAVY LIFT. Not sure short term target, right now map-reduce function Peter - attaching meta data to the calls, human readable - will need that clarity JB - not talking NLP, but request-translated-terms/types requested and accessed in raw data. KS: whats going over the wire a result of an agg routine. Will return written premium by x and y. DR: acceptance criteria - request, tells us XYZ, approve/reject - some plan lang explanation of what is being asked for. REG: these premiums these lines - should come out in the aggregate. Who writes the query? Analytics node? REGs? Here is what the output looks like, whats needed to gen output. Prob run test execution, these elements were accessed, accepted. KS: Added ability to test as a requirement DH: also want to know if there is extraneous data requested thats a backwards way to get some data PA: not quite sure what actor will write Extrax Pattern, will be run on certain analutivcs node, who owns that query JB: if in fact, aggregating total premiums per zip, other criteria involved wouldn't show up in req. If you asked "give me total premium on house on Main street" - different thing. Providing info in aggregate JM: solutioning - req is clear, if you use elements, tell me what you want to use DR: needs to be a req JM: might be hard, implementation JB - nature of query will specificy types of data JM - by def, person capable of reading code will be able to answer question. Must be operable by human beings PA: I will write an Extrax pattern to calc premium on X. Who will come in and validate that query is doing what it is supposed to be doing? JM: risk someone chooses elements does something wrong. DR: solution prob for how to verify, on us to solution for, need to know what was supposed to be requested PA: person running Analytics node needs to validate JB: query request, what you can request, minimal set to expand, translates to extraction logic DR: someone writing query should be responsible, result A and Inputs B - need to be able to verify only B was touched and ONLY A came out. what data pulled for what end - must be defined - shoudl be trivial for whoever is writing the query JB - specificying the things the query is for and validating thats what it does JM - saying you can block someone AND block/report. "I reject this request" vs "You said you needed 5 things and we see you requested 7 so..." JB specifying what it is intended to do is a starting point DR - then governance JB - glossary DR - not thousands of elements
Information Requests	IR.7	5/23/22	Information requests shall define the logic for extracting and aggregating data	DR: interpretation - doesn't need to be pseudocode level or extremely details but has some detail JB - business justification request? DH/JM - yes JB - specifies purpose, what elements, who its for, how done - human understandable JM - will be metadata page, very descriptive, processable by humans JB - logical request KS - human TRANSLATABLE (understandable)
Information Requests	IR.8	5/23/22	Information requests shall identify and define the calculations to be used in aggregations, analysis, and reporting	JB - similar to logic. Combine with IR.7
Information Requests	IR.9	5/23/22	Information requests shall define the specific use of the information	JB - use and access - REG only, single use? JM - who in the sense of roles not names, will know what they want to do with it. Privacy +. Different than "WHO". KS - restriction/constraint. If you say you use it for that, thats all you can use it for. JB "specific purpose and not other things" - like licensing JM - commercial vs personal all the time.

Information Requests	IR.10	6/1/22	Information requests shall define the permitted accessors to the information and users of data	JB: the WHO. Use declarative, WHO is a restriction JM - redundant with IR.4 DH - who has access to final report JB - other was access in transit. RELATED to IR.4. JM - lifecycle flow - who has access throughout DR - implementation has that data in the same place, doesn't hurt to be explict with requirement JB - tempted - come up with a draft of template of a term sheet for this DR - few weeks ago - definition of that request template. DH: beyond the smart contract - business level
Information Requests	IR.11	5/23/22	Information requests shall communicate the proportion of individual carrier information to the population of data in the extraction prior to final commitment to participate	JB - keep carriers protected from self-detection. Data can't be deidentified. Provided to each contributor. DH: Travelers is 25% of a pop, can decide if they want to be a part of it or not JB - only know when you have the total DR - requirement: maximum acceptable, sep req that says "no darta will be pulled or aggregated UNLESS it can be confirmed. Might have to do pseudo-extraction to get a rough size. JB - consent to request, what it is asking , data is contrib to the analytics node as "pending" but not approved for use until such time there is sufficient data to let the node say what the totals were DR - maybe do with a lighter weight. Shallow (25% of WHAT) JB - general metrics, so many policies outstanding JM - language of "prior to final committment to participate" DH - two step - what portion you will have (query all avail carriers, who will participate) then when there is a sense of what % of the total WILL we participate. Others face same thing KS - time problem - bartering back and forth JM - regardless of how we do it, data wont be seen until we meet the threshhold. We won't see data unless X%. Multi-stage scares me a lot. DR - once extracted have we lost control? Governance. In Analytics node. Lost effective technical control. Def recourse. Affirmative tech control is lost. Jm - governance level requirement. Whole solution requires not release data w/o reaching threshold. You pull one carrier then ouch KS - micro-req - define participation threshold - then argue governance DH - 2-step process, another requirement below, set at 15%? KS - % of what? premium, loss? DH - depends on whats being asked for KS - reports just dont tell one thing, define that and then deal JB - requires more thought IMPORTANT ONE
Information Requests	IR.12	5/23/22	Information requests shall be for one time use only. Additional uses for data will require a new request.	JB - licensign of its use, one use, baseline, mayube beyond 1-time use. Use can be controlled or specified JM - what if you know something is 1/4 or annual. Each submitted as a sep request DH - 1 req per year or some timeframe sufficient PA - some indication - has your org approved before? changed year to year? JM - grand vision - if you did have something monthly, set as monthly recurring, could be useful DH - specific req recurring, do it on a time period - this month X next month similar but not the same. Dont want scoppe of any req expanded beyond what was agreed to DR - capability JM - RECURRING important but maybe out of scope for now JB - data not being used without consent, without apprvoal, who is using it

Information Requests	IR.13	6/1/22	Information requests shall identify the path information will flow from its raw form through final reporting (e.g. carrier data store to private analytics node to Multi-Carrier aggregation node to Regulator)	PA - path: REG makes request, to analytics node, ANode requests data DH - clear where info is flowing, no side trips the data goes to, not aware of as carrier TE - openIDL will deploy everything from point you say OK, Data calls - fields that define purpose DR - leave mongo, go to adapter, then aggregated then ANode, combined/anon, TE - combined and anonymized, presumptive owner of ANode, has channels with each reporitng carrier, as each consents will be looking at pile of data from each carrier who said yes KS - 2 things, one what system sis set to do archtirecturally, then what is in the agreement of the call (consent?) TE - reqs on openIDL now, on reqs on carrier's perspective, on the ANode now, reqs for openIDL operating the analytics node for phase 2 obligations, committed to "what we do with data we got" DR - contracts are the data calls themselves TE -real world contracts DR - blanket TOS, defines things like SLAs and counterparties TE - carriers and openIDL DR - can't imagine no TOS JZ - w/in openIDL there will be SLA for stat reporting TE - SLA as part of the network, openIDL needs to become an agent DR - same verbiage can hit both reqs DH - concerned with deviating from normal path BH - data leaves company, knwo what it is going to do/go to PA - consider running ANode will be offering TOS DR - if implementation doesnt hit these, make sure - imp to be explicit JB
Information Requests	IR.14	6/1/22	Information requests shall identify the form information will flow from its raw form through final reportings (raw data; carrier summarized aggregated and anonymized data; reported data)	JB - similar to prev, relates to spec on anonymization, agg vs anon, abstrat detail identifiable. Text is one thing, code is another, some way to formalize/codify nature of call, what being requested, identifies things other than narrative statement (nature of req), analysis of metadata interface DH - one is path this is form KS - how much in the prose vs Extract Pattern, EP has gory details. When filling in req, fields req/fields output? right now data call, fill out, explain what trying, that form extended for deeper info - these are the items req, agg will happen, etc.? JB - this req indicates KS - loose prose and no form? PA - structured stuff, table to fill out KS - asking struct questions, all the things you have to ask JB - design, how to design metadata DH - may not be part of initial, will be part of final ask before final approval is provided KS - get the gist but before I approve this tell me why/what fields DH - person doing extract pattern would be able to JB - could be done in some form of survey of a page (heres what i want, looking for, data-specific not necc technical). anyone implementing call will need to know exactly what regulator wants anyway
Information Requests	IR.15	5/23/22	Information requests have an expiration date and time from which consent is needed, if applicable	DH - deadline for responding, no response = no (comes up later down pg) KS - have to know who was able to respond and interact with other req, what % of the result is travelers, etc. If 20 people say they will respond and only 4 do and travelers is more than 25% (addressed above) JB - what is the time bracket, time bracket use of info. Basis of analyzing when new reqs made - can I do this? when can I do this? If I do this when? Stages of Consent (not single date/time) PA - defining what % of the data you are submitting - raw #s? amount of cars? % total records? DH - % of whatever is being requested PA - explicit JB - # of diff ways, not fully detailed PA - by carrier, etc.

Information Requests	IR.16	6/1/22	All requests for information, its approval, the disposition of data from its raw form through final reporting shall be tracked, recorded and archived within OpenIDL	PA - where tracked and recorded? Private channels between carrier and analytiucs nodes? on chain? KS - everything on-chain except raw data, every interaction, consent, etc. PA - Eric in VA, makes data call for auto stuff KS - eric creates data call, goes on ledger, uses UI, fills out form, data call on ledger, as diff orgs interact with that (like/dislike) recorded on ledger PA - how will ind carriers know % of their data vs total data on a data call? KS - TBD TE - captured, outside of this goup KS - extract pattern put into data call on the ledger, json file with map-reduce, consents registered and stored with the data call PA - actors consenting or not: KS: Carriers KS - they will have logins to the UI based on permissions, have people able to act on their behalf PA sign in? JB Alerts and pushes. NEEDS BREAKDOWN OF REQUEST TYPES
Information Requests	IR.17	5/23/22	Carriers who participate in information requests shall receive a copy of the final information presented as well as their individual carrier results	PA - receipt + copy of the full payload DH - whatever is shared with ANYONE I want a copy JB - inc Regulator? DH - anonymized, should be able to see the whole thing, concerned about 25%, wants to see their OWN results JB - every call? clear the benefit of anon agg data is benefit to carriers AND regs PA - using openIDL creating any calls that would be bad for DH to see the whole pic DH - aggregated data only, not detail JZ - can't anticipate all, from beginning, agg data is made avail to carriers, state reports are public info, fund principals, value to carriers and they get to see reports. Can have Robin weigh in, everyone needs to know when states get info, one of the reasons why they use stat reporters in past, anything that goes to state entity can be given to anyone who requests. NOT private enterprise when discussing stat reporting JB - how would that data be returned JZ - data thru channel to analytics node where anonymized TE - goal, from arch, make it so each. node can be a data owner node and analytics node so that transactions can be chained together. Chain req together from data source to delivery. Look at arch as an actors:data owner/info receiver/network governance. Can resp to EP, stat reporting network, agg data in analytics node needs to look at that like another data set. Anon-Agg-Test for final delivery (our of visibility of regulator). Should automate AAIS role, so timeliness much faster, so EP happens, is transparent, give the Regs. JB sharing of anon/agg data, one place could be shared is the PDC of the common channel TE - which common channel? NOW - default channel and peer to peer channels. Idea - one default channel (openIDL) or another one (other networks). Default channel cant be everything to everyone unless super lightweight. JB - means for returing info to submitters and dedicated channel for that purpose (better in openIDL) - not the default channel (used for comms) but some channel dedicated for returning results TE - stat agent, executing rules for annuyal stat report for ea state, combined data doesnt have value for submitting carriers today. How do we give more value back not just info reported and compliant acc rules, but all this data that could be used by the states (loss valuation, etc) should be best data product avail (benchmarking, trends in market, etc.). Giving data back to that reporting member. Carrier could have own analyutics node, have own EP that dug into field x
Information Requests	IR.18	6/1/22	Carriers decide in which information requests they will participate	JB - given with the disc around consent, summary of reqs DH - up to the carriers to participate OR assumed to participate
Information Requests	IR.19	6/1/22	Carriers must provide an affirmative response prior to any information being extracted to the private analytics mode	JB - along with IR.18 (consent on record)

Information Requests	IR.20	5/23/22	Final reports shall be archived by OpenIDL for 3 years	JB - network of communication and collab, who is doing archiving (analytic node? carriers have their copy? cloud archive?) - identify is every member responsible for their own archiving. openIDL is the network. DH do we need a data center? PA - archive means a place for archiving JB - ID how accomplished, more than one requester of info, what is a final report, mult requestors, people providing info to diff requestors, one of the issues - is private data collection used for things in transit, complexity DH - is openIDL just a network or is it also an intermediary? JB - resp for maintaining, monitoring is this something that becomes a cost factor, if it is archived does it need to be accessible? cheaper ways to do that if not on chain all the time. Need to look at who might provide archival process. Role question. SB - risk and liability? JB - if archiving is of interest, each. node archived each org could do that -WHY? what reasons for archiving. Needs more detail JZ - diff conversation, idea of archiving beyond scope of openIDL, behind carriers holding data, disppears after the fact and hash - outside of scope of RR JB - outside of initial scope PA - three years after time generated DH - published
Information Requests	IR.21	6/13/22	Information requests should be testable. Should be able to execute a dry run and know exactly what would be returned if the data call executed	JB - seem to occur anyway if you have something to be run to begin with, ought to be able to do it in HDS and test PA - setting up testnet for us to und cost to op network - talk about a POC HDS or generic HDS, test environment? JB - intent of this item, a per req basis, request should be testable - talking about if you do get a data call or info request, test locally to see if it runs - looking for test facility for data calls and extracts? or verify executable? DH - didn't add it KS - consent to something, need to know what you will return before you consent PA - dev/UAT/Prod looking to maintain in openIDL? JB - sep subject - know what you return on a req by req basis KS - fits a prev req - see just what they are returning, a dry run
Information Requests	IR.22	6/21/22	NOTIFICATIONS: Carriers, Regulators: New Data Calls, Consents, etc. (*TBD)	what groups of actors would receive them, approve vs evaluate push-pull subscribe will generate more reqs
Access and Security	AS.1	5/23/22	Carrier's raw data will be "walled off" from other entities with access only through permissioned protocols	Straightforward requirement, w/in Carrier HDS KS: multi-tenant node as well? logical JB - yes SK: analytical node? same concept? per carrier? JB - raw data IN the carrier node KS: know the data comes to Analytics node carrier-identified, want to make sure no one has access to that data w/in the ANode JB - NO access to raw data, doesn't apply to analytics node DR - once on ANode, not wide open, still some permissioning, implementation and access will be different KS: Sep req - aggregated data, what shows up on ANode, confusing raw data DR - still a need, just b/c outside CarrierNODE still needs to be defined JB - qualification - raw data, implies on CarrierNODE SK: clarification to Dale - raw data on carrier side or raw data could mean ANode, aggegated? JB - concept of raw data is HDS DR - catch all term - carrier identifiable data only accessed by permissioned protocol JB - best to deal with life cycle, when data does move DR - if Lifecycle changes, dont need to keep changing requirements DR - ANY carrier data must have permissioned access pattern of some kind - never just open - still needs controls (even in ANode)

Access and Security	AS.2	6/1/22	Carriers raw data shall not leave its control - a secured limited access "private analytics node" may be established for processing information requests	DR - think DH referring to the adapter, raw data shouldnt leave but might need to be a mechanism to access raw data JB - API adapter to access the data PA - hold this for a tenant, how does ND with the VINs go? Fact we hash the VINs, make this still workable? KS - VINs are result data DR - not sure ND is a violation of the tenet PA wants to revisit KS - is a VIN PII? Heard "no" it is not, could be returned as a result of an extrax, not have to be returned hashed JB - anonymize w/ encryption, comparison with DMV, compare equiv VINs and policy data KS - heard not necessary JB - raw data not anonymized KS - stuck on "private analytics node" - raw data? JB - adapter that interfaces with the HDS at the Carrier node, in the Carrier permiter, separates Fabric request by not having directly on CarrierNode, but thru extrax pattern to get results. KS - boundaries still in CarrierNODE still? JB - some adapter with API, where reqs are made thru well-defined channels, nature of which not entirely clear (get data in serialized fashion?) - not that difficult once est extraction request and get the data
Access and Security	AS.3	6/1/22	If multiple information requests are being processed at the same time, separate "private analytics nodes" with separate access shall be employed	KS - "private analytcal nodes" ? JB - each a sep channel/protocol of an interaction, each request has its own logical management DR - concern, if you approve mult reqs, access diff data is fine, in theory AGGREGATION could pull datasets together KS - no crosstalk with extractions JB - sep logcal worlflow of each request SK - for each data call data set is different, 1st = combined prem for zip, or 2nd could be somethign else, - saying those two cannot combine the data while the data call is being serviced? KS - PERIOD - time irrelevant, no crosstalk JB - think of it as sep channels KS - logically seperate JB - API not fleshed out, needs to be, est conversation ID for a data call SK: little bit of solutioning - can one API service all data calls - flesh out - how do we sep all data calls KS - function gets result JB - same API, mult instances DR - preclude - long lived node, caching every data call ever made, prohibited by this req - ability to return. Req woould throw that part of the arch out JB - adapter not a cache DR - not getting to how JB - stipulation how data utilized, combos occur, lifetimes
Access and Security	AS.4	6/1/22	If multiple information requests are being processed at the same time, the data for each request will be segregated	Jb - saying the same thing as AS.3 DR - maybe not just the node but in transit, maybe broader DALE - not having the data comingled and access to that data (in flight, not raw) comingled with other information requests KS - dont want two extraction patterns to interact or crosstalk - cant talk to each other about what they have
Access and Security	AS.5	6/1/22	Carrier data may be transmitted to a private analytics node only as the result of an approved data request via a permissioned access protocol	Jb - goes back to the concept of consent - we might want to suggest a substiturion for private analytics node for "API CHANNEL" - avoid sep node per se - - unless we all accept priv analytics node DR - Ken's use of adapter works JB - workflow adapter or interface DR - INTERFACE KS - heard this as not the same as before - what we called the adapter in prev - this is the ANode KS - "inteface" in that req means DESTINATION in terms of data CLARIFICATION FROM DALE - it is the interface, transmitting of data beyond HDS, basic fund of thru permissioned acess and thru a data request THAT HAS BEEN APPROVED JB - priv channel between carrier and ANode -priv channel? YES Dale - convo Ken and Dale have had, little bit of solutioning - where does the data land when it leaves the HDS JB - connection/relationship between carrier and ANode where it is kept private KS - PRIVATE CHANNEL JB - not the adapter, Private channel to ANode Dale - not leaving HDS w/o permission
Access and Security	AS.6	5/23/22	Carrier data may be transmitted to a private analystics node that has been aggregated and anonymizated through a secured protocol	JB - already talked about and accepted, maybe AND/OR anonymized, def have to have some means of disintermediating them

Access and Security	AS.7	6/1/22	Carrier data in the private analytics node shall only be used for the purposes for which permissioned access has been granted	JB - similar to reqs above (SEAN)
Access and Security	AS.8	6/1/22	Carrier data in the private analytics node shall be immediately purged upon completion of the processing for which permissioned access was granted	JB - similar, cert period of time was allowed to use that data along with permissioned access - license to use for reporting purposes JB - node collecting this for analysis on behalf of carriers SK - does this mean Data purged after every data call is serviced? JB - period of time intended for data (ad hoc, ongoing report) - use is only for request, nothing else - can see working on long running report, data every quarter, not just when you first receive it - concern - not to accumulate lots of data b/c available - must be specific for request SK - timeframe? Data calls perpetual? DC today, how long is it needed? JB - talked about specification of meta data that subscribed request (rentention, etc.) - Recurring call, mult times per year or adhoc for incident, would be described and part of the making of the data call - longer running or recurring, understand but not used for anything else
Access and Security	AS.9	5/23/22	No Personally identifiable information (PII) data shall be transmitted	agreed SK - exceptions? meaningful dataset w/o some PII JB - provenance of PII, out of your control if it leaves your perimeter - PII not transmitted is a safe assumption KS - changes transmitted to "outside carrier control" JB - *NO PII* shall be required to leave the carrier KS - dont want to say "cant be in HDS" because it can be - when it leaves HDS it would not be in there - HDS has data avail to extraction, PII could be in there
Access and Security	AS.10	5/23/22	No altering or embellishing data including appending outside data is permitted throughout the processing of the information request unless approved by carrier	JB - carrier may have outside info it can use, if willing to submit, but once collected it would not be done AFTER carrier released it KS - carrier has to approve it SK - good requirement KS - would be in the extraction pattern - known thing that has to happen, approve ExtraxPattern you know the embellishment would happen - embellishment would be part of the extrax pattern
Access and Security	AS.11	5/23/22	No changes to request, attributes used, extraction patterns, accessors, users, or specific use of the data is permitted post consent	KS - works diff right now - not really conset makes it immutable - makes it the issuing of it that makes it immutable - locked down - after ISSUANCE it is immutable JB - no changes to req can be made after its issued, could be when a req is issueed, modification of request based on feedback KS - thougth thru during prev design sessions about flow - when you issue that vehicle version it becomes immutable on a blockchain JB - procedure for revising - versioning of the requests? KS - make that a requirement SK - making it immutable through life cycle is a challenge, putting digital rights on a payload JB - not the results it is the REQUEST KS - Dale discussing request data
Access and Security	AS.12	5/23/22	Only authorized approvers may commit carrier to a data request	KS - two layers - auth org (carrier) and then the users INSIDE the org - Dale looking for permissions, credentialed roles, etc. JB - will involve identity and credentialing - needs review
Access and Security	AS.13	5/23/22	Data request communication shall be through a communications protocol within OpenIDL and archived within OpenIDL	JB - what Fabric does with chaincodes sending out and getting responses KS - second half adds something JB - written on chain in gen channel, where archive of the requests is KS - log of comms JB - general channel of the Fabric blockchain would have it, artifact of comms protocol being used KS - could this be said as the "communications are auditable or logged" JB - instead of archived? KS - archive is specific, hard to get to JB - through an auditable comms protocol, opp to say "hey lets do this on blockchain" comes with the request KS - application needs to use blockchain correctly to do this

Access and Security	AS.14	5/23/22	Individual carrier contribution to a data request will not exceed 15% of the population of premium, losses, exposures, etc. for a given information request	SK - good one, how to measure KS - have to provide what metric to say "15%", has to be specific to data call which threshold not crossing JB - may want to say "defined % of contrib based on nature of data call" KS - metric has to be specified, dont care about premiums then needs to somethign else JB - % AND metric SK: unless carrier provides data will not know 15 or 20% JB - 2 phase consent - generate data set, then look at it compared to others and decide if you agree to continue ANode would have to perform that service - 2 phase consent SK - "as of this datte, this is the % of..." JB "in this slice of time, these are the results"
Access and Security	AS.15	6/1/22	OpenIDL is responsible for fulfilling multi-carrier information requests including extraction patterns, aggregations and formatting of final reports	JB - monitoring the network, saying openIDL is responsible is misstated - needs to be rephrased - DESIGNED to fulfill SK - given, implicit JB - openIDL governing network - mult sub-roles to be fullfilled
Communication	C.1	6/1/22	All requests for information via OpenIDL will be through a secured communications portal within OpenIDL	PA - Angular JS? KS - requests for information? Extraction? Data Call? Extraction Pattern triggered by data call? JB - make the req at API level or protocol for extraction PA - why/how being secured Beak it apart tomorrow
Communication	C.2	6/1/22	All communications will be written (electronic) and be archived by OpenIDL for 10 years	PA - kinds? Nodes talking DH - request, approvals, final reports, etc, maybe auditable? PA - banking, held all for 7 years, is 10 years industry standard for Insurance? DH - put it down, up for debate PA - bound, delete everything? garbage collection after set date DH - internal record retention reqs, not sure if industry standard JB - archived by openIDL - who is the party, actor w/in who would do that? Comms or requests, on common channel, written on blockchain and stay there but data transferred to ANodes, sent thru private data collection repos, used as buffers to send data, who would be resp for archiving data payloads sent for reporting purposes? ANode? any ANode involved? PA - seems like a funct of ANode JB - openIDL is the network DH - question last time - is openIDL a network or is it also an intermediary? JB - openIDL, org governing and certifying / monitoring network, archival process agreed upon by the producers and consumers of data - gets into agreements that exist between makers of data extract reqs, and receivers PA - come back to, mult ANodes, person in charge a a specific node has control over what it is doing. AAIS is one, doing state auto coverage reports, resp for keeping those records (jsut like today). State of VA, making adhoc calls, would hold levers and switches for those calls and results JB - requirement may not be able to be sustained for all openIDL participants - MORE SPECIFICITY NEEDED KS - better define communications, lot of diff comms happening in this process, some are def happening on ledger, some not. Ex: the "why"s omeone doesnt like a data call could be resolved w/ a telephone call, do we want to define what parts are archived clearly DH - ties back with info req, whole info req, whatwever means to comm the internt and fields, not necessarily data, this is the back and forth going thru the network JB - did discuss clarification, consent, all those things on chain, as long as chain maintained should be there KS - stil nuance, hit things like "unliked it" without context, you dont hear chitchat b/w parties about why. Very different level of auditability DH - written comms thru network, whats archived, verbal = not JB - not trade desk recording for audio calls KS - whatever info captured on data call itself and events (consent, like, etc.) network activity
Communication	C.3	6/1/22	A non-response to a request for information will be considered a decline to participate	DH - dont want assumed participating KS - in order to say, require/decline you have to know who you expect to respoond. Respond? IN JB - no response to request is NOT considered consent DH - dont have permission to do it JB cannot book as decline KS - already know ND, ND wants top ten to participate, id 10 they want answers from, feels like req that the regulator, can put in there "I expect you Carrier X Y Z to respond". Is there a req to define who you expect to respond "we cant do this if you 10 dont respond". JB - could have equiv of consent list, not everybody on the network, req of type might be for participants listening to it, think if theres a mult set of people in the community make req to, req list (mailing list style). From consent protocol - **non response is NOT considered consent.** Assumption - need to ID who you are waiting on consent from.

Communication	C.4	6/1/22	Requests for information must come from an authorized representative of the requesting body	PA - define various roles in requesting bodies, some who have access to machine who wont be auth to make request, what are the roles JB - credentialling and validation of requests, consents the same DH - who at the insurance dept can ask for data or information JB credentialing, passed on along with data call made on behalf (intermediary w/ ANode)
Communication	C.5	6/1/22	Requests for information must state the regulatory authority for the information being sought	PA - statute for extract pattern DH - sometimes market conduct, need to und that (diff protocols in company) - not obligated to provide info just because someone asks for it - must be legal means for someone to ask, for internal audit need to und what that legal authority is PA - walk thru, auto coverage report, 50 states doing business writing auto in, 50 reports turned in, each state ind needs to give justification why each wants it? DH. - stat reporting not right for this, but a data calls (like Hurricane use case from ELowe) JB - req from auth commissioner, as long as authorized DH - get person and statute TODAY when they get data calls - PERSON AND STATUTE **NEED REGULATORS INPUT ON HOW CALLS ARE PROCESSED** DH - dont want to support fishing expeditions JB - if regulator has auth to ask under compliance requests, whats involved in the regualtor specifying, input from AAIS would be helpful
Communication	C.6	6/1/22	Agreement to participate in a request for information is conditioned on OpenIDL providing the carrier the proportion of data that carrier is providing to the population of data	Jb - 2 phase consent PA - more solution based discussion, not just a giant neverending "carrier 7 bailed" issues Jb - cant move to processing until you get a quorum of carriers PA - not sure, lets say REG makes req, Dale calls them up, need Req - REQUESTOR CAN CANCEL A REQUEST BEFORE IT IS FINISHED DH - need that requirement
Communication	C.7	6/1/22	Final agreement to participate in a request for information is valid once received by the OpenIDL communications portal	DH - comms side of the requirement - at what point is it considered a valid consent? when received by the portal. Need date and time
Communication	C.8	6/1/22	Final agreement to participate may be recinded up to an hour after final agreement is received by the communciations portal to affirm participation	DH - some facility to change your mind (stop the presses), mult reasons (error, etc.) JB - introduce the cutoff by which things would be in motion, biz process cutoff, DH - dont want someone starting on it, fat finger rule, undo JB nature of the request and how quickly acted on, received in the hour, take a week to start - whats the nature of the request, some timeframe, time to change mind after x time, depending on what time of call it is GW - rescission timeframe KS - odd requirement - most systems give you an "Are You Sure"? Not saying bad, but odd DH - "YES" and boss says you shouldnt have done that JB - req could be, abiliity to rescind as long as possible, depends on timeframes work would be done, specific to call, no generic 1 hour grace period, some calls quicker to process than others, window is not constant for all calls DH - hour is a placeholder (TBD discussion) JB - flash crash of may 2010 - cancel reqs didn't get through - we dont have those types of realtime probs GW - business process? JB - per carrier, per policy of carrier
Information Requests	IR.23	6/28/22	The requester can define what organizations should respond to a request.	KS - REGS can compel? DH - can compel, but not required to go thru openIDL, can go to state directly, JB - if they want to use openIDL, gen case all carriers KS - another requirement?
Information Requests	IR.24	6/28	Requester can terminate a Data Call prior to release of final report(s) at which point all data about that call would be deleted, while communications about that request would stay intact	'
Information Requests	IR.25	6/28	Carriers do not have to respond to a request via openIDL. They can go direct to the state (out of band)	KS - do they need to log in openIDL that they went out of band (new Requirement under communications) DH - no response same as a "no" (see earlier reqs) KS - no need to log they have gone somewhere else

Operating Infrastructure	OI.01	7/8	openIDL.org (foundational network) includes ability to test a fully functional mock version in a non-production framework, in addition to running a production-oriented one	JB - Testnet place by which people can either investigate - sandbox etc. - system testing can be done - sans impact on production, deployment of same resources and use of same code. Mainnet is the main openIDL network. DR: Is it always possible to meet this requirement? Feels like an implementation detail, not a requirement. JB: Inclusive, not exclusive KS: Danger of implying **one network** - as opposed to multiple JB: idl governance per se covers both test net and main net JB: Simply stating that what we're trying to do here is part of openIDL organization PA: this is saying openIDL should be highly testable. (Capability to test in a non-production capacity). JB: openIDL predicated on hyperledger fabric as a means of communication.
Operating Infrastructure	OI.02	7/8	Mainnet is the live openIDL network and is the sum of the Nodes, Data, Data Calls, Extraction Patterns and Smart Contracts that make up openIDL	DH - mainnet and testnet - solutions rather than reqs.
Operating Infrastructure	OI.03	7/8	Entities that can operate Nodes on openIDL are Members, Associate Members, Infrastructure Partners and openIDL (the organization)	
Operating Infrastructure	OI.04	7/8	Only approved entities (Members, Associate Members) can request, access or process data from openIDL	refers to IO.05
Operating Infrastructure	OI.05	7/8	All entities “on” an openIDL community must be approved by the GB and TSC after evaluation and due diligence by openIDL (Policies and Procedures to be developed)	KS - more than one network (collection of participants in a particular biz case) - currently stat reporting, only SR network - mult networks with mult gov structures - more generic than mainnet JB - TSC and GB calls (recent) - able to manage the communities - reqs for joining openIDL are still some level of validation, joining an app community depends on what those reqs might be - not a decentralized anon org - some need for openIDL.org to coord and orchestrate procedures - monitor and govern - using fund network infra, one org could be member of different communities, activities and roles specific to that application KS - each community may have its own GB and TSC JB - talking about openIDL's network (anyone can run the software). Communities can have own boards/procedures, not as if someone at GB is approving apps KS - setting context of openIDL single community - couching reqs in context of stat reporting JB - reqs is to recognize reqs and stakeholders, dont get hung up on progress
Operating Infrastructure	OI.06	7/8	**<Network>** will run the most recent, stable build of openIDL codebase	

Operating Infrastructure	OI.07	7/8	All updates to openIDL (patches, critical vulnerabilities fixes, software upgrades, modules, features, capabilities, etc.) will be coordinated by openIDL and require subsequent approval by openIDL Maintainers and then openIDL TSC	KS - update mainnet, participants not controlled by openIDL, hosted or on-prem, has to stay in sync JB - not things you do in lab/rapid change dev, changes to data standards and network configs, few and far between, objectives to have the types of things take place amongst community of collaborators, max felxibility and timelines, specify these are not a way to maintain a single application, coordination KS - big non functional requirement JB - not the kind of thing, every other day notice from your browser "time to update" DR - territory - work, always avoid breaking integrations, never be forced to make an update w/o lots of lift, goes to arch, what lift do I get out of being connected 24/7? Needs to be convinced by connected 24/7 - how many nodes need to be up at a given time? JB - how much a node needs to be active to resp to traffic vs how much work to be done - different - DR - 5 carrier nodes, whats the consensus? Fabric - KS - we decide for ourselves what consensus is DR - 5 and 3 aren't online, cant make writes, not enough approvals KS - not making consent at ledger level, consent in the application, putting an event onto the network, not expecting all to run chaincode, etc. - consent needed to do a report, respond to a request JB - consent needed to write a block to a chain, DR - some extract pattern, sucked out of HDS, aggregated, put somewhere, some record writtern to blockchain - not majority of nodes avail, wont happen, not enough nodes, or say so trivial so few on, passes by default - if not 24/7 uptime whats the point? Stateful vs Stateless argument - requires ops team, on call, which a lot of integrations dont need - asking "why? where's the value prop" - looking "ops-y", someone at Travelers needs to not just send data out but someone to respond, patch, someone on call, no negligible hit - or pay someone to run node for them, not cheap, understand reqs, almost pre-supposing need for that exists KS - codify - shouldn't need that DR - doesn't think we should, hasn't seen whole solution, get all funct reqs, maybe need - hasn't seen it, not saying "we can't" KS - dont want to be up 24/7 JB - 2 diff levels of activity, listening, what it takes to maintain the network itself, communicate at system level, what the level of timeline request to get back information - asynch interaction, distinguish between both, not a trading system, business level, processing or responding can be asynch, with fabric you can designate what blocks can be written DR - then why? ordering BH - right place to have that conversation? JB - other reqs for network to function, may not be 24/7 it might be M-F 9-5, not doing "heartbeats" every second, DR - NFR avoid any need for on-call or pager duty JB - ob jective to minimize operational overhead, biz req for how freq req needs to be responded to vs network responsiveness DR - regional carriers and smaller players, not wanting unfunded mandate, low barriers to entry, minimal numbers of nodes required JB - solutioins where service orgs can help with this, reduce the overhead or costs of that listening, und more what are the actual reqs for network integrity vs timeliness
Operating Infrastructure	OI.08	7/8	openIDL SLA TBD	
Operating Infrastructure	OI.09	7/8	Testnet is a secondary openIDL network used for evaluation and testing	
Operating Infrastructure	OI.10	7/8	Testnet is a subset and will include a smaller number of nodes than Network depending on the use case and testing	(duplicative)
Operating Infrastructure	OI.11	7/8	All code changes will be tested on Testnet and approved (Maintainers and TSC) before being deployed to Mainnet	(duplicative)

Operating Infrastructure	OI.12	7/8	openIDL Testnet and NETWORK may have a code “roll back”, with notification and approval of TSC, at any time to a previous version	DR - irreveribility not a feature its a bug - no reason to let mainnet not work JB - redeployment from prev version, to do that with a blockchain that is immutable, open question - code deployment DR - if there is a mistake, records are fine to be corrected - NEEDS to be on MAINNET - usually fixe with a new release, etc. KS - what if it is the ledger? rollback of the ledger? why other networks always go forward? New vers of old code doesn't break new stuff DR - double spend, permissioned blockcagin doesnt need feature, altering write log, can change, records and audit trails, design constraint using somethign immutable JB - the types of data structs in terms of on-chain might not break, whats written on blocks fairly minimal KS - written on ledger is data call, has structure, params for start and end, new code to support new params and data calls from UI, interdependencies between code and whats on the ledger JB - app logic, diff aspect of network infrastructuee, need to identify different levels of changes, here talkiung about actual fabric KS - upgrades to fabric itself? JB - rolling back network code vs app code, not talking rollbacks and fixing things DR COULD IN theory have bad code that can't be removed, problems of their own, biggest prob with blockchains is inability to rollback with code problems - dont need to replicate that here if we can avoid JB - Fabric code that supports fabric itself and the versions
Operating Infrastructure	OI.13	7/8	There is no SLA for Testnet.	There IS AN SLA - notification - combine OI.14 and OI.13
Operating Infrastructure	OI.14	7/8	Any downtime for Testnet will be communicated via TBD openIDL mailing list	
Operating Infrastructure	OI.15	7/8	Prospective members can use the testnet to understand openIDL, must be onboarded by openIDL team (process TBD)	
Operating Infrastructure	OI.16	7/8	Nodes are the infrastructure that makes up and powers the openIDL networks (mainnet or testnet)	
Operating Infrastructure	OI.17	7/8	All Nodes are activated via the openIDL Certificate Authority following approval by the openIDL GB (Business/Legal) and openIDL TSC (Technical/Operating)	JB - after due diligence and validation procedures DH - what the resp of the GB and TSC are in evaluating these new members/nodes (REQUIREMENTS NEEDED)
Operating Infrastructure	OI.18	7/8	All nodes must be maintained by Node Operators (by or for Node Owners), are continuously monitored by openIDL, and must remain in Consensus at the approved TBD rate	KS - not a human governance question, tech ability will determine governance issue
Operating Infrastructure	OI.19	7/8	All Nodes are based on the openIDL Fabric implementation a. Existing version: TBD	

Operating Infrastructure	OI.20	7/8	All Nodes can perform the following operations (TBD final node architecture) but any node's capabilities are based on their approved role: 1. Monitoring/Telemetry Operations a. View the existing network status b. Pull a report on the health of the node c. Pull a report on the health of the entire network d. Automatically Report Node health statistics to the Monitoring Node (openIDL) 2. Carrier Operations a. Receiving Data Calls (request receipt) b. Evaluating Data Calls (human readable) c. Responding to Data Calls (Accept/Reject/No Response) d. Contributing Data (TBD Requirements) e. Storing Data (TBD Requirements) 3. Statistical Agent Operations a. Develop extraction patterns b. Distribute extraction patterns c. Implement extraction patterns against Carrier submitted data d. Package aggregated data e. Submit Carrier data to State Regulators ABILITY TO PERFORM A FUNCTION IS ROLE BASED AND ALL ASSIGNABLE ROLES ARE MANAGED BY THE GOVERNANCE MODEL	PA - #1 any particular node, using UI carrier node and AAIS node - not every node can run extract patterm KS - node same, but operations different, from network perspective, all should act the same but funct or application can vary (permissions, deployment footprint, etc.) PA - positive rejection, "not responded to" will we log it as ? JB/KS - will default to rejection, maturity time of a data call DH - major point - w/o affirmed approval not to be assumed it is approved KS - allow to say no but don't have to - carrier ops feels redundant KEEP CARRIER OPS - REFINE PA - how much of a role defined for SA in this network? Mature state regulators making call, wasn't sure SA was making all EPs KS - current rules SA makes EP, carrier can like/Unlike/consent - regulator can create and update data calls, permissions based on roles - gone thru process - regulator creates data call, carrier like/unlike, negotiated, issuances, stat agent and carrier consents JB - regulator makes request that makes sense to them and SA makes an extract pattern that fts, State may find someoen to do that that acts on their behalf - proxy EP dev, need to cert those participants part of due dilligence DH - we should have only one stat agent handling data call - wouldn't want mult SAs, mult EPs and diff results for each SA KS - only one place for EP, need to consider, mult SAs in the process could overwrite each other EPs, need to consent at the end of the day, couldn't have mult EPs on the same data call JB - a state might have someone help them with an EP - trad sense of reporting DR - worded vague - capable/allowed? Carrier shouldn't have EP write capability KS - EP dev is part of a role JB - governance and accepted by Carriers on the network, accept that a cert agent can write an EP DR - tech capable but not enabled JB - permission and acceptance by community DR - all nodes do all things? bad JB - set of agg data might be of interest to a carrier, might query something as a future benefit to carriers DR - all nodes all capabilities, unless you have a stated use case you dont have that capability - cant write EPs w/o a reason JB - must be accepted into role - GOVERNANCE REQUIREMENT TO CERTIFY A NODE'S ROLES
Information Requests	IR.xx	7/11/2022	Support the notion of what use cases are supported by the data in the HDS. HDS data is not good for all purposes. When creating an extraction, one must know that the possible consenters are able to respond.	KS - know the current use case (stat reporting) - if only Stat reporting no need for this req, but other data calls need indications for whats required per data type - future use cases will require new scope (MVP or not, etc.) DR - captured in some of DH's reqs, ("describe data you want") KS - leave it here and compare/review DR - dont know how to track to this - how do we say "done"? KS - know covered when stat data doesn't support, support it - system can capture the knowl that you are able to respond to a data call - assuming stat data, a stat report will be satisfied, when we go beyond, things required that might not be in the stat data, beyond scope of current MVP, to satisfy means we are able to define somewhere in the process, a set of data required to fulfill this data call and the carrier is able (consent?) JB - one is more of a, new apps? und data for that initiative (strategic vs tactical/immediate) KS - not for MVP for stat reporting DR - not all carriers will put the same data in THIER HDS above and beyond what is required, how will evolve, wont get every carrier to put same data beyond whats req by obligations, whole thing pushed to data call/data extract/governance process - base level stat reporting: heres what you need - every call built off base data or addl request - cant have requirement to have more data than data call and then carrier must consent PA - would it be a good exercise to go thru reqs, id which are stat reporting vs network as a whole? what applies to every application? DH - could but these are the reqs as we start solving specific arch for stat reportings, see network vs app, taking note as we go, do need to track, now decide how we show risk to reqs and hit them - simple column or complex (rate risk to reqs) - next step - how do we show we met the reqs, figure out as we start solv ing the stat reporting arch JB - most reqs are network as a whole, stat reporting example for that that entails - new funct, new reqs, need for planning for new apps, discussed notion adhoc queries, data calls made, data in those calls are whats stipulated to get consent - DMWG stat reporting is defined DH - data store needs to be extensible in some way, rest (gov, process, consent) - tech requirewment: db shouldnt be overly structured where you cant add or remove data without breaking things JB - org and collab req, process for considering intro of new aspects to the model as an ongoing process DR - tech req - boils down to cant build something so locked down you cant add - gov stuff later, PA - one thing, ahead of, as ND takes off, get engagement from new carriers and application - make sure they dont torpedo what we are doing, diff use cases, ways we could show clear sep between what we are doing and other teams in next 6 months BH - worst part is, lot of people banging up ahgainst stuff, we need to stay focused and do what we are doing, keep ND sep KS - tomorrows TSC, talk about how we track diff threads, dont get muddy on the tracks - need to know whats going on with ND, nto take down this project

Non-Functional Requirements	NFR.01	7/18	Operational costs should be minimized - minimize on-call requirements	KS - minimize always on-requirements and operational costs PA - see "minimizing costs" - what does it mean? DR - squishy KS - reqs like "always on" - not a tight req DR - decision on 2 arch, network reqs always-on and one doesnt - unless a need can only be satisfied this way, "this is the better approach that meets NFR" - should be looking KS - should not require always-on? as a req? DR - love it, not always-on from ANYONE's perspective, even if we outsource to vendor or provider, it is EVERYONE - no 24/7 need - not sure we are ready PA - doing cost saying wherever possible, need to add KISS as well, JB continuty of the network at a minimum level, maintaining code presence, DR - perform some action, no consideration needed if someone else is operating or not - ex: I need to write, I shouldn't worry if there is a certain number of carriers or regs on - naked internet - connectivity on the network and it should work - availability always but shouldnt need consensus mech - write at any time, not worry about # of people there to write data JB - part of the issue - what extent does tech require levels of connectivity DR - if we start getting forced to have complexity in terms of "how many nodes", whatever, makes it the point "this is not simplest" JB - cost of listener listening, analysis needs to be done KS - current wave we are using fabric, AAIS node or comm node would be always on DR - end point always needs to be there , boil down to a simple requiirement that import needs to be there, thats it, measurable and simple PA - endpoint? DR - agreed to it but not enough quorum, but didnt go - PA - your submissioon indenpendent of someone elses submission DR - not needing a NOC or a lot of analysis of network health helps too (indirect or direct way) that helps (need something on to write to) JB - more tech eval than actual reqs of the protocol DR - figure out as we are building, north star to say "lets simplify", but not directly measure
Non-Functional Requirements	NFR.02	7/18	Runtime should be minimized - don't require constant running processes that cost non-trivial amount	DR - nuanced but captured KS - specific req about always-on DR - reads more as, w/in arch, once minimized and simplify that, thinking about more granularly, determine network arch and topology, minimize resource usage within "no heartbeats needed", etc. KS - intention - dont want constant running processes where we need to be, Fabric requires one place, but not disagreeable to community, single node on AAIS node JB - gets back to tech, KS - 2 things, 1 - david brought up to load data - could be a lambda (inexpensive) or fabric has challenges with serverless, fabric has certain reqs to minimize needs for constant "on" DR - make Arch to minimize the reqs for maintenance, and once decide big picture, design individual implementation to min the need for polling, processes, serverless vs., etc. - make last one real at implementation level JB - diff aspects to the cost DR - decide network doesnt need 3 modes to write - just needs one - how do you build that one node? second one - how to build in most efficient way, EC2 response or some listener triggering lambda - one more cost effective, implementation details A. Arch clean and simple B. then cost effective / lasting JB - not just single node central solution
Non-Functional Requirements	NFR.03	7/27	Use the simplest possible solution (KISS)	
Architecture	A.1	14 Nov 2022	The architecture is documented to the satisfaction of the TSC	
Infrastructure	I.1	14 Nov 2022	The software can run in AWS	
Infrastructure	I.2	14 Nov 2022	Carrier nodes can be hosted to the satisfaction of carriers.	The node can be hosted internally by those carriers that require full control. Acceptable hosting options can be found for carriers that find third party hosting acceptable.

Next Actions on Requirements:

- PA - need to get reqs appoved, in some way, eval current arch against reqs and defining gaps
- JB - run thru to understand, another pass is needed for which need to be held as "understood" vs "more work" - dont just accept all of this, need to und a pass "which really are key and how they affect us"
- DR - doing, these are the requirements, these are them
- JB - we weren't voting as we discussed - review/compliation - restating? some degree, going back, looking at them, what needs further discussion
- DR - re-litigating? wrap process in as we start building, may not meet every one on the first pass - risk to reqs analysis - change the req or change the architecture, can't get right on day 1 - dont want to go thru list again and relitigate
- JB - anyone feels there is something to address, get feedback
- BH - live together?
- JB - homework, see if something needs clarification, discussion on as-needed basis
- DR - captured int he build process
- PA - take a week or two, all review?
- JB - some very clear, some had discussion, objective to get thru list, discuss, open items, imp for us to all take a look
- DR - hybrid - moving forward assuming this list is right, anyone wants to bring up "this doesn't feel right", but lets not hold start of Arch Definition to wait for that process - looking heavily over next couple of weeks - do it in context of defining the Arch will get better results
- PA - standing first agenda item, if someone has a req to discuss, give a week to review and then discuss
- DR - makes sense, still come into more focus as we build
- PA - define arch in way we feel comfortable
- KS - do we want to follow a particular process people like for defining architectuere (KS is not dogmatic), does someone want to put forward a process they prefer to use?
- PA - I like pictures and diagrams over huge things of text
- KS - scenarios to support, funct req and tech req intermixed, define some business scenarios to walk through
- PA - auto coverage report?
- DR - start there, dont like trad sequence diagram or trad flowchart, once scenario defined, big fat block, mixes process and arch, says clearly where do things live, what processes pull out, ref business process KS and PA mentioned
- JB - stages
- DR - reqs + stages is messy
- KS - break it into scenarios, start with bullet list, as we see better ways to describe scenario, take and draw arch, need to come up with scenarios - has scenarios of a data call, how diff from stat reporting, as we walk thru happy path, get other cases, etc.
- PA - high level: loading the raw data, regulator making data call, carrier responds to data call
- KS - creation of the request, then consensus mech of agreeing to or not consenting to the form of req nd then the creation of the actual code to the EP and then creation of report - arch of where those things happen and if they are meeting those reqs
- PA - final stage, getting into ELowe's hands, figure out vehicle for that, not sure if all regs are interested in data calls, can subscribe to resources for data calls, 50 states with diff target for reports
- KS - will bring bullet list of steps for rough data calls, work on that in next meeting, get comfortable level, iterate on both, have valid set of use
- PA - DMWG call Friiday on inputs and outputs, how report created
- KS - est assumptions, stat plan is initial format, clarify over time
- KS - feels fluid, continuous discussion - get to HDS when we get to it
- PA - dmwg - keep working, can do some data model discussions in Friday call - diff audience
- SK - approach looks good, need to start digging into Arch, on
- PA - any value to meet with chainyard or David's guys, discuss what they like and dont like from deep code level? start with clean slate
- JB - when the need arises, bigger pict and drill down
- KS - green field
- SK - order or prioritiization? all must-have? discuss in process
- KS - see this challenges some reqs (change req or go back and ponder more)
- JB - some reqs more importance than others, will come out
- DR - trad risk-reqs process (w/o scoring systems) - see it as ad hoc process

Time	Item	Who	Notes