On behalf of Iron Mountain, the largest provider in the world of registry and registrar data escrow services, I appreciate the opportunity to comment on Draft Applicant Guidebook Version 4. The following comments pertain specifically to Specification 2 Data Escrow Requirements.

Part A – Technical Specifications

Section Specific Comments:

1.1 The Specification states: a Full Deposit will reflect the state of the registry as of 00:00 UTC on each Sunday. This implies that all registries will make their Full Deposit sometime shortly after 00:00 UTC on each Sunday. Having the same Full Deposit time for all new gTLDs can create a significant technical bandwidth burden on the Escrow Agent if it escrows a large majority of new gTLD data. This potential problem can be mitigated if this section instead states the Full Deposit will reflect the state of the registry as of *time* (UTC) on each *day* as mutually agreed on by Registry Operator, ICANN and Escrow Agent.

2. This section states: The formatted, encrypted and signed Deposit file(s) must be sent, by authenticated, secure file transfer. The section is in disagreement with Section 4.13(5) of Part A which says "This specification does not require any particular transmission mechanism", and "acceptable options would include electronic delivery…delivery of a physical medium….or USB storage devices as agreed with the Escrow Agent." Iron Mountain's recommendation is the Specification requires electronic escrow unless approved by ICANN. It is very difficult to manage the timing and receipt of deposits which are submitted physically. There is also a much higher likelihood physical deposits can be lost in transit and end up in the hands of someone other than the Escrow Agent. It is a best practice to reduce the number of touch-points which increase errors, allow for quicker and more efficient handling of deposits, and increases the secure handling of data.

4.4 It appears that ICANN is giving the option to Registry Operators to submit their escrow deposits in either XML or CSV format. If that is the case, this section is ambiguously worded and needs to more clearly state the option. It is also important to mention that having multiple file formats can slow down ICANN's or another Registry's ability to utilize the escrowed data.

4.8 There is a statement that the order in "which fields are presented indicates the order in which they are expected to be in the respective record". This statement needs to be tightened up – meaning it should say the order in "which fields are presented ~~indicates~~ is the order in which they ~~are expected to~~ must be in the respective record". If registry deposits have different data in different order, it's almost impossible to perform automated or partially-automated verification. The more manual any part of the escrow process is, the more costly it will be to the Registry Operator. This inconsistent ordering of fields can also cause integration problems if a registry fails and escrow files are given to a new registry to be integrated.

4.8.7 This section states that IP address syntax must be either IPv4 or IPv6. Depending on what is truly required to meet the verification requirement discussed in Section 7 of both Parts A & B – there needs to be a way to identify which syntax is being used. Iron Mountain suggests changing the file type from "NSIP" to "NSIP4" or "NSIP6", depending on the syntax.

4.13 Iron Mountain has two comments on this section.

(4) This section states a "suggested" algorithm for Hashes is SHA256. Iron Mountain recommends requiring a singular Hash algorithm with SHA256 being preferred. The more consistency that is promoted across registry escrow deposits the more usable and quickly the data can be utilized (if necessary), and it reduces the cost to registries because the Escrow Agent doesn't need to support multiple logics. Consistency also increases the quality of the Escrow Agents deposit verification as it limits the scope of options inside what could be 10's of 1,000's of escrow deposits.
Additionally, there should be more detail regarding HASH. An example is: Registry Operator shall generate SHA-256 hash for each file (after file splitting, if applicable). The hash string(s) shall be submitted in a single, uncompressed text file along with the respective file name(s). The text file with checksums shall be composed of ASCII lines of text. Each line shall consist of the hash value for one file, followed by white space, followed by the name of the file

(5) See Iron Mountain comments on Section 2 of Part A. There is inconsistency between these two sections of the Specification.

7. (4) The section states each file will be "validated against the format defined in this specification". It is not clear exactly what needs to be validated. Is the escrow agent validating that the file is in either CSV or XML format; are they validating the proper number of columns, handles, objects, etc. have been deposited; are they validating that all fields that should have content do; that there isn't gibberish being deposited? The list goes on. Also, by not specifying what verification means, how can ICANN ensure consistency across all Escrow Agents?
A suggestion for what verification could be is: the Deposit file will be split it in to its constituent reports (including the format report prepared by Registry Operator and appended to the Deposit) check its format, count the number of objects of each type, and verify that the data set is internally consistent. This program will compare its results with the results of the Registry-generated format report, and will generate a Deposit format and completeness report.

Part B – Legal Requirements

General Comments:
To date, all registry data escrow contracts have been three-party agreements with ICANN being one of those parties. The current DAG has changed that precedent and merely requires ICANN be a named beneficiary. This creates a two-party agreement which goes against the most critical best practice in any escrow arrangement – which says a beneficiary should also be a party to the agreement. While ICANN has certain enforceable rights as a third party beneficiary to the escrow agreement, it is prohibited from amending, modifying or terminating that agreement. It is foreseeable that at some point in the future ICANN may wish to modify or amend the terms of the escrow agreement and in such an event it will be forced to rely on the Registry Operator to implement any changes. Also, leaving the escrow agreement and its terms up to the Escrow

Agent and Registry Operator to decide means escrow Agreements could vary tremendously between Escrow Agents which does not make it easy for ICANN to ensure a minimum level of expectations are met and nearly impossible for ICANN to ensure compliance. By way of example – length of time for escrow deposits to be retained is stipulated in the escrow agreement. Every escrow agreement could have varying, or worse – no, retention requirement and ICANN would have control over this as – once again – it's not a party to the escrow contract. If there is one Registry Agreement with ICANN and the Registry Operator it makes sense there should be one escrow agreement with ICANN, the Registry Operator and the Escrow Agent. It is in the best interests of stability, and registrants that ICANN continue its best practice of being a party to every registry data escrow contract.

Section Specific Comments:

1. "Registry Operator must contact and inform ICANN as to the identity of the Escrow Agent". It seems imprudent that an Escrow Agent does not require ICANN approval. According to Specification 2, anyone can be named as the Escrow Agent for a Registry Operator.

6. The requirement that Escrow Agent will deliver all contents in its possession within 24 hours may not be technically feasible depending on the volume of contents, their location, and method of delivery. For example, if the Escrow Agent has sixty days of deposits in its possession for a registrar with one million domains that have the maximum number of data fields to be deposited (i.e., IDNs, DNSSEC, handles, etc.) – it would take the Escrow Agent longer than twenty-four hours to pull all of that data from its servers, get it into a transferrable format (ftp files, CDs, DVDs, etc.) and send it to ICANN. Additionally, there is not description of how ICANN would like released data delivered. Electronically? On physical media?

7.1 As previously stated in Section 7.(4) of Part A – this requirement is not specific enough. Please see comments in Part A 7.(4).

7.2 Registry Operator must begin developing modifications, updates, corrections and other fixes of the Deposit if it fails a verification procedure as promptly as possible and Escrow Agent is required to notify ICANN of a successful verification within twenty-four hours. There needs to be a more specific timeline for the Registry Operator to fix issues with its deposits.

8. There is a requirement that Escrow Agent amend its escrow agreement with Registry Operator within ten calendar days of any amendment to Specification 2. To start, the Escrow Agent isn't a party to Specification 2, so requiring it to make changes to its own agreement because of a change that occurred in someone else's contract is inappropriate. Second, ten days is not enough time for the Escrow Agent to consider whether it's willing to make these changes and should they decide not to accept the changes, it's definitely not enough time for the Registry Operator to find a new Escrow Agent, contract with them, and begin depositing its data. Iron Mountain is not sure what the intent of his clause is, but the result is the Escrow Agent is held hostage.