| **Results** | |
| --- | --- |
| **Number of records in this query:** | 67 |
| **Total records in survey:** | 67 |
| **Percentage of total:** | 100.00% |

Top of Form



Bottom of Form

| **Field summary for 821** | | | |
| --- | --- | --- | --- |
| **Assuming these features are fully configurable and not mandatory to operate the system (but rather determined by policy), do you feel that DNRD-DS should have a standardized permissions framework for both DNRD-DS users (those querying the data) and for the data elements itself (meaning certain DNRD-DS users may see more or less data depending on their permission level – i.e. permission level A may see a registrant’s address but permission level C may only see the registrant’s name.)** | | | |
| **Answer** | **Count** | **Percentage** |  |
| Yes (1) | 39 | 58.21% |  |
| No (2) | 11 | 16.42% |  |
| Indifferent (3) | 7 | 10.45% |  |
| Comments | 8 | 11.94% |  |
| No answer | 10 | 14.93% |  |
| **'Other' Responses** This "elevated access" idea is a very poor one. I'm against it.  This question is so confusing that the results may not be reliable. I cannot answer it without knowing more about the policies behind the permissions framework registrars should have the permission needed. like .TEL private whois and requiring retrieval of the admin email for transfers. can't get that with the current whois lookup Heinrich Himmler In the IETF. Policy in ICANN, protocol definition in the IETF. Did I mention? Policy in ICANN, protocol definition in the IETF. Depends on requirements of law misuse can be averted. prior permission through a online mechanism should help  This should be policy driven and not in the protocol. | | |  |
| https://limesurvey.icann.org/tmp/d27882451a0d5ed149618658d381cc51.png | | | |

| **Field summary for 822** | | | |
| --- | --- | --- | --- |
| **Do you believe that it would be technically and operationally useful to have all DNRD-DS users, even in open and anonymized DNRD-DS services have to make use of a login credential during the query process?** | | | |
| **Answer** | **Count** | **Percentage** |  |
| Yes (1) | 23 | 34.33% |  |
| No (2) | 26 | 38.81% |  |
| Indifferent (3) | 6 | 8.96% |  |
| Only in specific circumstances; please explain (4) | 4 | 5.97% |  |
| Comments | 9 | 13.43% |  |
| No answer | 8 | 11.94% |  |
| **'Other' Responses** There should be no anonymous use of Whois where special access is given.  There's a balance between securing the data and inconveniencing "normal" users -- I would envision an Anonymous class of users that have access to certain data (perhaps rate-limited) and Authenticated users that would have access to data based on their credentials (and perhaps NOT rate limited, again depending on credentials) Felix Dzerzhinsky Possibly.  users who mine the whois for email addresses and spam would then be known, as long as the logins are not anonymous. users (readers) of whois need to identify themselves and be validated just as much as registrants (writers) have to do Thin WHOIS is operated on thousends of servers. Logins whould be a nightmare. For special access like "updates" oder "member access" a different interface, which needs authentication should be used. I want the whois as public as possible. It is important to keep it open.  Publicly available data should not require authentication. in case of proxy whois usage. | | |  |
| https://limesurvey.icann.org/tmp/08ce9750149c6ba4f58bfaa164caa025.png | | | |

| **Field summary for 824** | | | |
| --- | --- | --- | --- |
| **Where do you see granulated access to DNRD-DS on a 1 to 5 scale of importance? ["1" being the Most Important, "5" being the Least Important]** | | | |
| **Answer** | **Count** | **Percentage** | **Sum** |
| 1 (1) | 12 | 21.82% | 45.45% |
| 2 (2) | 13 | 23.64% |  |
| 3 (3) | 14 | 25.45% | 25.45% |
| 4 (4) | 4 | 7.27% |  |
| 5 (5) | 12 | 21.82% | 29.09% |
| **Sum (Answers)** | **55** | **100.00%** | **100.00%** |
| Number of cases | 67 | 100.00% |  |
| No answer | 12 | 17.91% |  |
| Arithmetic mean |  | 2.84 |  |
| Standard deviation |  | 1.44 |  |
| https://limesurvey.icann.org/tmp/b00f006805197e028a854a39366d2cb8.png | | | |

| **Field summary for 825** | | | |
| --- | --- | --- | --- |
| **Is granulated access to DNRD-DS data a requirement in support of local laws in your operating jurisdiction?** | | | |
| **Answer** | **Count** | **Percentage** |  |
| Yes (Y) | 17 | 25.37% |  |
| No (N) | 15 | 22.39% |  |
| No answer | 35 | 52.24% |  |
| https://limesurvey.icann.org/tmp/540d47ece9397d42adbd7a1f42961793.png | | | |