|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Item #** | **Type** | **Page #** | **Line #** | **Section** | **Comment (with rationale)** | **Suggested Change** |
| 1 | G | 14 (27) | 646 | 2.4.3 | Submission for Request for Contribution for Indicated Section. | Methods to secure individual IoT devices fall outside the scope of the NBDRA standard; however, it is worthwhile to note that IoT devices present unique security challenges (OWASP, 2015) due to limited hardware capability, rapid market evolution, and lack of a widely used security standard. While some progress has been made with industrial devices (NIST 800-82, IEC 62443), consumer device manufactures have no regulatory or market incentive to secure their devices.  Until IoT hardware reaches sufficient maturity to allow TLS communication and support other cryptographic authentication mechanisms, IoT data required for a BDRA will typically be collected under a single provider per device type or class. Volume and Velocity for an individual IoT device are low, due power and processing constraints, though in an aggregate provider very high volumes are easily realized. Veracity of this provider is strongly dependent on hardware and protocol implementation details which might be opaque to relying Big Data consumers.  IoT aggregate NBDRA Data Providers should authenticate individual IoT device connections prior to accepting data wherever possible. While statistical analytics might detect a security breach, relying on this alone is undesirable as it lacks a means to distinguish between individual and compromised devices – resulting in a complete loss of functionality in the event of a breach. |
| 2 | T | 17 (30) | 779 | 2.4.7.6 | An abuse-resistant glass-break mechanism for time-critical situations (such as fires, medical emergencies) across multiple Providers will likely require AI, as policy reconfiguration for even a highly skilled human operator would take too long, or be too easy to bypass. The mechanism must have strong authentication and non-repudiation, with the identity, location, and motive of the initiator preserved permanently through a cryptographic mechanism (such as Block Chain). |  |
|  |  |  |  |  |  |  |