Coordinated Vulnerability Disclosure Reporting at ICANN

ICANN has a policy to enable the reporting of vulnerabilities and/or security threats that affect either ICANNs assets or third party assets where ICANN may be required to act in a reporter function.

The purpose of the documented policy is to lend clarity to the mechanisms that people may use to inform ICANN of vulnerabilities and the processes and safeguards that ICANN will use.

This process was perhaps most notably used upon discovery of a DNS related vulnerability in the Microsoft windows operating systems during work carried out by JAS Global Advisors on behalf of ICANN. The process enabled us to invoke confidentiality surrounding data that may otherwise have led to discovery of the issue had it been disclosed. "JASBUG" as it became know was estimated to affect over 300 million devices globally and details were kept "confidential" between ICANN, JAS and Microsoft for more than a year until a time that Microsoft could implement and release a patch in their operating system.

https://en.wikipedia.org/wiki/JASBUG

The document includes references to both secure electronic communication and how to revert to voice communications in the event that electronic communications are not available.

The guidelines can be found at the following URL, are based on Industry best practices and include references to such

https://www.icann.org/en/system/files/files/vulnerability-disclosure-05aug13-en.pdf