Statement of Work: Expert Review & Validation of ICANN Domain Abuse Activity Reporting System Methodology

ICANN's Domain Abuse Activity Reporting (DAAR) project provides a system for studying and reporting on domain name registration and security threat (domain abuse) behavior across top-level domain (TLD) registries and registrars. The overarching purpose of DAAR is to report security threat activity to the ICANN community, which can then use the data to facilitate informed policy decisions.

DAAR was designed to provide the ICANN community with a reliable, persistent, and reproducible set of data from which security threat (abuse) analyses could be performed. The system collects TLD zone data, a very large body of registration data, and complements these data sets with a large set of what we determined to be high-confidence reputation (security threat) data feeds. We intend that the data collected by the DAAR system might serve as a platform for studying or reporting daily or historical registration or abuse activity. The system currently gathers data to report on domain names that are associated with four threats (cyberattacks): phishing, malware hosting, botnet command-control, and spam delivery.

ICANN is seeking the assistance of a subject matter expert (SME) in cyber threat identification/mitigation and the role(s) that domain names play in the execution of the cyberattacks mentioned in this Statement of Work. We expect the SME to study and write a review of the DAAR system methodology for publication, including a set of findings or recommendations. Specifically, we request that the SME:

- Validate the collection and processing of zone data, domain name registration data and abuse data, or document any problems or shortcomings.
- Confirm or contest that the sources of abuse data that ICANN has selected meet industry or academic criteria for reliability, accuracy, low false positive rate, and false positive remediation. In the event that the SME refutes sources, indicate which sources and why.
- Validate the means by which the DAAR system attributes abuse domains to TLDs, or document any problems or shortcomings.
- Confirm or contest that the assertions we make that spam is a security threat. We ask that the SME correct or expand assertions, if necessary. If possible, complement the existing list of academic or commercial research citations.
- Validate the generation of statistics, or document any problems or shortcomings.
- Confirm that the DAAR system description is sufficiently complete for other parties to reproduce similar results using the same publicly or commercially accessible data.

Please provide a Curriculum Vitae or resume, a program of work (including time to present your findings and recommendations to our team and possibly other ICANN staff), an estimated completion date, and a fee (fixed or hourly, if hourly, please offer an estimate). Indicate experience with public review process or expert testimony in the CV or resume. We will require a non-disclosure agreement.