Sub Topic 4 – Future Challenges	
Topic	Future Challenges
Related Bylaw	4.6 (c)(iii)
Skillset	Threat Intel, Policy, Cybersecurity, IETF
Description of activity	The sub team will be responsible for reviewing the long term strategy of ICANN to plan for and mitigate potential threats to the secure and resilient operation of the unique identifiers systems it coordinates.
Topics for Consideration	1. How do we assess "Future challenges to security and stability a DNS?" 2. Explore forecasting research on the Internet unique identifiers 3. What has been, or could be, the impact of the evolution and the number and types of devices in the DNS? 4. How effective are ICANN's security efforts to known threats and preparation for future threats? 5. What emerging technologies are trends should we consider? [new items to discuss] : • ICANN OCTO Middleware research • ICANN Emerging Technologies (ask ICANN) • Internet Governance issues • Privacy regulation i.e. GDPR

Definitions	**Assets** – What are we trying to protect. Attackers can use an Identifier System(s) to target and attack property, information, or people, e.g., by using the DNS to implement denial of service attacks. They can also attack aspects of an Identifier System by using it in a manner that is abusive or malicious, for example, by using fraudulent registration information or hijacking names or addresses. Importantly, these forms of attacks can be executed in tandem. Each of these assets performs a different critical function; a specific attack against one may threaten the security, stability, or resiliency of the Identifier System as a whole. These assets include: • Authoritative domain name servers and recursive and stub resolvers, as well as domain name registration data, registries, registrars, and registrants. • IP addresses and autonomous system numbers (ASNs) employed by the global Internet routing system, along with associated network infrastructure components (e.g., routers, switches, address management systems) and regional Internet registries. Protocol parameters and the implementations of the associated protocols that make use of those parameters, both individually and within the context of larger systems that incorporate those protocols and protocol parameters. **Vulnerabilities –** Weaknesses or gaps that can be exploited. Vulnerabilities may be flaws within Identifier System assets themselves, or within measures intended to protect them. These vulnerabilities include design defects, coding errors, configuration mistakes, and other gaps that weaken an asset's attack resistance, stability, or resiliency. **Threats –** What we're trying to protect against. Threats include both entities and events which may exploit an asset's vulnerabilities. Threats to Identifier System assets include attacks against domain name servers and name resolvers, or network elements such as routers or switches. The threat landscape includes attacks against domain and address registration services as well as natural disasters such as storms that trigger power and network outages which degrade Identifier System operations. **Risk –** The probability that threats will exploit vulnerabilities to obtain, damage or destroy assets. In this document, we attempt to identify high-risk types of attacks against Identifier System assets. To do so, we focus on high-impact vulnerabilities that are being actively exploited by threats, as well as new vulnerabilities at high risk of exploitation.

Work Items/ Areas of Focus	**Top Identifier System Attacks** • Route Insertion Attacks ○ As it affects the unique ID system (what could happen, how it could be prevented, etc.) • Coalescence of registry/backend operators for multiple TLDs ○ Multitudes of victims for one high-value compromise/outage/etc. ▪ DNS Denial of Service Attacks (coordinate w/other Sub-Topics) ▪ DNS DDoS Attacks ▪ Web Services Attacks impacting Identifier Resources ▪ Software ▪ Resource Registration Account Compromises • Identifier Hijacking via Social Engineering • DNS Zone File Attacks ○ ? • Parallel Root Name System Risks ○ Namespace ambiguity/competition/etc • DNS and Surveillance Attacks ○ Undermining DNS' utility and perceived trustworthiness • DNS Misuse as Covert Channel ○ How the attacks (TTPs) are evolving to use identifier spaces in new ways ○ Empower ICANN to investigate attacks that are using new and more sophisticated TTPsBo **New dependencies:** • New crytpo-systems in DNSSEC ○ Can DNSSEC continue to offer security in the future and evovle where it needs to (e.g. PQ) • New uses for DNS (IoT, etc.) ○ Can the DNS evolve as new systems use it • ~~Threat Intelligence blindspots~~ ○ ~~When technologies like QName Minimisation [sic] and DNS over TLS hide necessary telemetry from whitehats, miscreants have more latitude~~ • Alternate naming systems (interactions, conflicts, etc.) ○ Namecoin, • Censoring • Loss of confidence in standards bodies • Adoption of systems that don't adhere to standards **Performance security (SSR2 scope):** *Issue high level recommendations towards ICANN technologies(routing, switching, computing environments, DNS related services) resources utilization* *(Traffic, processing/power/memory utilization, ...)*

	• Identify a list of the types of technologies used by ICANN • Recommend forecasting techniques to be used by ICANN to determine future utilization • ICANN role in return: Recommendations need to be considered in future technological planning or architecture designs by ICANN. **Technology selection security (SSR2 scope):** • Vendor security technology evaluation process (how to test solutions) • Vendor security technology selection process (how to select a solution) • Vendor security technology implementation process (what vendors need to do when deploying solutions) • Vendor security maintenance process (how vendors should maintain their solutions) • Vendor responsibilities and SLAs (patching vulnerabilities, technology development/deployment) • Vendor accountability for security problems • ICANN role in return: Selection recommendations need to be considered in future technology selection processes employed by ICANN **Threat intelligence (SSR2 scope):** • The need for an ICANN threat intelligence team • The need for ICANN to have established communication with top threat intelligence sources to know about the latest threats • The need for adapting threat intelligence internally, to identify attacks and threats accordingly • ICANN role in return: Threat intelligence recommendations to be adapted by ICANN towards enhancing blocking of cyber-attacks, identifying causes of new breaches, and knowing about the latest threats endangering similar organizations. NB1:Recommendations provided should be vendor/technology neutral, as to be valid for future utilization NB2: issues of DDOs, route injection all fall under “Sub Topic 3 – DNS SSR” as they are issues probably currently being dealt with. What is not dealt with, is how they could be used in the future, which falls under threat intelligence. I do not believe should predict protocols misuse options through new vulnerabilities, which has an unlimited scope.

Team Members	Kerry-Ann, Matogoro, Amin Hasbini, Noorul Ameen, Eric, Denise
Rapporteur	Kerry-Ann