Security Framework Drafting Team

Framework for Registry Operators to respond to Security threats

ICANN 54  |  21 Oct. 2015
Agenda

- Background - 5 min.
- Opening Remarks by co-chairs of the Framework Drafting Team - 15 min.
- Approach to Drafting the Security Framework - 15 min.
- Discussion of Selected Topics by Drafting Team - 35 min.
Background – Security Framework

- **Beijing GAC Advice on New gTLD Safeguards (Apr. 2013)**
  - “Security checks” as one of the 6 Safeguards applicable to all new gTLDs
  - 2 components: identifications of threats + response to identified threats

- **NGPC Resolution 2013.06.25.NG02 (Jun. 2013)**
  - Include security checks in Specification 11 section 3b
  - “sollicit community participation to develop a framework for Registry Operators to respond to identified security risks that pose an actual risk of harm, notification procedures, and appropriate consequences, including a process for suspending domain names until the matter is resolved, while respecting privacy and confidentiality”.


- **Registries volunteering to lead the drafting of the Framework (Jun. 2015)**
Objective of the Framework
- Reduce the impact of new gTLD-related security threats on Internet users through timely industry self-regulation
- Become a reference set of non binding standards for Registries, Registrars and interested parties

Framework Drafting Team formed in July 2015
- 30 Registry representatives
- 5 Registrar representatives
- 10 Public Safety Working Group (PSWG) representatives

Objective of the Framework Drafting Team
- Produce the substance of the framework grounded in:
  - Industry experience
  - accepted best practices
  - consultation with relevant communities
- Build the Framework collaboratively and in the spirit of mutual agreement
Opening Remarks by Drafting Team Leadership

- Jonathan Flaherty, PSWG co-chair
- Theo Geurts, Registrar co-chair
- Yasmin Omer, Registry co-chair
Registries and Registrars to lead drafting effort
- PSWG provide input on Framework based on expertise
- Environment of ‘openness’ and collaboration
- Flexibility in favor of specificity: Less is more
- Guiding principles and common shared interests
- Engagement in building trust
Framework Drafting: Target Timeline

- Preliminary Consultation (GAC + Registries)
  - ICANN 52 - Engagement w/ GAC + Registries
  - Consideration of Input Received by ICANN
  - ICANN 53 – Joint Registries/GAC meeting

Development of Security Framework:
- Formation and initiation of the Framework Drafting Team
- ICANN 54 – Framework Drafting Team Face-to-Face

Next Steps:
- 1st Draft for PSWG Review
- Reviews and Revisions
- Final draft
- Public Comment Period
- ICANN 55 – Community Engagement
- Release of Final Framework for Responding to Security Threats

Timeline:
- 2015
- 2016
Discussion of Selected Topics

Registries

- Typical Abusive Domain Name Processing by Registries
- Registry Operator Roles in the DNS Ecosystem
- Responses to Security Threats: from notification to appropriate consequences

PSWG

- Existing Abuse Best Practices
- Approach, application, notification & response
- Timely security threat feeds
- 2 way Registry/PSWG threat sharing
- Quarantine of domains via 3rd party Registrar
- Long term mitigation at scale
Security Framework Drafting Team

Framework for Registry Operators to respond to Security risks

ICANN 54 | 21 Oct. 2015