
ICANN
ANNUAL GENERAL
60
ABU DHABI
28 October–3 November 2017

Security Framework

ICANN60 Public Session

Framework for Registry Operators to Respond to Security Threats

Security Framework Drafting Team

29 October 2017

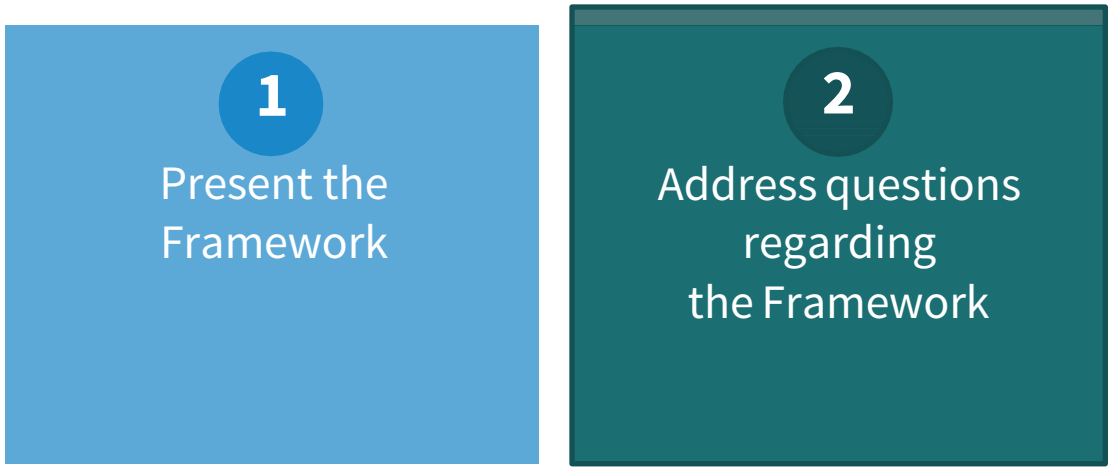
Agenda

1. Introduction
2. What Who How
3. Background
4. Presentation of the Framework
5. Illustration
6. Next Steps

Welcome to the Security Framework Public Session

Topic : Security Framework for Registries to Respond to Security Threats

Objectives:



Presenters:

Alan Woods, Compliance Manager, Donuts Inc.

Iranga Kahangama, GAC PSWG Member, Federal Bureau of Investigation, United States

Brian Cimbolic, Deputy General Counsel, Public Interest Registry

Dennis Chang, GDD Services and Engagement Program Director, ICANN

What is the Security Framework

- A voluntary and non-binding document designed to articulate guidance as to the ways registry operators may respond to identified security threats.
- Result of a two-year collaborative effort of the members of the Security Framework Drafting Team (SFDT)

- **Published** on 20 October 2017 https://www.icann.org/resources/pages/framework-registry-operator-respond-security-threats-2017-10-20-en

- The Framework has been reviewed and supported:
  - Registries Stakeholder Group (RySG),
  - Registrar Stakeholder Group (RrSG)
  - Public Safety Working Group (PSWG)
  - Governmental Advisory Committee (GAC)
- And completed Public Comment process https://www.icann.org/public-comments/draft-framework-registry-respond-security-threats-2017-06-14-en

Who is the Security Framework Drafting Team

- Security Framework Drafting Team (SFDT) comprises of:
  - Registry Operators
  - Registrars
  - Members of the Public Safety Working Group (PSWG) of the Governmental Advisory Committee (GAC)
  - ICANN Org

- SFDT has 63 members from 45 organizations

- SFDT Leadership Team
  - Alan Woods & Brian Cimbolic- Registries
  - Iranga Kahangama - PSWG
  - Theo Geurts - Registrars
  - Dennis Chang - ICANN Org

Security Framework Approach - One Team

- Agreement on the targets of the Drafting Effort
  - Non-binding standards to serve as a reference for self-regulation
  - Grounded in industry experience and accepted best practices
  - Mutual agreement among parties
  - Consultation of relevant communities
- Approach of the Security Framework Drafting Team
  - Opportunity to build bridges with registries, registrars and PSWG
  - Educate each other in frequent face-to-face and on-line meetings
    - Eg: multiple meetings in ICANN57 & ICANN58
  - Set realistic expectations based on capabilities and limitations
  - Collaborative authorship of the Framework
  - Collaborative planning and delivering to on-schedule

Background

- Beijing GAC Advice on New gTLD Safeguards (Apr. 2013)

3. **Security checks**— While respecting privacy and confidentiality, Registry operators will periodically conduct a technical analysis to assess whether domains in its gTLD are being used to perpetrate security threats, such as pharming, phishing, malware, and botnets. If Registry operator identifies security risks that pose an actual risk of harm, Registry operator will notify the relevant registrar and, if the registrar does not take immediate action, suspend the domain name until the matter is resolved.

4. **Documentation**—Registry operators will maintain statistical reports that provide the number of inaccurate WHOIS records or security threats identified and actions taken as a result of its periodic WHOIS and security checks. Registry operators will maintain these reports for the agreed contracted period and provide them to ICANN upon request in connection with contractual obligations.

Background

- ICANN Board New gTLD Programme Committee (NGPC) Resolution 2013.06.25.NG02 (Jun. 2013)

NGPC Proposal for Implementation of GAC Safeguards Applicable to All New gTLDs

3. Security Checks (GAC Register # 2013-04-11-Safeguards-3)

REGISTRY AGREEMENT

SPECIFICATION 11

PUBLIC INTEREST COMMITMENTS

3. Registry Operator agrees to perform the following specific public interest commitments, which commitments shall be enforceable by ICANN and through the PICDRP. Registry Operator shall comply with the PICDRP.

b. Registry Operator will periodically conduct a technical analysis to assess whether domains in the TLD are being used to perpetrate security threats, such as pharming, phishing, malware, and botnets. Registry Operator will maintain statistical reports on the number of security threats identified and the actions taken as a result of the periodic security checks. Registry Operator will maintain these reports for the term of the Agreement unless a shorter period is required by law or approved by ICANN, and will provide them to ICANN upon request.

Development of "*the Framework for Registry Operators to respond to identified Security Risks*"

Because there are multiple ways for a Registry Operator to implement the required security checks, ICANN will solicit community participation (including conferring with the GAC) in a task force or through a policy development process in the GNSO, as appropriate, to develop the 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. The language include in Paragraph 3 of the attached PIC Specification provides the general guidelines for what Registry Operators must do, but omits the specific details from the contractual language to allow for the future development and evolution of the parameters for conducting security checks. This will permit Registry Operators to enter into agreements as soon as possible, while allowing for a careful and fulsome consideration by the community on the implementation details.

Presentation of Security Framework

- Walkthrough of Draft Framework, section-by-section
  - Objective
  - Scope
  - Categories of Action by Registries
    - On Existing Domain Names
    - On Unregistered Domain Names
  - Reporting of Security Threats
  - Registries Response to Reports of Security Threats

Illustration of Security Framework (Botnet)

1. LEA identifies Botnet Command & Control domains in New gTLD
2. LEA reaches out to anti-abuse point of contact of relevant Registry, providing:
   - Level of priority (may be high in this case)
   - Substantiated information about domain names
   - Specify actions that should be taken
3. Registry acknowledges receipt of a reported threat asap ('promptly')
4. Registry may, per its policies and operating procedures:
   - Validate source of report
   - Verify threat (taking into account higher degree of fidelity when from a relevant LEA)
5. Registry indicates response taken to report of Security Threat, potentially within 24 hours of acknowledgement of report. Typical responses may include:
   - Escalate to the Registrar (provide opportunity to investigate/action)
   - Suspend the domain names (stop resolution)
   - Sinkhole the domain names (redirect services to a security research partner investigating the threat)
   - Register and sinkhole pre-emptively domains according to DGA algorithm (though this approach likely requires going through an Expedited Registry Security Request process with ICANN organization)

Next Steps

SFDT Discussion on future of the Framework and the role of the SFDT

1. How, who, and when should the Framework be updated?
2. What additional material is appropriate for this voluntary non-binding document

Engage with ICANN

Thank You and Questions

Visit us at **icann.org**
Email: email@icann.org

twitter.com/icann

gplus.to/icann

facebook.com/icannorg

weibo.com/ICANNorg

linkedin.com/company/icann

flickr.com/photos/icann

youtube.com/user/icannnews

slideshare.net/icannpresentations