

Security Framework Drafting Team

Framework for Registry Operators to respond to Security threats

ICANN 55 | 9 Mar. 2016

Agenda

- ⦿ Background and Status - 5 min.
- ⦿ Opening Remarks - 15 min.
(Co-Chairs of the Framework Drafting Team)
- ⦿ Discussion of Selected Topics by Drafting Team - 45 min.
- ⦿ Next Steps and Timeline - 10 min

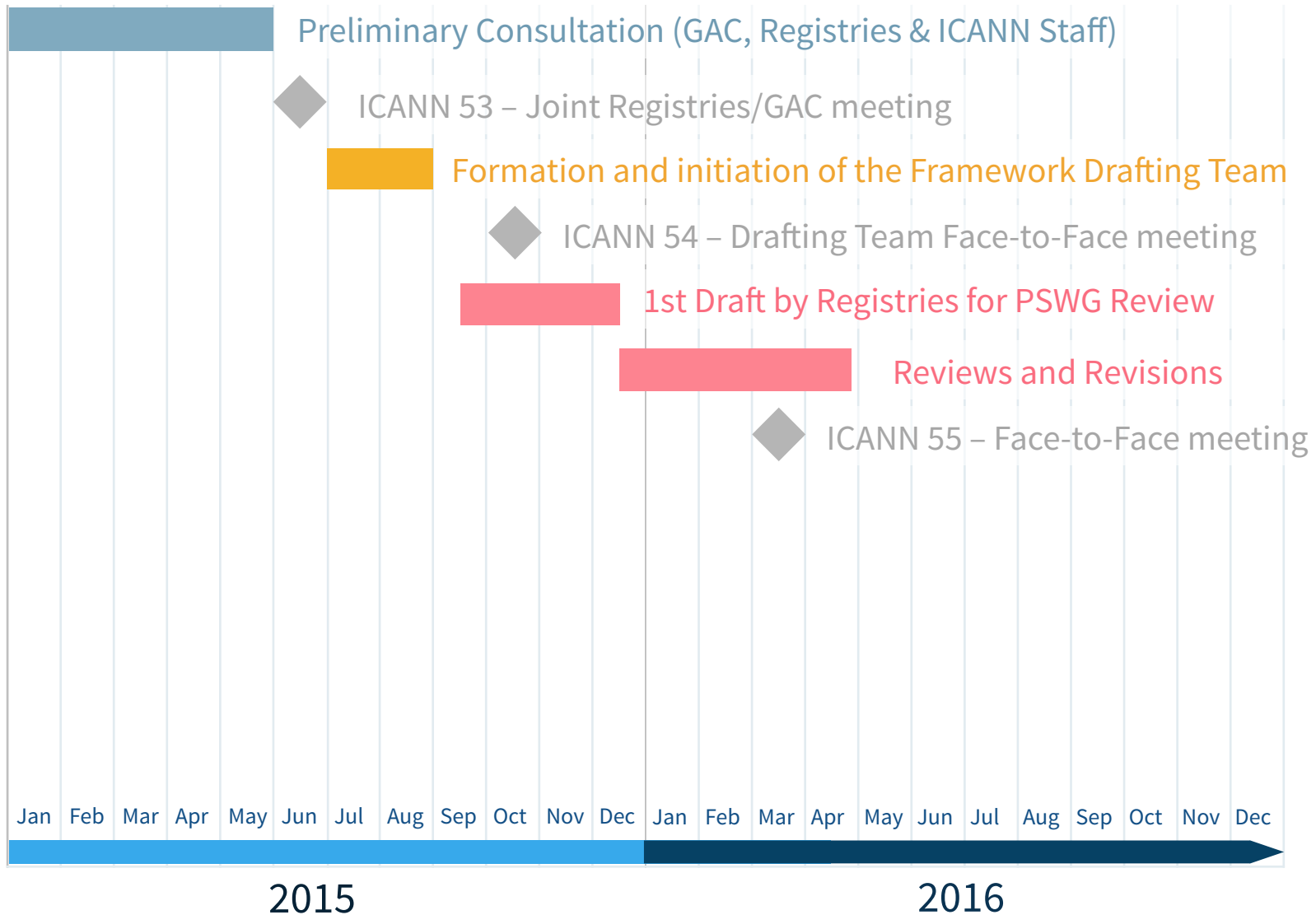
Background – Security Framework

- ◎ **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)**
 - Included identification of threats in the Registry Agreement Specification 11 Section 3b
 - “solicit community participation to [develop a framework for Registry Operators to respond to identified security risks \[...\]](#)”

Background – Security Framework

- ⊙ Consultation between ICANN Staff, Registries and GAC (Aug. 2014-Jun. 2015)
- ⊙ Formation of the Framework Drafting Team (Aug. 2015)
 - **Composition:** 45 representatives (30 registries, 10 PSWG, 5 registrars)
 - **Objective:** build collaboratively, and in the spirit of mutual agreement, a reference set of non-binding standards grounded in industry experience, accepted best practices and consultation with relevant communities
- ⊙ Security Framework Drafting not to be confused with Spec 11 3b Clarifications Advisory (separate but complementary initiatives)

Framework Drafting Timeline (as of 19 Feb.)



Opening Remarks by Drafting Team Leadership

- ◎ Alan Woods, Registry co-chair
- ◎ Jonathan Flaherty, PSWG co-chair
- ◎ Theo Geurts, Registrar co-chair

Discussion of Selected Topics

Definitions

- ⦿ Drafting Team discussing definition of threats, “severe threat” and “abuse”
- ⦿ Included in current registries draft:
 - “Abuse” preferred to “Malicious Conduct” overall
 - Severity: potential consultation with PS/LE Agency as appropriate (§ 4.4 Timely Response)

Referral to Public Safety/Law Enforcement Agency

- ⦿ PSWG available to assist registries when dealing with security threat
- ⦿ Included in current registries draft:
 - Possible forwarding or reporting of information to PS/LEA when making a determination (§ 3.3.2 Accuracy)
 - Possible forwarding before taking actions if threat unclear (§ 4.2 Proportionality of Response)
 - Intelligence Sharing (§ 5.6)
- ⦿ Additional discussion: definition of PSWG Trusted Contacts

Discussion of Selected Topics

Timeliness of Response

- ⦿ PSWG proposal: 24 hour timeframe to respond to security events
- ⦿ Included in current registries draft:
 - Timeliness based on severity of threats (§ 3.3 Analyse Data)
 - Timely and reasonable time frame In the interests of proportionality (§ 4.4 Timely Response)

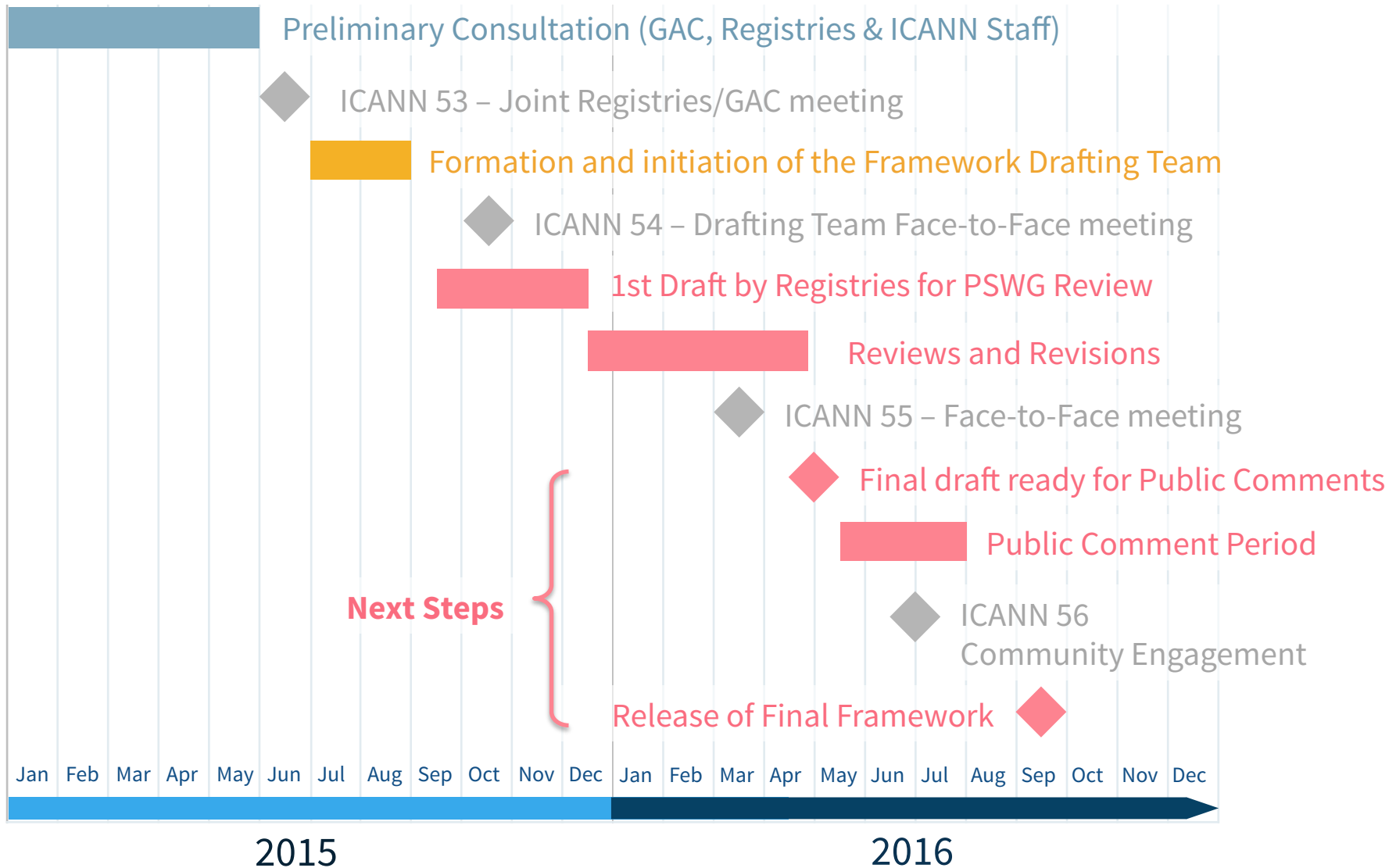
Candidate Topics for inclusion in the Draft Framework

- ⦿ Example responses to Security Threats, incl. sample responses
- ⦿ Automated/preventative measures implemented by registries

Other Topics

- ⦿ Update to PSWG on Healthy Domains Initiative

Framework Drafting Timeline (as of 19 Feb.)



Engage with ICANN



Thank You and Questions

Reach us at:

Email: engagement@icann.org

Website: icann.org



twitter.com/icann



[gplus.to/icann](https://plus.google.com/icann)



facebook.com/icannorg



weibo.com/ICANNorg



linkedin.com/company/icann



flickr.com/photos/icann



youtube.com/user/icannnews



slideshare.net/icannpresentations