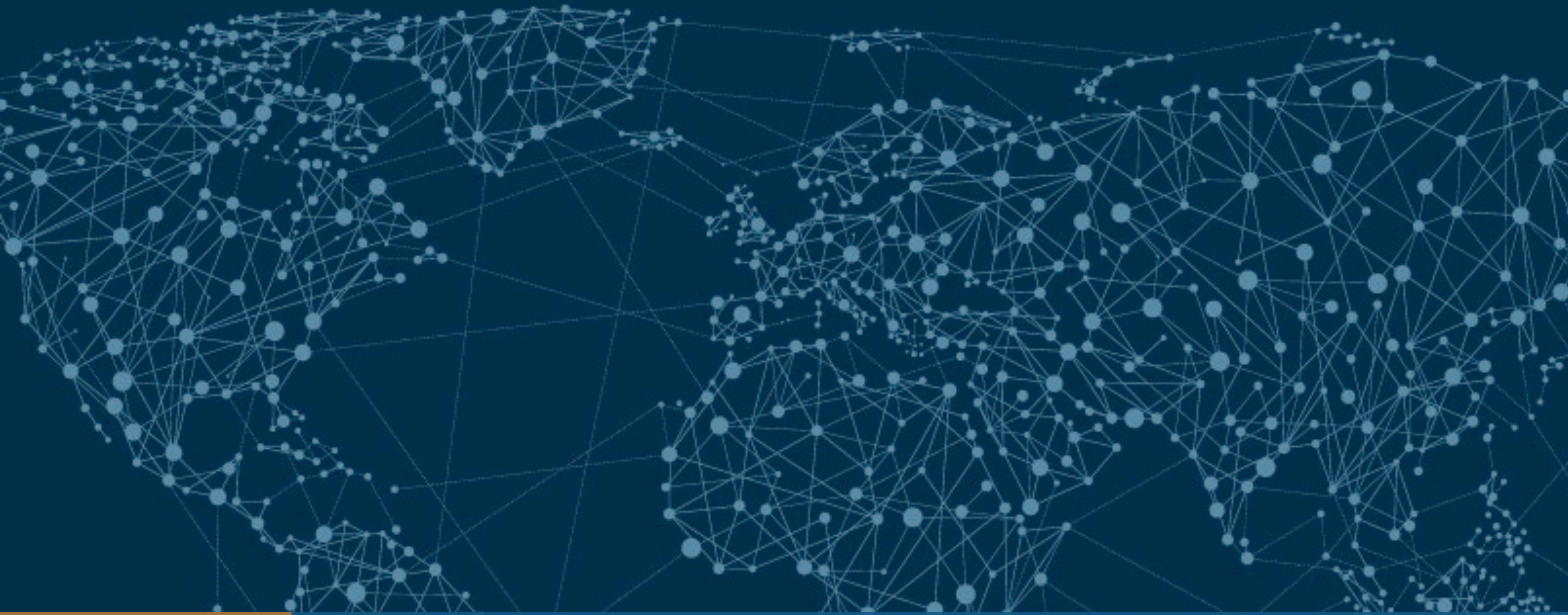


Security Framework Drafting Team

Framework for Registry Operators to respond to Security threats

18 Aug. 2016

Agenda

- Background and Timeline (reminder) - 5 min.
- Taking stock, Path Forward - 10 min.
  (Remarks by Co-Chairs of the Framework Drafting Team)
- Discussion of Selected Topics by Drafting Team - 40 min.
- Next Steps - 5 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 […]”

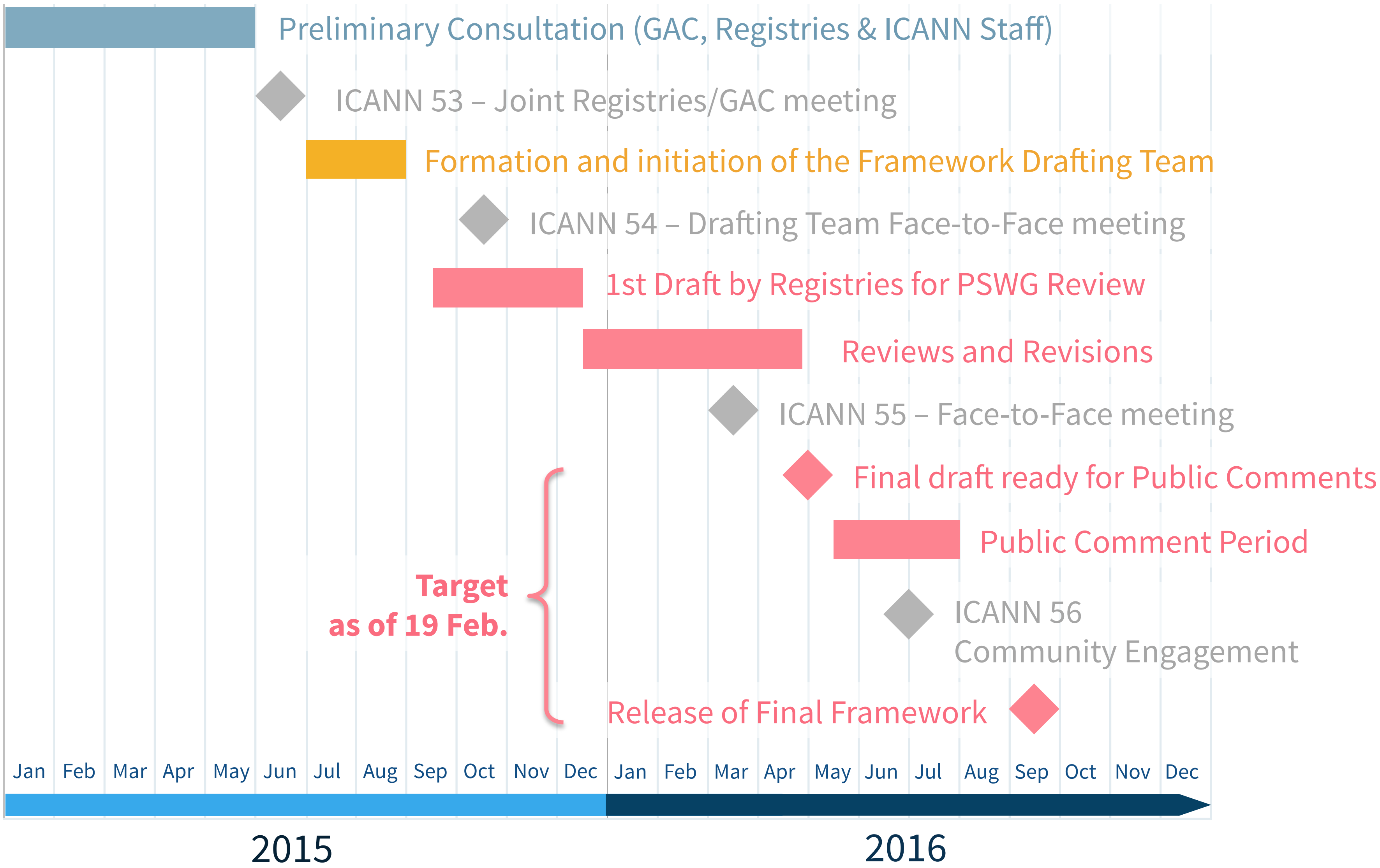
Background – Security Framework

- Consultation between ICANN Staff, Registries and GAC (Aug. 2014-Jun. 2015)

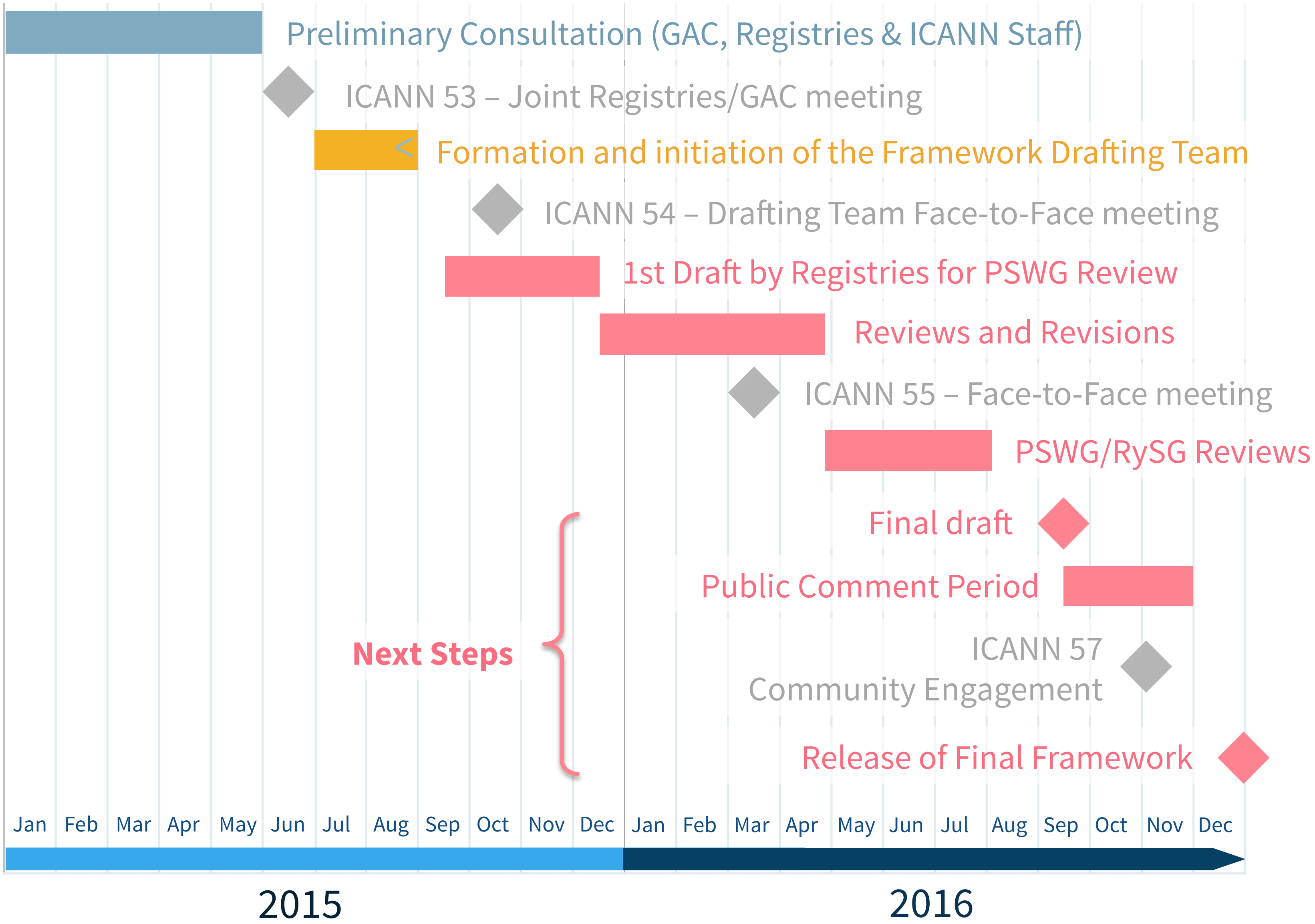
- Formation of the Framework Drafting Team (Aug. 2015)
  - Composition: 45 representatives (30 registries, 10 PSWG, 5 registrars)
  - Objective: build collaboratively, and in the spirit of mutual agreement, a reference set of non-binding standards grounded in industry experience, accepted best practices 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.)



Framework Drafting Timeline (as of 18 Aug.)



Opening Remarks by Drafting Team Leadership

- **Alan Woods**, Registry co-chair
- **Robert Flaim**, PSWG co-chair
- **Theo Geurts**, Registrar co-chair

Discussion of Selected Topics

Timeframe for registry response

- Ideally incidents should be handled in an uniform and quick fashion
- it is understood that registries have different models.
- The PSWG and GAC will find it hard to only use “reasonable time” (too subjective)
- One compromise solution: may be prioritize incidents with corresponding response times.
  - We could refer to the APWG model or other established and objective security frameworks
  - For instance:
    a. Top Prioritization: Imminent threat of injury or death to life and limb, child exploitation, imminent threat to critical infrastructure. Response time 24 hours?
    b. Middle: Botnets, malware, etc. Response time: 72 hours?
    c. Bottom: TBD

Discussion of Selected Topics

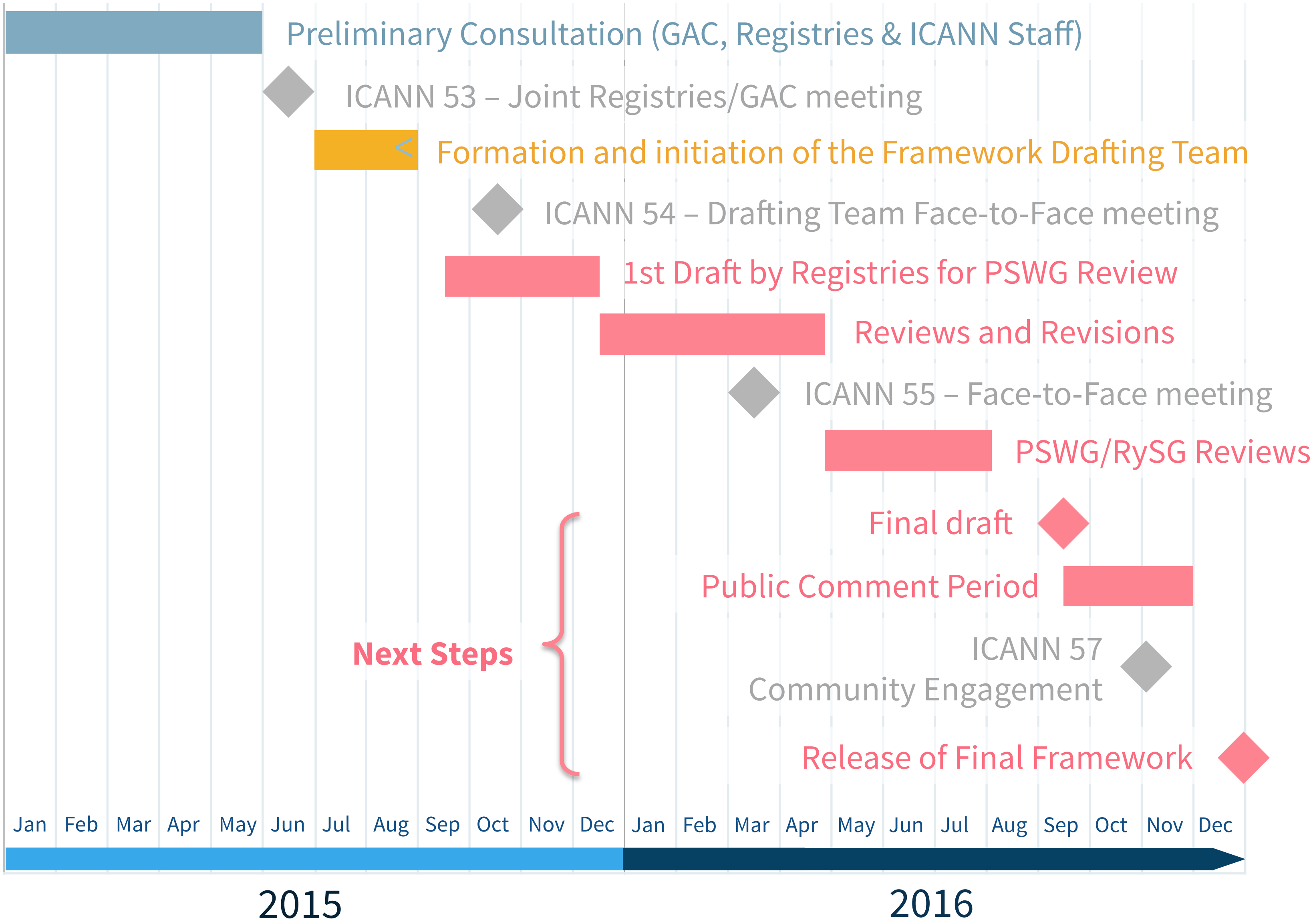
Annex A - Examples of Responses to Abusive Activity

- Would be useful with specifics

Annex B –Example of Actual Registry Anti-Abuse Policy

- PIR's example proposed by PSWG was only to show that there are registries who have a methodology
- It will be necessary to have the Security Framework provide some guidance as a baseline
- Details could certainly be manipulated.

Framework Drafting Timeline (as of 18 Aug.)


Preliminary Consultation (GAC, Registries & ICANN Staff)
ICANN 53 – Joint Registries/GAC meeting
Formation and initiation of the Framework Drafting Team
ICANN 54 – Drafting Team Face-to-Face meeting
1st Draft by Registries for PSWG Review
Reviews and Revisions
ICANN 55 – Face-to-Face meeting
PSWG/RySG Reviews
Next Steps
Final draft
Public Comment Period
ICANN 57
Community Engagement
Release of Final Framework
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
Oct
Nov
Dec
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
Oct
Nov
Dec