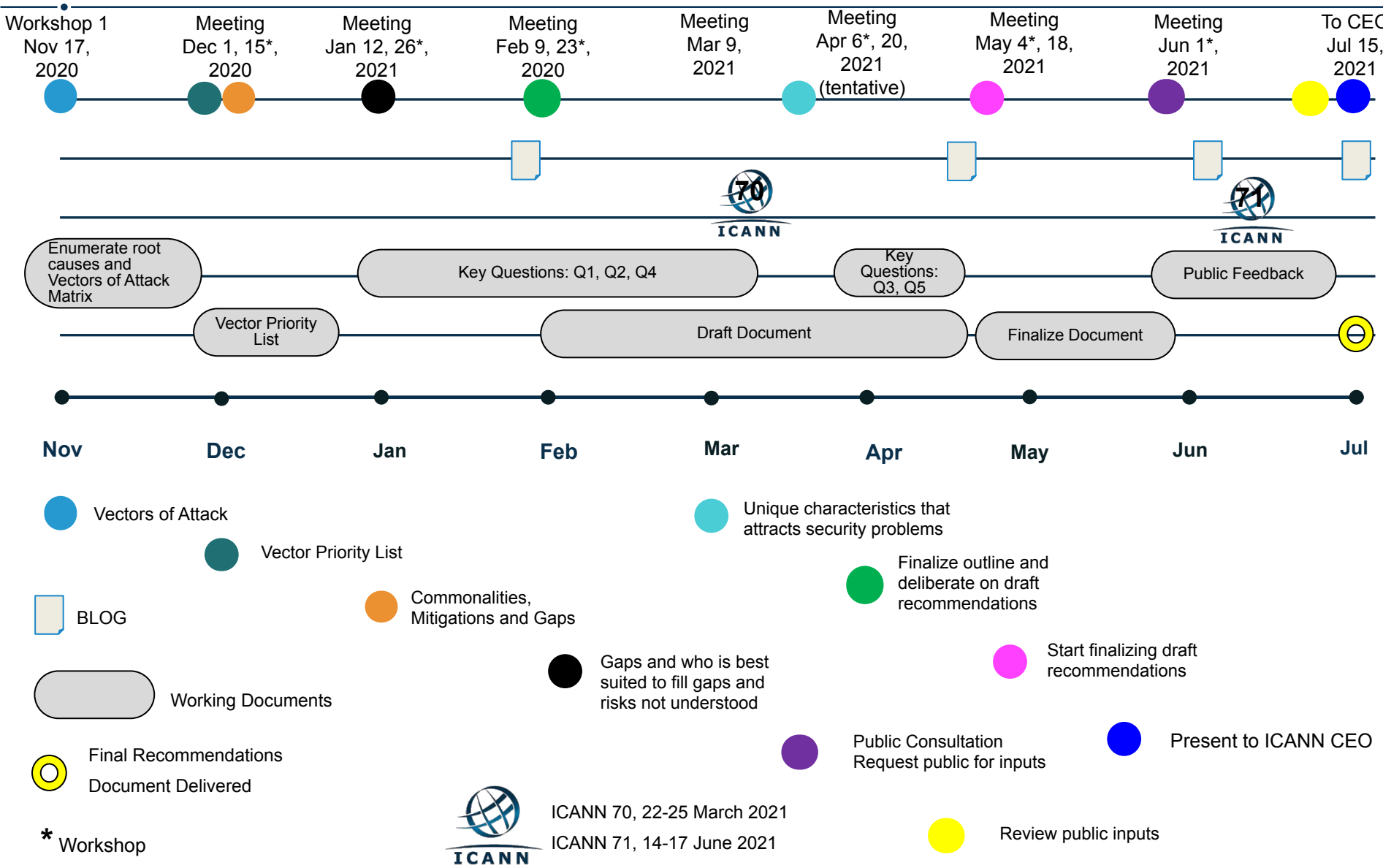
PROJECT: DNS SECURITY FACILITATION INITIATIVE (DSFI)



Vectors of Attack

Vector Priority List

BLOG

Commonalities, Mitigations and Gaps

Working Documents

Gaps and who is best suited to fill gaps and risks not understood

Final Recommendations Document Delivered

Public Consultation Request public for inputs

* Workshop

ICANN 70, 22-25 March 2021

ICANN 71, 14-17 June 2021

Unique characteristics that attracts security problems

Finalize outline and deliberate on draft recommendations

Start finalizing draft recommendations

Present to ICANN CEO

Review public inputs

General Project Plan

Goal - Nov: #1; Dec #2; Jan #3; Feb #4

1. Compare the campaigns discussed so far and enumerate root causes that allowed the attacks to be instantiated. List the attack vectors used for each campaign. Ex: credential compromise, phishing scam (lookalike domain), phishing scam (hijacked domain), etc ; Rate attack vectors in order of which ones are most often seen.

2. Deliberate on answers to Charter Questions **#1, #2 & #4**: What mitigation techniques and best practices exist to address these attack vectors? What are the most critical gaps in the DNS security landscape? What are the risks in the most critical gaps in the DNS security landscape that may not be well understood?

3. Deliberate on Charter Question **#3 & #5**: Who is best suited to fill the gaps that exist in the DNS security landscape? Does the DNS have unique characteristics that attracts security problems, which other Internet services don't have?

4. Start deliberating on some draft recommendations which would include addressing what ICANN should NOT do and what ICANN should do (perhaps in a coordination function). Assess whether any discussions so far lead to

Key Questions

The DSFI-TSG will explore, analyze, and make recommendations that address gaps in the current DNS security landscape:

1. What are the **mechanisms or functions currently available** that address DNS security?

2. Can we identify the **most critical gaps** in the current DNS security landscape?
   a. What are the technical requirements needed to address the gaps?
   b. What operational best practices need to be developed, modified, promoted, or implemented to address the gaps?
   c. What are hindrances to deployments of best practices and other technical measures?

3. Who is **best suited** to fill those gaps?
   a. Is there a role for ICANN org here? Where can ICANN org facilitate improvements to the DNS security landscape?
   b. What strategic partnerships should ICANN org make to enhance DNS security?

4. What are the **risks associated with these gaps** that may not be well understood?
   a. What are the risk considerations?
   b. Where are there gaps in knowledge of the threat models to the DNS ecosystem?
   c. What externalities do people need to be aware of?

5. Does the DNS have **unique characteristics that attract security problems**, which other Internet services don't have?
   a. What can we learn from other protocols or industries that face similar issues (e.g., critical infrastructure industries)?
   b. How can we improve on any existing practices?

December 15th Workshop

Deliberate on answers to Charter Questions #1, #2 & #4: What mitigation techniques and best practices exist to address these attack vectors? What are the most critical gaps in the DNS security landscape? What are the risks in the most critical gaps in the DNS security landscape that may not be well understood?

1. What are the mechanisms or functions currently available that address DNS security?

2. Can we identify the most critical gaps in the current DNS security landscape?
   a. What are the technical requirements needed to address the gaps?
   b. What operational best practices need to be developed, modified, promoted, or implemented to address the gaps?
   c. What are hindrances to deployments of best practices and other technical measures?

4. What are the risks associated with these gaps that may not be well understood?
   a. What are the risk considerations?
   b. Where are there gaps in knowledge of the threat models to the DNS ecosystem?
   c. What externalities do people need to be aware of?

Need volunteers for working with Steve and Samaneh to develop templates for December 15th Workshop.

January 26th Workshop

Continue presentation/discussion of vectors of attack.

Deliberate on answers to Charter Questions #1, #2 & #4: What mitigation techniques and best practices exist to address these attack vectors? What are the most critical gaps in the DNS security landscape? What are the risks in the most critical gaps in the DNS security landscape that may not be well understood?

1. What are the mechanisms or functions currently available that address DNS security?

2. Can we identify the most critical gaps in the current DNS security landscape?
   a. What are the technical requirements needed to address the gaps?
   b. What operational best practices need to be developed, modified, promoted, or implemented to address the gaps?
   c. What are hindrances to deployments of best practices and other technical measures?

4. What are the risks associated with these gaps that may not be well understood?
   a. What are the risk considerations?
   b. Where are there gaps in knowledge of the threat models to the DNS ecosystem?
   c. What externalities do people need to be aware of?

February 23rd Workshop

Presentation/discussion of common mitigations to vectors of attack.

- Which mitigation techniques cover the most attacks?
- Are there mitigation techniques that could benefit from ICANN's facilitation in some manner?
- Are there any gaps in mitigation for attacks that have been identified?

Aim to further answer Charter Questions #1, #2 & #4:

1. What are the mechanisms or functions currently available that address DNS security?

2. Can we identify the most critical gaps in the current DNS security landscape?
   a. What are the technical requirements needed to address the gaps?
   b. What operational best practices need to be developed, modified, promoted, or implemented to address the gaps?
   c. What are hindrances to deployments of best practices and other technical measures?

4. What are the risks associated with these gaps that may not be well understood?
   a. What are the risk considerations?
   b. Where are there gaps in knowledge of the threat models to the DNS ecosystem?
   c. What externalities do people need to be aware of?