b1) Is AuthInfo Code still a secure method for inter-registrar transfers? What evidence was used by the Working Group to make this determination?

The Working Group agreed that it should first establish clarity around the function and definition of the AuthInfo Code and ensure that terminology is clear before addressing specific security requirements. The Working Group used the following text on ICANN.org as a starting point for discussion on the definition of the TAC: "An Auth-Code (also called an Authorization Code, Auth-Info Code, or transfer code) is a code created by a Registrar to help identify the Registered Name Holder of a domain name in a generic top-level domain (gTLD). An Auth-Code is required for a Registered Name Holder to transfer a domain name from one Registrar to another." The Working Group agreed that the term "identify" is inappropriate in this context, because the code does not verify identity in practice. Instead, the TAC is used to verify that the registrant requesting the transfer is the same registrant who holds the domain.

The Working Group considered that a number of different terms currently apply to the same concept, including AuthInfo Code, Auth-Info Code, Auth-Code, Authorization Code, and transfer code. None of these terms clearly describe the function of the code. The Working Group believes that it is clearer for all parties, and particularly registrants, if a single term is used universally. The Working Group believes that "Transfer Authorization Code" (TAC) provides a straightforward description of the code's function, and therefore should serve as the standard term in place of the alternatives.

Regarding the security of the TAC, the Working Group agreed that metrics could support deliberations on charter question b1. In particular, Working Group members were interested to see if there has been a change in the number of unauthorized transfers following adoption of the Temporary Specification for gTLD Registration Data. ICANN's Contractual Compliance Department provided the Working Group with updated metrics regarding complaints received, which covered the periods both before and after the Temporary Specification went into effect. While the Working Group agreed that it is difficult to make conclusions from the data without more granular metrics on the outcomes of the complaints received, the Working Group noted that there was no notable increase in complaints following the date that the Temporary Specification went into effect. A spike in complaints might have been an indication of security shortcomings that would need to be investigated further.

The Working Group considered that in addition to examining metrics regarding past performance, it is important to consider future-state objectives for the TAC. The Working Group agreed that from this perspective, additional security features are appropriate to protect registrants, [particularly in light of the potential elimination of requirements for the Gaining FOA]. In considering potential security enhancements, the Working Group considered the

benefits of requiring these measures, while also taking into account usability considerations and operational impacts on contracted parties in implementing new requirements.

Candidate Recommendation 1: The Working Group recommends that the Transfer Policy and all related policies use the term "Transfer Authorization Code (TAC)" in place of the currently-used term "AuthInfo Code." This recommendation is for an update to terminology only and does not imply any other changes to the substance of the policies.

Candidate Recommendation 2: The Working Group recommends that the Transfer Authorization Code be defined as follows: "A Transfer Authorization Code (TAC) is a code created by a Registrar of Record to validate that a request to transfer a domain name in a generic top-level domain (gTLD) is submitted by the authorized person, which may be the RNH or another appropriate party. The individual demonstrates that they are the authorized person by providing the TAC. A TAC is required for a ~~Registered Name Holder to transfer a~~ domain name to be transferred from one Registrar to another."

Candidate Recommendation 3: The Working Group recommends that the Transfer Policy require that the TAC must be a minimum of [16 characters] [32 characters] in length or any alternative minimum length prescribed by ICANN from time to time.

Candidate Recommendation 4: The Working Group recommends that the Transfer Policy require that the TAC include at a minimum of one uppercase letter, one lowercase letter, one number, and one special character.

Candidate Recommendation 5: The Working Group recommends that the registry verify at the time that the TAC is created in the registry system that the TAC meets the requirements specified in Recommendations 3 and 4.

Candidate Recommendation 6: [The Working Group recommends that the Registry notifies the Registrar of Record ~~[and registrant] receive a notification~~ after [number] failed attempts to enter the TAC. The Registrar of Record may subsequently also provide a notification to the registrant that these failed attempts have taken place. ICANN Org may change from time to time the number of failed attempts that trigger a notification.] OR [The Working Group recommends that after [number] failed attempts to enter the TAC, it is not possible to attempt a transfer for [period of time]. ICANN Org may change from time to time the number of failed attempts that trigger this result.].

b2) The registrar is currently the authoritative holder of the AuthInfo Code. Should this be maintained, or should the registry be the authoritative AuthInfo Code holder? Why?

In considering this charter question, the Working Group focused on evaluating and defining specific roles and responsibilities of registries and registrars in the transfer process, noting that each party has an important role to play in the transfer process. While some Working Group members expressed the view that registry management of the AuthCode would be more uniform, standardized, and transparent, others noted that standards will be set through policy and enforced by ICANN Contractual Compliance regardless of whether the authoritative holder is the registry or registrar; therefore, it is not clear why it would be better to have the registry be the authoritative holder.

The Working Group ultimately did not identify a compelling reason to shift ownership of the TAC to the registry and therefore determined that the registrar should continue to own and generate the TAC. The Working Group further agreed that the registry should continue to verify the validity of the TAC. The Working Group provided recommendations to improve security practices with respect to the TAC to be implemented at the registry.

Candidate Recommendation 7: The Working Group recommends that the registrar continue to own and generate the TAC. The Working Group further recommends that the TAC is only generated by the Registrar of Record upon request by the registrant. After confirmation of successfully setting the TAC at the Registry, w~~W~~hen the registrar provides the TAC to the registrant it should also provide information about when the TAC will expire.

Candidate Recommendation 8: The Working Group recommends that when the registry receives the TAC, the registry must securely store the TAC using a one-way hash that protects the TAC from disclosure~~by using a secure password hashing function (for example, bcrypt)~~.

Candidate Recommendation 9: The Working Group confirms the following provision of Appendix G: Supplemental Procedures to the Transfer Policy contained in the Temporary Specification for gTLD Registration Data: "4. Registry Operator MUST verify that the "AuthInfo" code provided by the Gaining Registrar is valid in order to accept an inter-registrar transfer request."

b3) The Transfer Policy currently requires registrars to provide the AuthInfo Code to the registrant within five [calendar] days of a request. Is this an appropriate SLA for the registrar's provision of the AuthInfo Code, or does it need to be updated?

The Working Group agreed that the Transfer Policy should continue to require registrars to generate, set and provide the TAC to the registrant within a specified period of time following a

request. While some Working Group members felt that the standard time frame for a transfer should be shorter than five calendar days, Working Group members noted that exceptions may be necessary to accommodate specific circumstances. The Working Group did not identify a compelling reason to change the five-day SLA, but noted that it may be appropriate to update the policy language to highlight that five calendar days is the maximum and not the standard period in which the TAC is to be provided.

b4) The Transfer Policy does not currently require a standard Time to Live (TTL) for the AuthInfo Code. Should there be a standard Time To Live (TTL) for the AuthInfo Code? In other words, should the AuthInfo Code expire after a certain amount of time (hours, calendar days, etc.)?

The Working Group clarified its understanding that the Time to Live (TTL) is the period of time that the TAC is valid once the TAC has been created. The Working Group noted that there are no existing policy requirements regarding TTL. The Working Group believes that it is good security practice to have a standard maximum TTL for the TAC, because old, unused TACs are vulnerable to exploitation. The Working Group further believes that a minimum standard TTL will prevent a losing registrar from providing a prohibitively short window of opportunity to legitimately transfer the domain.

Candidate Recommendation 10: The Working Group recommends that the Transfer Policy include a standard maximum Time To Live (TTL) for the TAC of [14 days].

Candidate Recommendation 11: The Working Group recommends that the Transfer Policy include a standard minimum Time To Live (TTL) for the TAC of [period].

b5) Should the ability for registrants to request AuthInfo Codes in bulk be streamlined and codified? If so, should additional security measures be considered?

[For the Working Group to confirm: This question will be addressed when bulk transfers are discussed more generally in Phase 2.]

b6) Does the CPH TechOps research provide a logical starting point for future policy work on AuthInfo Codes, or should other options be considered?

The Working Group carefully reviewed the TechOps proposal and considered input from those involved in development of the proposal. The Working Group appreciated the expertise and relevant experience of those who developed the proposal and therefore considered it a logical starting point for discussion. The Working Group agreed, however, that it is important to consider (i) the range of views and interests that may not have been represented in the development of the proposal, and (ii) any new information or interests that have come to light since the development of the proposal. Therefore, in developing its recommendations, the

Working Group deliberated on each of the charter questions taking into account both the relevant elements of the TechOps paper as well as all other available information and inputs.

b7) Should required differentiated control panel access also be considered, i.e., the registered name holder is given greater access (including access to the auth code), and additional users, such as web developers would be given lower grade access in order to prevent domain name hijacking?

[For the Working Group to confirm: Initial discussions seem to indicate that there should be no new policy requirements.]