AUTH-INFO CODES

INTRODUCTION OF CURRENT APPLICABLE POLICY LANGUAGE

Current Transfer Policy Text re: AuthInfo Codes

- I.5.2 Registrars must provide the Registered Name Holder with the unique "AuthInfo" code and remove the "ClientTransferProhibited" within five (5) calendar days of the Registered Name Holder's initial request if the Registrar does not provide facilities for the Registered Name Holder to generate and manage their own unique "AuthInfo" code and to remove the "ClientTransferProhibited" status.

- I.5.3 Registrars may not employ any mechanism for complying with a Registered Name Holder's request to remove the "ClientTransferProhibited" status or obtain the applicable "AuthInfo Code" that is more restrictive than the mechanisms used for changing any aspect of the Registered Name Holder's contact or name server information.

- I.5.4 The Registrar of Record must not refuse to remove the "ClientTransferProhibited" status or release an "AuthInfo Code" to the Registered Name Holder solely because there is a dispute between the Registered Name Holder and the Registrar over payment.

- I.5.5 Registrar-generated "AuthInfo" codes must be unique on a per-domain basis.

- I.5.6 The "AuthInfo" codes must be used solely to identify a Registered Name Holder, whereas the FOAs still need to be used for authorization or confirmation of a transfer request, as described in Section I.A.2 and Section I.A.4 of this policy.

Current Temp Spec/Interim Reg Data Policy Text re: AuthInfo Codes

- 3. Registrar and Registry Operator SHALL follow best practices in generating and updating the "AuthInfo" code to facilitate a secure transfer process.
- 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.

WORKING DEFINITION

[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.] (source)

- Does this definition require updates or changes?

Some WG members expressed concern that the term "identify" may be inappropriate in this context. Some support was expressed a modified definition that focuses on correlating that the registrant asking for the transfer is the same registrant who owns the domain: "An Auth-Code (also called an Authorization Code, Auth-Info Code, or transfer code) is a code created by a Registrar to validate that a generic top-level domain (gTLD) transfer request is submitted by the authorized person. An Auth-Code is required for a Registered Name Holder to transfer a domain name from one Registrar to another."

- Can the WG agree on a final form as a candidate for a preliminary draft recommendation that this definition formally exist in the consensus policy?

Draft Recommendation 1: The Working Group recommends that the Transfer Policy use the term "Transfer Authorization Code (TAC)" in place of the currently-used term "AuthInfo Code."

Rationale: 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" provides a straightforward description of the code's function, and therefore should serve as the standard term in place of the alternatives.

Draft 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 to validate that a generic top-level domain (gTLD) transfer request is submitted by the authorized person. A TAC is required for a Registered Name Holder to transfer a domain name from one Registrar to another."

Rationale: 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 adjusted the text of the definition to clarify this point.

EARLY WRITTEN INPUT ON THIS TOPIC

Early Written Input received from SSAC on this subject:

The role and significance of the authInfo code was changed dramatically with the introduction of the Temporary Specification for gTLD Registration Data.[1] The SSAC notes that it now functions predominantly as the sole authentication credential used to authorize an inter-registrar transfer. While the process appears to have been working for the past three years, it unfortunately exposes registrants to a domain hijacking vulnerability because the credential is not supported with best practice security principles, processes, or procedures. The SSAC recommends the Transfer Policy Review Team consider this concern and seek the necessary enhancements to the current process that will ensure a secure, stable, and resilient transfer solution in the best interests of the registrant.

The SSAC has previously spoken about registrants and the issues they face when using an authInfo code and transferring between registrars in SAC007,[2] SAC040,[3] SAC044,[4] and SAC074.[5]

In SAC007 the SSAC stated that, "Registrars have an obligation and strong business incentives to reduce the risk of domain hijacking and loss due to mishandling of names and registration information." As part of this obligation registrars should make the use of the Extensible Provisioning Protocol (EPP) authInfo code more uniform, and establish a uniform default setting of domain locks across registrars. The SSAC is supportive of these discussions being in scope and looks forward to a consensus resolution on these important issues from the GNSO Transfer Policy Review PDP WG.

The SSAC again talked about transfer policy in SAC040 in the context of measures registrars should take to protect registrants against account hijacking. SAC040 reiterated the advice given in SAC007.

SAC044 reiterated much of what the SSAC had already said on the subject in SAC007 and SAC040, yet directed towards registrants. Where SAC040 provided advice to registrars on what they should implement, or make more uniform, SAC044 provided similar advice to registrants on how best they can protect their domain names from hijacking. The Transfer Policy Review PDP WG may find this advice helpful as they consider the benefits to, and role of, registrants in a secure, stable, and resilient transfer process.

---

[1] *See Temporary Specification for gTLD Registration Data, https://www.icann.org/resources/pages/gtld-registration-data-specs-enSAC1194*
[2] *See SAC007: Domain Name Hijacking: Incidents, Threats, Risks, and Remedial Actions*
[3] *See SAC040: Measures to Protect Domain Registration Services Against Exploitation or Misuse*
[4] *See SAC044: A Registrant's Guide to Protecting Domain Name Registration Accounts*
[5] *See SAC074: SSAC Advisory on Registrant Protection:Best Practices for Preserving Security and Stability in theCredential Management Lifecycle*

In SAC074, the SSAC built upon its previous work by providing additional advice to registrars. Specifically that registrars and registries followSection 5 of ICANN's 2015 Inter-Registrar Transfer Policy for handling an authInfo code.[6] This report documents specific and anecdotal security concerns at registrars. Although not specifically stated in SAC074, it motivates a need for more uniform handling of the authInfo code. TheTransfer Policy Review PDP WG may find issues highlighted in this report helpful as they consider changes to the handling of the authInfo code to create a more secure, stable, and resilient transfer process for registrants.

See Early Written Input received from RySG on this topic under discussion on charter questions b2 and b4 below and Early Written Input received from the BC under charter questions b1-b6 below.

CHARTER QUESTIONS

RETENTION/OVERALL SECURITY OF AUTH-CODES

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

Note: In answering this question, the Staff Support Team has added a non-exhaustive list of questions for the WG to consider. Many questions were derived from survey feedback to the Transfer Policy Status Report.

Early Written Input received from the BC on this charter question: *It appears secure in the absence of other evidence.*

Deliberations:

The Working Group agreed that it is helpful to establish clear goals for the AuthInfo Code and that responses to more specific questions about security goals can naturally follow once those broader objectives are established. One possible goal of the AuthInfo Code is to ensure that the registrant asking for the transfer is the same registrant who owns the domain, in other words, a correlation check. From a security point of view, it was noted that an excellent way to achieve this goal is a one-time password. It was further noted that the AuthInfo Code functions much like a one-time password, but it is not fully implemented in this way. The Working Group suggested that usability should also be taken into account when considering possible security requirements.

Some Working Group members suggested that metrics about the security of AuthInfo Codes could support the WG's deliberations on these charter questions. For example, WG members

[6] *See SAC074: SSAC Advisory on Registrant Protection:Best Practices for Preserving Security and Stability in the Credential Management Lifecycle*

were interested to see if there has been a change in the number of unauthorized transfers following adoption of the Temporary Specification. The Working Group asked ICANN's Contractual Compliance Department if it had any metrics in this regard and also noted that registrars may be positioned to provide metrics, as well.

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 for gTLD Registry Data 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.

The Working Group noted that there are several different terms used by different parties that all refer to the same concept, and that this inconsistency may be confusing to registrants. The Working Group agreed that the term Transfer Authorization Code (TAC) is a clear and accurate description of the Code's function and agreed that it should be used consistently.

The Working Group agreed that it would be helpful to have standardized requirements for generating and providing/obtaining the AuthInfo Code. The Working Group noted that while it may not be well positioned to provide specific security requirements, it can establish goals and policy parameters to guide the development of specific security requirements by experts, for example CPH TechOps.

- Some survey respondents noted the AuthInfo Code requires updated security features. Does the Working Group agree? If so, what policy considerations should the group consider? For example, should registrars be required to incorporate a mandatory two-factor authentication requirement or similar added verification layer?

Some Working Group members expressed the view that AuthInfo Codes have proven to be secure, while others stated that additional security features are appropriate and necessary to enhance security. Working Group members briefly discussed specific security features, and in particular, whether two-factor authentication should be required, but concluded that it would be more productive to discuss specific security features once the WG has agreed on goals/principles regarding AuthInfo Codes and their security.

- Should a minimum character limit for the AuthInfo Code be considered? Why or why not?
- Should the auth-code be periodically updated? If so, what policy requirements should be considered?
- Should there be policy requirements around managing the syntax of the AuthInfo Code? If so, why?

- Under what circumstances should the Registrar NOT provide the AuthInfo Code following a request from the registered name holder? If any, should these reasons be considered for a potential policy update?
- What other factors (if any) should be considered regarding the security of the AuthInfo Code?
- What other factors (if any) should be considered regarding the retention of the AuthInfo Code in the inter-registrar transfer process?

AUTHORITATIVE HOLDER OF AUTHINFO CODES

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?

Note: As a starting point, the CPH Tech Ops Group concluded "to reach a uniform, transparent, and predictable process, Registries should be in control of the storage and processing of the AuthCode, regarding the technical part."

Early Written Input received from RySG on this charter question: *The RySG believes the current process provides registrars with the greatest flexibility.We understand that no later than at the time of the transfer the incumbent registrar would ensure the registry has the authInfo code available to compare to the value offered by the gaining registrar. This allows the registry to validate the transfer request and, upon validation, to complete the transfer. We believe this minimal registry role supports the greatest opportunity for registrars to create services that are most beneficial to their registrant community.*

Early Written Input received from the BC on this charter question: *Registrar should be authoritative holder.*

Deliberations:

The Working Group conducted preliminary discussions on this charter question and discovered that there was not yet a clear agreement on who should be the authoritative holder. Working Group members noted that it first might be helpful for the group to reach agreement on requirements for the process as a whole, after which the Working Group can delineate specific roles and responsibilities for registrars, registries, and registrants. The Working Group noted that the term "authoritative holder" may ultimately not be an appropriate term to use in making recommendations about roles and responsibilities. Rather, the Working Group may consider that the registry and registrar each manage specific elements of the process. Some Working Group members further noted that any roles and requirements for AuthInfo Codes that are defined in policy recommendations must take into account different business models, including models in which resellers require access to AuthInfo Codes.

In discussing processes related to the provision of AuthInfo Codes, some Working Group members noted that it is possible for systems to be designed such that neither the registry nor

registrar stores the AuthInfo Code for any length of time. For example, the registrar can be responsible for supporting the registrant in generating the AuthInfo Code on demand. The registry may only need to store the AuthInfo Code (or a hash of the AuthInfo Code) briefly in order to verify that the AuthInfo Code provided by the registrant matches the AuthInfo Code on record. In such a scenario, there may not be a need for an "authoritative holder."

- What does the WG consider to be the advantages (if any) of maintaining the registrar as the authoritative holder of the AuthInfo Code?
- What does the WG consider to be the disadvantages (if any) of maintaining the registrar as the authoritative holder of the AuthInfo Code?
- What does the WG consider to be the advantages (if any) of changing the authoritative holder of the AuthInfo Code to the registry?
  - Some Working Group members believe that:
    - If it is in policy that the registry is the authoritative holder, the management of the AuthCode will be more uniform, standardized, and transparent.
    - There is a security benefit of a neutral party with a standardized audit trail managing the process.
  - Other Working Group members believe that:
    - Standards will be set through policy and enforced by Contractual Compliance regardless of who is the authoritative holder, therefore it is not clear why it would be better to have the registry be the authoritative holder.
- What does the WG consider to be the disadvantages (if any) of changing the authoritative holder of the AuthInfo Code to the registry?

PROVISION OF THE AUTHINFO CODE

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?

Note: The Transfer Policy currently requires the Registrar to provide the AuthInfo Code to the registrant with five calendar days of a request. For reference, the CPH Tech Ops Group chose to retain the five-calendar day SLA.

Early Written Input received from the BC on this charter question: *Should be instant.*

Deliberations:

In initial discussion of this charter question, Working Group members noted that it would be helpful to first decide if the Working Group is seeking to make recommendations in the context of current processes or whether it will re-envision how the processes will work. Working Group members also agreed that it would be helpful to further explore different business models to

understand the potential impact of changing the SLA for providing the AuthInfo Code. In particular, Working Group members seek to understand if there are registrars that rely on manual verification processes that require longer SLAs.

In further discussion, Working Group members expressed support for continuing to have an SLA, although there were different perspectives on what that SLA should be. Some support was expressed for changing the policy language from "within 5 calendar days" to "up to 5 calendar days" to highlight that the SLA is a maximum time frame and not a standard time frame for provision of the AuthInfo Code.

- Does the WG consider the current five-calendar day SLA a reasonable SLA for provision of the AuthInfo Code? Why or why not?
- Is there any reason to shorten or lengthen the SLA?
- Should the current requirement re: mechanism to transmit the AuthInfo Code remain intact also? [Current requirement provides: I.5.3 Registrars may not employ any mechanism for complying with a Registered Name Holder's request to […] obtain the applicable "AuthInfo Code" that is more restrictive than the mechanisms used for changing any aspect of the Registered Name Holder's contact or name server information"]

EXPIRATION OF THE AUTHINFO CODE

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.)?

As a starting point, the CPH Tech Ops Group concluded "in regard to the TTL the group suggested a validity of no more than 14 days, presented as the total number of hours until TTL expiration. There was no resolution for a minimum TTL requirement, because registrars with different business models may have different requirements for how quickly a domain name gets unlocked and transferred. More work on any of these topics is needed."

Early Written Input received from RySG on this charter question: *The RySG is supportive of the concept of carefully managing the period of time during which a registrant may transfer their domain. We acknowledge that this is a beneficial security service to a registrant. Similar to our response to question b2, we believe that registrars should have the flexibility to manage the TTL according to the needs of their registrants.*

Early Written Input received from the BC on this charter question: *Yes. Should expire after period of time, such as 3 days, provided it is provided instantly.*

Deliberations:

- Should a standard TTL be required for the AuthInfo Code? Why or why not?
  - A number of WG members expressed support for TTL requirements, noting that TTL is a good security practice, because old, unused codes are vulnerable to exploitation.
    - Other WG members felt that TTL should only be considered if there is evidence that domains have been hijacked because unused codes were later accessed by unauthorized parties. Some Working Group members believe that TTL may not be needed absent this evidence.
  - One possibility is that there is a maximum system TTL that the registry is responsible for. Once the period ends, if the gaining registrar provides the code to the registry, it will fail.
    - Pro of registry being responsible for TTL: possibly more consistent implementation.
    - Con of registry being responsible for TTL: registrar loses control but still needs to provide the customer support when questions/issues arise.
    - Consideration: is it better security practice to have the registry or registrar responsible?
  - The Working Group considered the possibility that TTL could be at the discretion of individual registrars rather than being set by policy. It was noted that if there is a policy requirement regarding TTL, different business models should be considered to ensure that different types of registrars can implement the requirements.
- If so, is the TechOps proposal of "no more than 14 days" acceptable to the Working Group? Why or why not?
  - The Working Group clarified its understanding that the TTL is the period of time that the code is valid once it has been created.
  - From one perspective, 14 days may be too long for certain high-value domains. The Working Group considered that the TTL could be shorter in certain cases. This "finer grain" TTL could potentially be managed at the registrar.
  - It was noted that a standard minimum TTL could be recommended by the WG in addition to a maximum TTL. This could prevent a registrar from setting a TTL aggressively low to make it very difficult for a registrant to transfer a domain.
    - It was noted that even with a minimum TTL, the registrar still needs to be able to overwrite with a NULL code in case the TAC is compromised.

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

Note: As a starting point, this charter question was added in response to the following feedback to the Transfer Policy Status Report Survey from the RrSG:[It's] [d]ifficult for Registered Name Holders to retrieve [AuthInfo Codes] for a long list of domains as there are no requirements to permit bulk [AuthCode] requests. (Note: the discussion of partial bulk transfers and the BTAPPA process will be discussed in Phase 2 under question i2. This discussion is limited to the consideration of bulk retrieval of AuthInfo Codes.)

Early Written Input received from the BC on this charter question: *Ideally bulk requests should be streamlined. But in their absence registrars do provide this service, albeit manually.*

Deliberations:

- In light of this concern, should the bulk retrieval of AuthInfo Codes be considered? Why or why not?
  - The Working Group generally agreed that it should be possible to request AuthInfo Codes in bulk, but that it should be up to the individual registrar to determine how to handle these requests.
- If yes, should additional policy requirements be considered? For example, should an added layer of protection be considered for the provision of more than one AuthInfo Code?
  - At this time, there does not appear to be support for new policy on this topic.

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

Note: As a starting point, the Support Staff Team has included relevant portions of the CPH TechOps paper under the relevant charter questions; however, this does not prevent the WG from considering both the pros and cons of the TechOps suggestions and alternative proposals.

Early Written Input received from the BC on this charter question: *Yes.*

Deliberations:

In initial discussions, the Working Group supported using the TechOps proposal as a starting point but agreed that it is important to consider alternatives and examine what might be missing from the TechOps proposal.

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?

Note: As a starting point, this charter question was included in response to the following feedback from the Transfer Policy Status Report Survey, "I am concerned about who receive[s] [the AuthCode][.] [I]f we could confirm that only [the] registrant can receive [the AuthCode], then we may no longer need FOA."

Early Written Input received from the BC on this charter question: *Yes, ideally.*

Deliberations:

- Should differentiated control panel access be a requirement under the Transfer Policy as an added security measure? Why or why not?

Working Group members noted that there could be security benefits to differentiated control panel access, but that implementation would be difficult in practice for registrars. Some Working Group members expressed that requirements under existing law are sufficient to ensure good security practices with respect to account management. Working Group members discussed that the Working Group could provide a list of good security practices but not require these practices as policy.

SMALL GROUP OUTCOMES

HIGH-LEVEL PROPOSED PRINCIPLES:

- Transfer Authorization Code (TAC) is an Authorization Credential that upon presentation by a registrant recognizes that registrant as the owner of its corresponding domain name.
    - Consideration: Are there other uses of the TAC that need to be taken into account? Can we document those use cases?

- Should only exist at registry when a transfer is [eligible to be] in progress
    - This suggests that regardless of when a registrar creates a TAC, it is not passed to the registry unless a transfer is in progress
    - Clarification: TAC would only exist at the registrar when the RNH requests it/does something to trigger the creation. That way the Rr knows to also send it to the Ry.
    - Why:
        - Progresses the principle that TAC is a one-time password and there should be very little storage of the TAC.
        - Makes it clear when transfers can occur and cannot occur.
    - Consideration: Impact on existing business processes.

- Must be unique per registrant and per domain name
    - The value must be safe and secure and not reproducible outside of the registrar, i.e., one-time password
    - Consideration: impact on bulk transfers (see also charter question b5).

- Must not be retrievable from the registry
    - A registrar can set it but a registry will never respond with it, other than to validate if an accurate one was submitted (rate limits to avoid brute force)
    - A registrar would set a "NULL" or send new TAC to remove it from the registry or update the existing TAC
    - If a RNH needs to reconfirm a code, registrar sets a new one rather than providing the same code again.
    - Why:
        - Maintain uniqueness characteristic.
        - Avoid risk that the code could be picked up and used.

- Registrars should manage any TTL scheme
    - Why: Registrars maintain control of the transfer process.
    - See additional summary of discussion on TTL under charter question b4.

- SHOULD be updated at the registry upon completion of owner change process.
    - Why: Helps to ensure that once the code has been used it cannot be used again.

STRAWMAN LIST:

The following could potentially be requirements, industry practices, or optional items that CPs could adopt:

- The registrar creates AuthInfo code and it is hashed at the registry.
- It's not stored at the registrar and it is stored at the registry [but it only exists at the registry when the transfer is in progress].
    - Considerations:
        - How would this impact existing practices under different business models (for example, resellers)?
        - If the registrar no longer stores the code, it is not able to troubleshoot if the registrant is having trouble using the code. Counterpoint: The process could be that if a RNH needs to reconfirm a code, registrar sets a new one.
        - It's not stored at the registrar, how does this impact user experience for the RNH?
        - It's not stored at the registrar, what is the impact on bulk transfers?
    - See also summary of discussion on TTL under charter question b4.

    - It was noted that this bullet includes multiple concepts. This bullet might be better broken into several items considered individually in future discussions.
- Two-factor authentication, by whatever means the registrar sees fit (not necessarily using cell phone number, could be for example a security question).
    - Clarification: this item refers to two-factor authentication to access the account as opposed to two-factor authentication to request the code itself.
    - Considerations:
        - Is this something the WG could actually require or would be a suggested best practice instead?
        - Potential usability impact/increase in customer support requests.
    - Alternative: Use more general terminology rather than two-factor authentication, for example in “a secure manner” or using “a secure mechanism.”
        - Why: More general terminology provides more flexibility for how to implement. In addition, technology changes over time. If recommendations are too prescriptive they will become out of date.
        - Consideration: If not written in policy, how does a registrar demonstrate to ICANN in response to a complaint that the security measures the registrar implements are not limiting a RNH’s ability to transfer?
        - Additional consideration: If the language is too vague, will it actually result in increased security?
- 32 character min [Alternative: 16 characters].
    - Why: Reduces the chance of an unauthorized party guessing the AuthCode.
    - Considerations:
        - Tradeoff between security and usability in establishing the minimum length - a longer minimum may be less usable.
        - How do you decide on a minimum number? If a number is specified as a requirement, will it become obsolete/out of date?
- Require uppercase and lowercase letters, numbers, and special characters. Prohibit use of dictionary words.
    - Why: Reduces the chance of an authorized party guessing the AuthCode.
    - +Homoglyph consideration (0 vs O) see below.**
    - Additional considerations:
        - Use NIST as a guide for requirements?
        - Could you require using, for example, three out of four of the above to ensure complexity but avoid being too prescriptive?
        - What is a “dictionary word” -- which dictionary?

        - Could only specific dictionary words be prohibited, for example “password”? In which languages?
- Registry check to ensure AuthCode meets minimum syntax requirements.
    - Why: prevent fringe registrar actors from violating requirements.
    - Consideration: Implementation impact on registries.
    - Alternative: Could this check happen at the registrar instead? How could this look in practice?
- Failed attempt identification/notification after a certain number of requests to initiate a transfer.
    - What: ServerTransferLock at threshold x, notice to incumbent registrar, other
    - Why: Adds integrity to legitimate xfer [slow manual incumbent, automated gaining process], guards against illegitimate [brute force].
    - Considerations: Do we want registries to be “checking up” on registrars? Is this division of control desirable? If notification is implemented, who receives the notification (registrar only or registrar & RNH)?
- Can Transfer Lock status affect requesting/updating auth code in addition to just blocking a transfer request? In other words, should the lock need to be off in order for it to be possible to request/update the code?
    - Consideration: Is there clear added value to this measure?

**Homoglyph detail
Note on Uniqueness and Humans Note:
Not everyone will cut-paste these. Imagine someone writing the code down onto a post-it note to use, try to reduce confusion potential while preserving the random/uniqueness. The following considerations will help.

- Start/End character limitation can reduce the confusion potential on presentation of the string First and last char should be alphanumeric; punctuation at end; quotes or Paren, Curly, and Bracket open or close should not be at front or end of string, respectively. (Example: [P$o3ffe-=!A3d] - Would this cause a user to ask themselves, “are the brackets included?”)
- Homoglyph (lookalike) characters should be considered and more than one use from within a set should be avoided where possible within a given string.
  Non-Exhaustive Examples of visually similar (fonts or writing style can impact this):
    - Do not include both zero (0) and upper case “Oh” (O),
    - Pipe (|), Exclamation (!), lower case “ell” (l), number one (1), uppercase “eye” (I),
    - Lower case “bee” (b) and the number six (6),
    - Upper case “bee” (B), lower case “gee” (g) and the number eight (8),
    - Upper case “Tee” (T), the number seven (7),

- etc...

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. A TAC is required for a Registered Name Holder to transfer a domain name 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 that the TAC meets the requirements specified in Recommendations 3 and 4.

Candidate Recommendation 6: [The Working Group recommends that the Registrar of Record [and registrant] receive a notification after [number] failed attempts to enter the TAC. 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. When 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 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 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.]