# Change of Registrant (COR)

TPR Group 1(b): Part II

Meeting #111

ICANN

# Security Measures: Improper CORs

What should be the minimum requirement for Registrars when an improper COR occurs?

# Security Measures: Improper CORs

**What should be the minimum requirement for Registrars when an improper COR occurs?**

Option 1: Provide contact information for questions (current Transfer Policy)

- Before or within one day of the completion of the COR, the Registrar must send a notification to the New Registrant and Prior Registrant. This notification must:
    1. explain the request that was received
    2. list the domain(s) in question
    3. provide contact information for questions
    4. ~~inform them of the 60-day lock~~

- i.e. The Transfer Policy should not require any further measures from the Registrar, allowing them to address reports of improper CORs as they see fit, based on their own policies and practices.

# Security Measures: Improper CORs

**What should be the minimum requirement for Registrars when an improper COR occurs?**

**Option 1**: Provide contact information for questions (current Transfer Policy)

**Example Scenario:**

John Doe receives a notification that the email address associated with managing johndoe.com has been changed.

Since he did not request this change, he uses the email/phone number provided in the notification to contact his Registrar.

# Security Measures: Improper CORs

**What should be the minimum requirement for Registrars when an improper COR occurs?**

**Option 2:** In addition to providing contact information, require Registrars to investigate and respond to reports of improper CORs.

- E.g. 2013 RAA, Section 3.18: "*Registrar shall take reasonable and prompt steps to investigate and respond appropriately to any reports of abuse*."

- How the Registrar investigates and/or responds to the issue would still depend on its policies/practices and the facts of the incident

- Registrars cannot ignore reports of improper changes to a registrant's anchor contact method.

# Security Measures: Improper CORs

**What should be the minimum requirement for Registrars when an improper COR occurs?**

**Option 2:** In addition to providing contact information, require Registrars to investigate and respond to reports of improper CORs.

**Example Scenario:**

John Doe receives a notification that the email address associated with managing johndoe.com has been changed.

Since he did not request this change, he uses the email/phone number provided in the notification to contact his Registrar.

The Registrar responds to John's complaint, stating that based on the evidence, the COR was improper, and *reverses the change* (?)
**OR**
The Registrar responds to John's complaint, stating that based on the evidence, the COR was proper, so the *change remains in place*.

# Security Measures: Improper CORs

**What should be the minimum requirement for Registrars when an improper COR occurs?**

**Option 3:** Registrars must provide a dispute/appeal process through which a Prior/New Registrant can challenge and correct an improper COR.

- Non-prescriptive of what the dispute/appeal process should be, allowing Registrars flexibility in operationalizing

- How the improper COR would be disputed/appealed depends on the Registrar's policies and the nature of the incident
  - (e.g. was the registrant's account or anchor contact method compromised? Were the Registrar's procedures for updating anchor contact properly followed? Is there sufficient evidence? etc…)

# Security Measures: Improper CORs

**What should be the minimum requirement for Registrars when an improper COR occurs?**

**Option 3:** Registrars must provide a dispute/appeal process through which a Prior/New Registrant can challenge and correct an improper COR.

**Example Scenario:**

John Doe receives a notification that the email address associated with managing johndoe.com has been changed.

Since he did not request this change, he follows the dispute/appeal instructions provided in the notification.

John submits a ticket with answers to a set of questions and attached evidence about the incident, *per the Registrar's appeal process*.

The Registrar reviews John's answers and evidence, and determines that the change was improper. *The information is then changed back*.

# Security Measures: Improper CORs

**What should be the minimum requirement for Registrars when an improper COR occurs?**

**Option 4:** Registrars must provide a *specific* appeal process (TBD by WG) through which a Prior/New Registrant can challenge and correct an improper COR.

- All Registrars must follow a specific appeal process (or an appeal process with specific criteria) to ensure an improper change to anchor contact method can be corrected.
    - E.g. may require Registrars to retain the Prior Registrant’s data for a period of time
    - E.g. may require a specific timeframe by which Registrars must respond or act
    - E.g. may require Registrars to lock the domain name(s), preventing changes until the matter is resolved
    - E.g. may require specific types of evidence from the registrant

- What elements must the appeal process entail? (initiation - investigation - resolution)

# Security Measures: Improper CORs

**What should be the minimum requirement for Registrars when an improper COR occurs?**

**Option 4:** Registrars must provide a *specific* appeal process (TBD by WG) through which a Prior/New Registrant can challenge and correct an improper COR.

**Example Scenario:**

John Doe receives a notification that the email address associated with managing johndoe.com has been changed.

Since he did not request this change, he follows the appeal instructions provided in the notification.

The Registrar follows the (TBD) appeal process outlined in the Transfer Policy, and determines the change was improper. *The information is then changed back*.

# Security Measures: Improper CORs

**What should be the minimum requirement for Registrars when an improper COR occurs?**

**Option 5:** Other: __________

- ★ What other solutions are there to address improper CORs, not followed by a TAC request (e.g. CORs resulting from compromised accounts/anchor contact methods)?
- ★ Are any elements (or combinations) of the previous options useful toward a different solution?

# Poll Question 1 - Improper CORs

# Poll Question 1: Improper CORs

**Of the Options discussed thus far, which can you support as a minimum requirement for Registrars when an improper COR occurs?** *Select your first, second, and third choices (if applicable)*

**Option 1:** Registrars must **provide contact information** for questions (current policy)

**Option 2:** Registrars must **investigate/respond to reports** of improper CORs

**Option 3:** Registrars must **provide a dispute/appeal process** to correct improper CORs

**Option 4:** Registrars must **provide an appeal process with specific criteria** to correct improper CORs

**Option 5: Other**: __________

**Option 6:** None of the above

# Security Measures: COR followed by a TAC request

What should happen when a COR is followed by a request to transfer Registrars?

# Security Measures: COR + TAC request

**What should be the minimum requirement for Registrars when a TAC request follows a completed COR?**

**Option 1**: No special requirements are necessary.

- The TAC must be provided within 5 calendar days of the registrant's request, regardless of any recent change to the registrant's anchor contact method(s).
- There is no required 60-day Registrar transfer lock following a change to the registrant's anchor contact method.
- Registrars could potentially utilize the voluntary/Registry-level lock, without requiring a lock in the Transfer Policy.

# Security Measures: COR + TAC request

**What should be the minimum requirement for Registrars when a TAC request follows a completed COR?**

**Option 1:** No special requirements are necessary.

**Example Scenario:**

Jane Doe's email address is updated. The Registrar receives a TAC request from the new email address.

The Registrar provides the TAC within 5 calendar days, and sends a notification of TAC issuance to the registrant's new email address.

The TAC is used to transfer her domain name, janedoe.com, to a different Registrar.

The (Losing) Registrar sends a notification of Transfer Completion to the registrant's new email address within 24 hours.

# Security Measures: COR + TAC request

**What should be the minimum requirement for Registrars when a TAC request follows a completed COR?**

**Option 2**: The TAC must be provided within 5 calendar days ONLY if no objection from the New or Prior Registrant is received during that time.

- If there was a recent COR, a TAC request could trigger a notification to the New Registrant (and Prior Registrant?) informing them there will be a 5-day waiting period before the TAC can be issued.

- If the New or Prior Registrant contacts the Registrar (via designated channel) and objects to the COR/TAC request within this window, then the TAC would not be issued and the improper COR process would be triggered.

    - During the 5-day waiting period, if the New and Prior Registrant both contact the Registrar and provide their authorization to transfer Registrars, the TAC could be issued earlier (?)

# Security Measures: COR + TAC request

**What should be the minimum requirement for Registrars when a TAC request follows a completed COR?**

**Option 2:** The TAC must be provided within 5 calendar days ONLY if no objection from the New or Prior Registrant is received during that time.

**Example Scenario:**

Jane Doe's email address is updated. The Registrar receives a TAC request from the new email address.

The Registrar sends a notification to Jane Doe, saying that because of the recent change of email, there will be a 5 day waiting period.

By the end of the 5 days:
(A) no objection is received from the New or Prior Registrant. The Registrar issues the TAC within 24 hours.
**OR**
(B) the Registrar receives an objection from the Prior Registrant's email, stating that the recent contact information change was not authorized. The Registrar notifies the New and Prior Registrant that TAC cannot be issued, and its procedures for handling improper CORs is triggered.

# Security Measures: COR + TAC request

**What should be the minimum requirement for Registrars when a TAC request follows a completed COR?**

**Option 3:** The TAC must be provided within 5 calendar days ONLY if a recent change to the New Registrant’s (and Account Holder’s*) contact information is successfully verified, per the 2013 RAA Whois Accuracy Program Specification.

- When there is a change to the Registered Name Holder’s Whois information or the corresponding customer account holder contact information, the Registrar will typically send a verification request by email or phone.

- If the Registrar does not receive an affirmative response from the RNH within 15 days, the Registrar either verifies the applicable contact information manually, or suspends the registration.

- Registrars should deny any TAC requests received prior to an applicable verification of changed contact information.

*Per 2013 RAA Definitions (1.1): "Account Holder" means the person or entity that is paying for the Registered Name or otherwise controls the management of the registered name, when that person or entity is not the Registered Name Holder.

# Security Measures: COR + TAC request

**What should be the minimum requirement for Registrars when a TAC request follows a completed COR?**

**Option 3:** The TAC must be provided within 5 calendar days ONLY if a recent change to the New Registrant's (and Account Holder's) contact information is successfully verified, per the 2013 RAA Whois Accuracy Program Specification.

**Example Scenario:**

Jane Doe's email address is updated. The Registrar sends a verification request to the new email address.

The Registrar receives a TAC request from the new email address, which it denies because the new email address has not yet been verified.

Jane Doe verifies the new email address, and requests the TAC again.

The Registrar provides the TAC within 5 calendar days, and sends a notification of TAC issuance.

# Security Measures: COR + TAC request

**What should be the minimum requirement for Registrars when a TAC request follows a completed COR?**

**Option 4:** When a COR occurs, Registrars must place a 30-day inter-registrar transfer lock on the domain name(s), unless previously opted-out by the registrant. Additionally, the Registrar may remove this lock after placing it, upon agreement of the Registrar and the registrant.

- Provides 30 days for a registrant to report an improper COR (30 days is consistent with Phase 1a reqs)
- Allows Registrars to make the determination whether to remove the lock before the conclusion of the 30 days, should the registrant and Registrar both agree.

# Security Measures: COR + TAC request

**What should be the minimum requirement for Registrars when a TAC request follows a completed COR?**

**Option 4:** When a COR occurs, Registrars must place a 30-day inter-registrar transfer lock on the domain name(s), unless previously opted-out by the registrant. Additionally, the Registrar may remove this lock after placing it, upon agreement of the Registrar and the registrant.

**Example Scenario:**

Jane Doe's email address is updated. The Registrar places a 30-day inter-registrar transfer lock on janedoe.com.

The Registrar receives a TAC request from the new email address, which is denied by the Registrar, citing the recent COR.

Jane Doe's new email address requests the Registrar to remove the lock. After conversing with Jane, the Registrar makes the determination to remove the lock.

The Registrar provides the TAC within 5 calendar days, along with the notification that the TAC has been issued.

# Security Measures: COR + TAC request

**What should be the minimum requirement for Registrars when a TAC request follows a completed COR?**

**Option 5**: The Registrar must offer the Registrant an OPT-IN option for added protection(s).

- The opt-in option should be offered upon registration, or otherwise prior to a COR/TAC request
- Such added protections could possibly include:
    - multi-factor authentication (for COR/inter-registrar transfer requests)
    - requiring COR confirmation from both the Prior Registrant and New Registrant
    - longer waiting period before the TAC is issued when following a COR
    - voluntary transfer lock
    - Etc.

# Security Measures: COR + TAC request

**What should be the minimum requirement for Registrars when a TAC request follows a completed COR?**

**Option 5:** The Registrar must offer the Registrant an OPT-IN option for added protection(s).

**Example Scenario:**

Jane Doe receives a notification from her Registrar, detailing the optional protections it offers.

Jane Doe opts for two-factor authentication for any change to her contact information, as well as a longer TAC waiting period.

Later, Jane Doe wishes to update her email address and transfer Registrars.

In accordance with her selected options and the Registrar's policy, Jane logs into her account and then returns a unique code to the Registrar, sent via SMS.

The Registrar accepts her change of email address and her TAC request, issuing the TAC to the new email after the longer waiting period.

# Security Measures: COR + TAC request

**What should be the minimum requirement for Registrars when a TAC request follows a completed COR?**

**Option 6**: Other: __________

- ★ What other solutions could protect against unwanted Registrar transfers, in cases of potentially improper CORs?
- ★ Are any elements (or combinations) of the previous options useful toward a different solution?

# Poll Question 2 - COR followed by a TAC request

# Poll Question 2 - COR followed by a TAC request

**Of the Options discussed thus far, which can you support as a minimum requirement for Registrars when a TAC request follows a completed COR?** *Select your first, second, and third choices (if applicable)*

**Option 1: No special requirements are necessary**.

**Option 2:** There should be a **waiting period before issuing the TAC**, allowing time for **objections**.

**Option 3:** Before issuing the TAC, **changes to RNH/Account Holder information must be verified.***

**Option 4:** Following a COR, impose a **30-day transfer lock, but allow Registrars to lift it**, if agreed.

**Option 5:** Registrars must offer registrants an **opt-in option for added protection**.

**Option 6: Other**: __________

**Option 7:** None of the above

* according to existing procedures under the 2013 RAA Whois Accuracy Program Specification

# Appendix: Whois Accuracy Program Specification

# Whois Accuracy Program Specification

Within 15 days of any change in the Registered Name Holder, the Registrar will, with respect to both Whois information and the corresponding customer account holder contact information related to such Registered Name:

Validate:

- the presence of data for all required fields (RAA Subsection 3.3.1) are in a proper format for the applicable country/territory.
- that all email addresses are in the proper format
- that telephone numbers are in the proper format for international telephone numbers
- that postal addresses are in a proper format for the applicable country or territory
- that all postal address fields are consistent across fields (for example: street exists in city, city exists in state/province, city matches postal code) where such information is technically and commercially feasible for the applicable country/territory.

Verify:

- the **email address** of the Registered Name Holder (and, if different, the Account Holder) by sending an email requiring an affirmative response through a tool-based authentication method such as providing a unique code that must be returned in a manner designated by the Registrar, or
- the **telephone number** of the Registered Name Holder (and, if different, the Account Holder) by either (A) calling or sending an SMS to the Registered Name Holder's telephone number providing a unique code that must be returned in a manner designated by the Registrar, or (B) calling the Registered Name Holder's telephone number and requiring the Registered Name Holder to provide a unique code that was sent to them via web, email or postal mail.

# Whois Accuracy Program Specification

If the Registrar does not receive an affirmative response from the Registered Name Holder, the Registrar shall either verify the applicable contact information manually or suspend the registration, until such time as Registrar has verified the applicable contact information.

If the Registrar does not receive an affirmative response from the Account Holder[1], the Registrar shall verify the applicable contact information manually, but is not required to suspend any registration.

The Registrar is NOT required to perform the validation and verification procedures if the Registrar has already successfully completed the validation and verification procedures on the identical contact information and is not in possession of facts or knowledge of circumstances that suggest that the information is no longer valid.

HOWEVER, if the Registrar has any information suggesting that the contact information specified is INCORRECT (such as Registrar receiving a bounced email notification), the Registrar must verify or re-verify, as applicable, the email address(es).

[1] "Account Holder" means the person or entity that is paying for the Registered Name or otherwise controls the management of the registered name, when that person or entity is not the Registered Name Holder.