# **Design Team 5 (Authorization Function) report**

Design Team 5 is concerned with the choice posed most clearly by ICANN's Security and Stability Advisory committee report SAC 069: "From a technical and operational perspective, either (1) eliminating the NTIA authorization step entirely or (2) replacing it with an equally efficient process performed by another entity, may suffice to preserve the current stability of root zone change request processing." Design Team D has concluded that option 1 should be recommended, for the reasons set out below.

# What does the NTIA currently do?

According to [a document from the U.S. Commerce Department NTIA](http://www.ntia.doc.gov/files/ntia/publications/ntias_role_root_zone_management_12162014.pdf), authorization consists of the following steps:

* Ascertaining that the change was transmitted securely
* Ascertaining that it include the standard set of information (i.e., summary of requested changes) in the right format

In addition:

* ICANN self-certifies that it followed its processes
* ICANN formally asks for authorization

In other words, ICANN submits proposed changes, self-certifies that it has followed the proper process, and asks NTIA for authorization. NTIA verifies that the change request is submitted securely and is correctly formatted.

# Analysis of the Authorization Function

The DT-5 makes the following observations about the current authorization function:

1. NTIA does not independently verify the accuracy of the change or confer with the change requestor. Thus, the authorization function adds no substantive error-checking to the change process.
2. The change transmission and formatting steps currently subject to NTIA authorization have been automated. Manual authorization by NTIA, which focuses mainly on the formatting and secure transmission of the changes, adds little value to these automated processes.
3. NTIA relies on self-certification by ICANN that it followed its processes. If it turned out that ICANN submitted a new TLD or change request that was not based on its processes, the authorization function itself does not provide a means of catching that deviation. If a deviation from process was discovered by the NTIA or the broader community later, ICANN could only be held accountable through the NTIA contracting for the IANA functions operator. Thus, the leverage over unauthorized changes does not come from the authorization process itself.
4. There has never been a case where NTIA did not authorize a change request, but there was one case (.xxx) in which there was active discussion within the US of the possibility of refusing to authorize a controversial domain in response to vocal demand by domestic political actors.

In sum, the authorization function adds little to the security or accuracy to the process, but provides the USG with a residual power that could be used to (at best) retroactively punish ICANN (via the contracting process) for making unauthorized RZF changes or (at worst) veto a RZF change that was authorized by the policy process.

# Liability and the authorization function

Any new entity in the position of Authorizer would likely be legally liable if a serious error occurred that damaged registries and/or registrants. The NTIA role as authorizer removed most liability risk from both ICANN and Verisign; indeed, the function was instituted in October 1998 as Amendment 11 to the Cooperative Agreement with Verisign in order to protect Verisign from potential liability raised by an antitrust lawsuit. The USG (NTIA) role represented a significant challenge to anyone considering legal action against the parties involved in root zone changes. In any post transition environment, a private party who took over the authorization function would face similar liability issues.

***<more discussion of who or what might be liable in the absence of NTIA needed>***

# Conclusion 1

No authorization for TLD change requests is needed. Based on the above analysis, Change requests currently are generated by an automated system and the Root Zone Maintainer side will only accept securely transmitted and properly formed requests. The risk of mistakes are minimal and are not significantly mitigated by the existence of an authorization function.

# Conclusion 2

The risk of out of policy TLD changes, TLD creations or other deviations from process are best addressed not through an authorization function, but through other IANA-related accountability mechanisms.

Changing the authorization step to go beyond simply accepting a self-certification that policy was followed would require a DNS knowledgeable third party to be privy to all TLD change requests, implying a substantial change to existing processes, policy, and code. That is probably not the best way to guard against such problems. Preventing such occurrences is best handled through institutional arrangements that favor transparency, clear separation of the ICANN policy making and IANA implementation functions, and some kind of *post hoc* appeals or redress mechanism.