Supplemental Budget 2020-2024

Reflected in provisions for extraordinary
expenses constituted per 2020-12-31

Revised as of 2021-06-25 based on
Member input at 2021-06-22 Extraordinary Plenary

1. Introduction: Submission for approval of Supplemental Budget for 2020-2024 reflected in provisions for extraordinary expenses funded with the capital gain resulting from the Donuts-Afilias merger in 2020

1.1. Background

In late 2020, Afilias agreed to merge with Donuts, Inc (another Internet domain names registry operator). As a minority shareholder, CORE Association ("CORE") had no power to influence the merger decision. On December 31, 2020 CORE received a merger consideration of USD 3.12 million. As a result of the merger, Afilias has ceased to exist as an independent company. Since the value of Afilias shares on CORE's books had been based on the original cost, almost the entire merger consideration constitutes a capital gain.

This document describes a budget and corresponding provisions for extraordinary expenses for which CORE prepares a supplemental budget for the period of 2021 through 2024. These are constituted per 2020 and come in addition to the write-down per 2020 of intangible assets, such as ICANN application fees for gTLDs, whose valuation at cost until 2019 is no longer justified as a new gTLD round looms. The expected expenditure for further ICANN application fees, the disbursement of which will possibly take place as early as 2022, is provided for on the basis of the assumption that the fees have to be expensed, i.e. not carried as assets on the balance sheet. The provisions and write-downs are largely compensated by the capital gain resulting from the Donuts-Afilias merger in 2020.

In the course of 2020, CORE had already conducted negotiations, evaluations and planning for urgent changes and adaptations of its platforms, necessary for CORE's ability to provide the best possible service to its members, as well as influence practices of the Domain Name System in the interest of the public at large.

Moreover, as discussed below, the rationale of CORE's Afilias stake as a financial hedge has remained unchanged since CORE's first investment in Afilias, namely: the cost of CORE's public-interest efforts was likely to be proportional to growth in profits of a for-profit domain registry operator like Afilias Inc, and thus proportional to any increase in value of Afilias' shares.

CORE's approach remains unchanged in that it collaborates with stakeholders to develop viable reference platforms. These platforms are used to operate critical resources *in the public trust*. Overarching principles include open standards, adherence to best practices and fair competition.

1.2. Summary of the Proposed Provisions

The supplemental budget envelopes are:

Envelope	Provision in USD	Provision in CHF
Envelope 1: Security, Accountability and Privacy Enhancements of Registry Platform Expenditure required Adaptation of Registry Channel software to new needs with respect to Security, Accountability and Privacy. This involves the development of new infrastructure for Identity, Attestation and Proof based on the Domain Name System (DNS).	460,000	404,932
Envelope 2: Registration Channel Development Adaptation of Registrar Channel software with respect to the management of Registry pricing variation, and other administrative needs that were already identified back in 2020.	271,000	238,558
Envelope 3: Upcoming New gTLDs Processes Expenditure required related to the upcoming new gTLDs introduction processes due to regulatory and technology changes, funding of applications and potentially required objection proceedings and funding of public interest advocacy	1,450,000	1,276,416
Envelope 4: Community-based Content Ecosystem Pilot for dotSport Building on CORE's policy achievements for community-based internet extensions through the development of No-Tracking Content and Advertising Infrastructure which, contrary to existing advertising exchanges, does not convey personal identifiers of viewers.	85,000	74,824
Envelope 5: No-Trackers Ad-Exchange Pilot for dotSport The No-Tracking Content Alternative is an integrated data and protocol architecture for scalable content generation without relying on personal tracking of viewers.	140,000	123,240
Envelope 6: Transparency, Attestation and Public Access to Objective Information Extension of CORE's legacy whois service. Objective registration information is made available in the form of a service optimized for lookup of any domain name.	119,000	104,754
Envelope 7: Control of .whoswho TLD by CORE Counterbalance the negative effects of the longstanding decline and ultimate demise of the traditional Whois-based governance tools of the DNS by establishing the .whoswho TLD as a neutral and objective publishing tool, easy-to-use for lay users and experts alike, to support Security, Accountability, Privacy, Transparency and Public Access to Objective Information for the Internet Domain Name System.	360,000	316,903

	Total	2,885,000	2,539,628

Write-downs of intangible assets are separate from these provisions. The budget submitted for approval and provided-for in the accounts is a commitment for the respective total envelope amounts. The line items in each envelope and their work timelines may be adapted.

1.3. Role of CORE's Afilias Stake as a Financial Hedge

From 2007 to late December 2020, the assets of CORE Association included a residual stake in Afilias Inc of 16,808 shares. Originally created in 2000 for the purpose of launching the .info extension, Afilias was a for-profit US Delaware corporation operating domain registries. Its activities notably included the technical services of the .org extension, as well as many other extensions.

CORE was one of the founding shareholders of Afilias. CORE had maintained the Afilias stake as a financial hedge against the risk of extraordinary costs related to CORE's statutory obligation of protecting the public interest in the Internet Domain Name System. CORE's statutory purpose is to preserve and improve the Internet domain name system (DNS) as a critical resource in the public trust, by way of developing and operating reference platforms. The rationale of the hedge has remained unchanged since CORE's first investment in Afilias.

CORE's stake in Afilias was valued at the lower of cost or market value on CORE's books. CORE held 316,808 shares in Afilias from 2001 to 2007. In 2007, CORE sold 300,000 shares for USD 6,000,000 to other Afilias shareholders. The resulting capital gain was largely offset by special provisions for extraordinary expenses related to CORE's statutory public-interest purpose, in view of ICANN's planned expansion of the number of domain name extensions. These provisions were constituted per December 31, 2007, in line with a ruling by the tax office of the Canton of Geneva. The Internet Domain Name System was indeed expanded radically (albeit with many delays) and now includes 1000+ additional internet extensions.

On the basis of the 2007 provisions, CORE developed highly regarded reference platforms, both for the operation of community-based Internet Top-Level Domains and for the channel enabling registrars and Internet service providers to perform registrations. Community-based Internet extensions currently operated on CORE's platforms notably include ".swiss" (operated by CORE on behalf of the Swiss Confederation), ".radio" (operated by the Geneva-based European Broadcasting Union) and ".sport" (operated by CORE on behalf of the Lausanne-based Global Association of International Sports Federations).

Note: Although CORE has an international footprint with members and service providers in a number of countries, a significant portion of these expenses have ultimately funded the salaries of an average of 4.5 full-time equivalent staff members working in Geneva.

As already explained above, in late 2020 Afilias agreed to merge with Donuts, Inc (another Internet domain names registry operator). As a minority shareholder, CORE had no power to influence the merger decision. CORE received a merger consideration of USD 3.12 million on December 31, 2020 for its remaining shares. As a result of the merger, Afilias has ceased to exist as an independent company. Since the value of Afilias shares on CORE's books had been based on the original cost, almost the entire merger consideration constitutes a capital gain. As

such, in keeping with the original purpose of CORE's stake, it must be viewed in the context of a radical increase in the costs CORE faces to help protect the public-interest in the DNS.

2. Necessity of the Extraordinary Expenses

As said, CORE's obligation to implement the changes and adaptations presented in this document arises from CORE's own statutory purpose, which requires the maintenance of a structure through which the Registrars can cooperate. CORE is required to act in the interest of the current and future users of the Internet and, in particular, to preserve and develop the DNS as a public resource subject to the public trust (Art. 3 of CORE's Articles of Association).

Specifically, compared to 2007, when the pending enlargement of the top-level domain name space was the main factor to deal with, the current imperatives are largely related to fundamental changes in the role and trends of the DNS. These changes are:

1. A paradigm shift towards omnipresent personal tracking and targeting on the Internet driven by social networks and advertising exchanges;
2. A planned further expansion by ICANN, possibly by 2022, of the number of Internet extensions;
3. The advent of the European Union's General Data Protection Regulation (GDPR).

In the course of 2020, CORE conducted negotiations, evaluations and planning for urgent changes and adaptations of its platforms, necessary for CORE's ability to influence practices of the Domain Name System in the interest of the public at large.

2.1. Effects of ICANNs new planned expansion of the number of Internet extensions

ICANN has expanded the number of Internet extensions in several rounds. The previous rounds were conducted in 2000, 2004 and 2012. Over the past several years, ICANN's "Subsequent procedures for new gTLDs" Working Group has compiled recommendations for future expansions. On the basis of the Working Group's final report, it can be expected that the next gTLD expansion program will be initiated by 2023.

Even though CORE has invested vast resources in its registration platforms, the software platforms must be overhauled to address the needs associated with a new expansion. This is particularly critical in CORE's area of specialization, the community-based extensions (like .swiss, .sport, .radio, .cat, .barcelona, .paris, .scot, .gal) with strong policies, strong safeguards and strong security features.

2.2. Effects of GDPR and DSA combined with the Demise of the Whois Service

The traditional domain registration paradigm relied on the *publication* of data on the so-called Whois service as the principal mechanism of proof - such as proof of identity - and accountability. The paradigm dates back to 1985, an era when the publication of email

addresses and fax numbers was a viable form of documentation, and when very few people used the Internet. Over the years, this paradigm failed to be adapted: domain registrations are still based on little more than unverified assertions of whoever pays the domain name registration fee.

The European Union's General Data Protection Regulation[1] (GDPR) implies extraterritorial applicability and places strict limits on the collection and processing of personal data. However, the traditional domain name registration process not only lacks clear definitions and boundaries for personal data, but also depends on the publication of intimate contact information such as telephone numbers, email addresses and postal addresses. These can be replaced only on the basis of a redesign of the data model. Such a redesign requires the use of modern identity management tools.

As a result of the current measures to comply with GDPR, undertaken without reform of the data model, the scope and quality of data that is collected or published for domain registrations became inadequate to ensure security and accountability.

Most critically, the traditional domain registration paradigm was to accept unverified data, but to publish it. Thanks to publication of registration on what was called the Whois service, it became easier to correct if erroneous or out of date, and easier to discover if fake.

ICANN's current "temporary" specification for compliance with GDPR involves little more than simply redacting contact information from published domain name registration data. Modern identity management protocols - although already quite popular in conjunction with social networks - are not addressed, nor currently being much used for domain name registration.

The current approach in the DNS industry is to comply with GDPR without reform of registration practices and data model. As such, it does not even improve privacy. The deficiency of the domain name data model hampers privacy protection itself because it forces users to "voluntarily" supply even more sensitive data to unaccountable third parties.

The mere focus on hiding information in the current approach to GDPR compliance means that users' digital assets (such as domain names or contact records) have little value as a way to prove anything. But as identification and authentication is necessary, they are forced to provide their intimate identifiers (such as personal telephone numbers, social security numbers, or even fingerprint or face scans) to parties who have a legitimate reason to identify them, but no legitimate reason to hold such intimate identifiers.

In other words, strong and safe identity services are *key* to preserving privacy, because in their absence, users and service providers have no option but to rely on privacy-infringing practices.

ICANN's current data verification standards under the Whois Accuracy programs had already become almost meaningless for security in pre-GDPR times: email addresses, and even telephone numbers, can easily be created as throw-away resources by bad actors.

---

[1] https://eur-lex.europa.eu/eli/reg/2016/679/oj

The EU's new legislative initiatives Digital Services Act (DSA), Digital Markets Act (DMA) and the proposed NIS2 Directive[2] are also expected to require fundamental changes to CORE's systems. In particular, the NIS2 directive is likely to require verification of data.

In this context, CORE's statutory purpose calls for an initiative to restore viable access to verified and objective information about domain names, accessible to all Internet users. In doing so, the DNS industry can reverse the current race-to-the-bottom trend toward cheap, unverified, fast-rotating and insecure domain registrations.

2.3. Personal Tracking as a Factor in Domain Weaponization

Nowadays, content seen by users is increasingly personalized, either because it is delivered through social networks, or because it involves "sponsored links" (also called "clickbait").

As a result, the domain names usage paradigm has changed: rather than being visited at the initiative of users, domain names are sometimes used as projectiles. Or, as expressed in Internet jargon, traffic is "driven" to large sets of domain names.

Relying on artificial intelligence engines, online intermediaries can target each user selectively. Each user may be presented with different domain names because each user is pre-identified as receptive to a specific type of content.

At times this turns domain names into particularly dangerous instruments of fraud and disinformation. Domain names compound the power of personal targeting because:

- Domains used in personal-targeting-based attacks can be changed instantly and allow perpetrators to hide themselves.
- Domains used in personal-targeting-based attacks are outside of the responsibility and policy enforcement capability of the social network or advertising network used for targeting purposes.
- Many different domains can be used in tandem for a single attack.
- Malicious links are redirected immediately, and differently each time, based on the attackers' continuously updated assessment of a prospective victim's vulnerability.
- Security probes operated by law enforcement and specialized security companies can be outsmarted by sacrificing some attack domains. By the time an attack domain has been taken down, often because the attacker has deliberately sacrificed it, the attacker has gained strategic insights on how to circumvent defensive infrastructure.
- Attackers are organized on an industrial scale.
- Many domain-related crime networks offer sophisticated technical resources for online crime as no-questions-asked, remunerated services.

At the same time, users probably pay less attention to the domain name. Some users can be misled by visual appearance (e.g. logos), a problem exacerbated by the automatic displays of website thumbnails on most instant messaging and social media tools.

The personal targeting ecosystem, where bad actors may be difficult to distinguish from good actors, also allows domain names to be turned into get-away vehicles for any degree of deceit,

---

[2] https://ec.europa.eu/digital-single-market/en/news/proposal-directive-measures-high-common-level-cybersecurity-across-union

abuse and crime. While there are efforts by the domain name industry (registries and registrars) to combat domain name abuse, they remain largely futile so long as the traditional domain name registration paradigm, based on unverified assertions alone, is not strengthened with elements of formal proof.

CORE Association's statutory purpose is to preserve and improve the DNS in the public trust. It follows that CORE must develop its reference platforms to demonstrate the economic and practical viability of systems based on:

- verified accountability of domain holders,
- formally attested trustworthiness of domain names,
- sustainable advertising without personal tracking, and
- online identity services that protect personal data.

3. Expenses required for CORE to adapt its reference platforms

Envelope 1: Security, Accountability and Privacy Enhancements of Registry Platform

These are developments to expand CORE's Registry Platform in order to:
- Keep the system updated and according to ICANN Rules and industry standards;
- Respond to the current Security, Privacy and Accountability needs (as discussed in Section 2.3. above); and
- Respond to specific requests from CORE's TLD customers.

Scope for Envelope 1: Security, Accountability and Privacy Enhancements of Registry Platform	Work Timeline	Amount USD
Registry Subaccounts Fundamental revision of the TLD registry data model so as to achieve the ability for the registrars to optionally store the full registration channel information in the registry, combined with a separate ability for registrars to let their channel partners create, modify and delete their domain and other objects directly in the registry. Required because the inability to communicate with indirect registration channel partners constitutes a major barrier against the Security-Privacy-Accountability reforms. Currently needed to meet commitments to several TLD Operators for whom CORE provides technical services.	2021/2023	55,000
Trusted Notifier Support The ability to deliver alerts can no longer be based on the publication of contact data allowing anybody to send alerts, both for reasons of data privacy and because of the danger of abusive messages in the form of phishing and spam. The trusted notifier project permeates all systems and requires both a trusted notifier	2021/2022	15,000

registry and the ability for domain holders to appoint trusted notifiers.		
Registry Data Feed The traditional paradigm of the periphery-to-center information flow (from reseller to registrar to registry) is unable to handle an increasing number of tasks. As a way to avoid implementing separate protocols for each such case, the registry feed concept allows any one of a registrar's systems to subscribe to updates from the registry. Inasmuch as the registrar permissions a reseller's direct access to that reseller's Registry Subaccount, that reseller can then also subscribe to the updates for the reseller's object in the registry. One key objective is to enable multiple systems operating on behalf of a given registrar to be sure to receive all updates for the objects they handle, and to be able to get those updates directly from the registry. Related project: see Registrar Data Feed.	2021/2022	35,000
Backup Registry Services Provider Enhancement of Registry Feed capability to enable the real-time escrow in a separate registry system of different architecture. The separate registry system can subscribe to updates, retrieve part or all the objects, and retrieve the latest version or all versions of each object. In addition to receiving the data resulting from the update in the registry, the subscribing system receives a copy of the command that led to the update. This capability is critical to reduce risks inherent in migrations between software versions, to facilitate testing and to create a level playing field for fair competition between registry service providers.	2021/2022	40,000
Registration Client System Development The compatibility, usability and productivity of CORE's currently existing registration client systems - used among other things for registry flagship stores - are hampered by the absence of a registry data feed and a registrar data feed. Once these are in place, large portions of the current client systems need to be replaced with functions built on the data feeds. On this basis, the systems can be offered to CORE members and COREhub registration partners as a tool for interaction with their customers.	2021/2022	60,000
CDS/CDNSKEY Enhancement of DNSSEC provisioning on registry platform. CDS (Child DS Record) and CDNSKEY (Child DNSKEY Record) are alternatives to the provisioning mode currently used in CORE's registry platform. They have the advantage of making it easier for domain holders to rely on specialized DNSSEC name server providers who are not part of the registration channel. The objective is to cover all best-practice alternatives so as to diminish DNSSEC implementation barriers as much as possible.	2021/2022	30,000
Registry Lock Development of an advanced registry lock service in the registry software allowing authenticated personnel appointed by the domain holder to unlock and relock registry update or schedule updates for approval by the authenticated registrant-appointed	2021/2022	75,000

personnel.		
Federated Identity Services Modern identity agent and identity authority paradigm replacing the traditional paradigm of publishing identifying contact information, based on existing standards including ID4Me, OpenID Connect (OIDC) and OAuth2. This offers users a non-invasive alternative to the existing social login solutions like "Login with Google" or "Login with Facebook". Moreover, it can be used in combination with social login, allowing users to concurrently use, and switch between, multiple identity providers.	2020/2021	100,000
Telephone Number Authentication Service Component service needed for Registrant Authentication, Whois Accuracy	2021/2022	50,000
	Total USD	**460,000**

Envelope 2: Registration Channel Development

These are developments pending as of 31 December 2020 and aimed at enhancing and expanding CORE's Registrar Platform (GatewayNG):

- To keep the system updated and according to ICANN Rules and industry standards; and/or
- To better serve CORE's members and respond to their current needs.

Scope for Envelope 2: Registration Channel Development	Work Timeline	Amount USD
Multiprotocol access to via CORE's GatewayNG Since 1999, CORE has used its own protocol (currently Payload Version 2.0) to process provisioning commands from reselling members. As many members need to implement third-party software that uses EPP (Extensible Provisioning Protocol), CORE will implement EPP as a concurrently available alternative to Payload Version 2.0. This multiprotocol paradigm has been used in the past for registry platform software and will be implemented in CORE's registrar channel software.	2021/2022	70,000
Focus Shield Service Rebranding reverse proxy service / web cache service. In addition to the security shield and scalability benefits of existing reverse proxy caching, enables existing content management systems based on a single legacy-domain name to be operated in the background and direct visibility to a shield of new purpose-specific URLs with well-adapted domain names. Extension of current proof-of-concept project developed for .sport. Subprojects include: (i) Docker-based containerization for	2018/2021	50,000

high scalability, (ii) Standardization of site management data, (iii) Publication of code as open-source		
Duplicate payment transaction numbers checking Internal control mechanism that involves checking input to avoid the same bank transaction number being recorded twice, which could only be the result of an error.	2020/2021	1,500
Support for the command member.domains Function for members to obtain partial or full listings of their domain portfolio in machine-to-machine interactions based on an API command.	2020/2021	4,500
Transfer process action "domain acceptance" for Nominet (co.uk) Compatibility with push domain transfer paradigm used by Nominet for .uk domains	2020/2021	3,000
Integration of booking entries for ICANN fees Automatic booking entry generation for fees paid to ICANN, avoiding the use of a large number of individual microbilling transactions with penny amounts as these would make it difficult for members and staff to reconcile their accounts.	2020/2021	4,500
Dynamic announcements on dashboard Use of the control panel dashboard for important announcements. Addition of browser-based notification subscriptions available to control panel users.	2020/2021	6,000
Client Type "Internal" and "Agent" Extension of fundamental data model to support multiple principals on the same system.	2020/2021	3,000
Tariff Management Stage 1: internalAmount variable Extension of the automated billing function to reduce the number of billing rules	2020/2021	15,000
Tariff Management Stage 2: extended formula logic Extension of the automated billing function to allow a single formula to be used as a default for many different products. Is a prerequisite for future member-to-reseller account keeping services.	2020/2021	40,000
Running Balance Columns Enhanced security by way of a correction of the data model to ensure all transactions have an audit trail with running balances. Where such running balances are missing, and where possible, reverse calculation of past balances is used.	2020/2021	3,000
Dedicated original pricing columns Data model improvement needed to support statistical, accounting and controlling functions.	2020/2021	5,000
Price limit checking Enhancement of the price limit checking mechanism so as to provide better flexibility, higher security and less transaction failures due to non-significant price limit overruns.	2020/2021	2,000

Transaction information sent to external systems Revision of communications paradigm to dependent systems of processes to ensure that they have access to the original transaction amount in original currency before tax, irrespective of automatic currency conversion and automatic application of tax.	2020/2021	3,000
Audit Report improvements Enhancement of audit reports generated by the gateway for audit, controlling, error discovery and account reconciliation purposes.	2020/2021	10,000
Control Panel improvements (search, links, copy) Extensive usability improvements on control panel to support multi-object search, link to related information and copy-paste behaviour for data interchange with popular office automation software such as spreadsheets and word processors.	2020/2021	15,000
GatewayNG Overall Result Reports (internal invoicing) Statistical tool used to calculate aggregate effect of past charges and estimate aggregate future charges.	2020/2021	20,000
Store all non-zero account balances in book entry Adaptation of the running balance audit trail to the multi-currency paradigm.	2020/2021	10,000
Original amount and currency in CSV export Update to data export features to report original transaction data in addition to applied transaction data.	2020/2021	1,000
Implementation of "isSettlement" flag for accounting actions Update to data model to introduce systematic distinction between billing (charges and refunds) and settlement (deposits and withdrawals) on the basis of an explicitly recorded property. Needed to prevent erroneous processing as a result of unclear terminology when user action of system behaviour is dependent on the naming of transactions.	2020/2021	1,500
Support for maintenance announcements via EPP Implementation of a new EPP command / EPP extension for maintenance announcements.	2020/2021	3,000
	Total USD	**271,000**

Envelope 3: Upcoming New gTLDs Processes

CORE's business is managing Top Level Domains (TLDs). It currently manages three TLDs of its own and 15+ TLDs of its customers (like .sport, .radio, .eus, .cat, .swiss, .seat, .barcelona, .madrid, etc). TLDs cannot be freely created at any time but only when ICANN - the regulatory oversight entity- opens a so-called "new applications window". There was one window in 2000, another one in 2004 and a third one in 2012.

In 2012 CORE submitted 3 applications of its own, all of them for Internationalized Domain Names (that is, TLDs in non-latin scripts). It is evident that non latin scripts have faced multiple technical usability challenges that have prevented them from developing as expected. Back in 2020 CORE's Executive Committee agreed that CORE must submit in the next round at least the same number of TLD applications in latin script.

Additionally, CORE specializes in supporting Community-based applications which are often managed by non-for-profit entities which have limited or no access to capital markets. As it happened in 2012 for dotSport, CORE needs to be prepared to fund at least a couple of such TLD applications (and recover those funds afterwards in managing the TLD).

In 23 September 2020, after 6 years of deliberations, the ICANN GNSO "New gTLD Subsequent Procedures" Policy Development Process working group, concerned with policy for the further introduction of new generic top-level domains, issued a **Draft Final Report,** with the required public comment period on such draft report starting on December 22, 2020. In January 2021 a 400-page Final Report[3] was issued.

Although the timeline remains highly uncertain, it is possible that a new application process may begin by 2022. Note that in order to submit any application, a mandatory up-front "evaluation fee" must be paid to ICANN. While the Application Fee amount for the next round is not yet fixed, it is expected to be somewhere between USD 150,000 and 175,000 per TLD application.

This means that in line with its statutory purpose, CORE must devote staff resources to community and public-interest advocacy by way of participation in the ICANN working groups concerned with the policy implementation, and that CORE must re-create a TLD Introduction Support capability as it did previously in 2000, again in 2004, and from 2008 through 2012. As can easily be appreciated from reading the Final Report, the complexity of the process has further increased. The public-interest stakes, and those for affected communities have further increased.

As was the case for the 2012 round of new gTLDs, CORE's role may also include the preparation of defensive TLD applications, the filing of Community Priority Evaluation requests, and the filing of objections proceedings[4].

Scope for Envelope 3: Upcoming New gTLDs Processes	Work Timeline	Amount USD
Community and Public Interest Advocacy in ICANN regarding new gTLDs While ICANN's multi-stakeholder process is an important assurance of stability and inclusion, it is also potentially subject to overrepresentation of narrow interests that may be in conflict with those of communities and with the public interest. This is particularly acute in the context of processes governing the	2020-2023	100,000

---

[3] https://gnso.icann.org/sites/default/files/file/field-file-attach/final-report-newgtld-subsequent-procedures-pdp-02feb21-en.pdf
[4] In the context of ICANN's 2012 new gTLD round, CORE prepared, and was instrumental in helping the respective community organizations prevail in, two community objections proceedings (.sport/.sports), one string confusion objection proceeding (.sport/.sports), one Community Priority Evaluation Proceeding (.radio) and one originally defensive TLD application (.swiss).

introduction of new generic top-level domains (new gTLDs). CORE's advocacy of the public interest and of community interest in the ICANN process has been critical in the past and requires funding for the active role of CORE's delegates. Two awareness programs, named "Mind the Internet" and "Mind the Domain" respectively, are part of the advocacy drive and benefit from visibility CORE endeavors to achieve via the Public Access to Objective Information projects. The "Mind the Internet" outreach program is designed to raise awareness among domain holders about safe domain registration practices; the "Mind the Domain" reaches out to Internet users at large to provide information about safe navigation and how to check domain names for trustworthiness.		
Outreach and preparation of informational material Includes online information material, online events and sponsorship of ICANN meetings as well as related events. May include expo material as and when in-person ICANN meetings are phased in again.	2020-2023	100,000
Post-2012-Round new gTLD Application fees Based on an expected application fee of USD 175,000 and an expected need to submit or fund 5 TLD applications. Applications may be needed in defense of existing community-based TLDs or existing needs. As the applications are unlikely to constitute assets with market value, the prudent assumption is that the application fees must be expensed once committed.	2022 or later	875,000
Post-2012-Round Objection Proceedings and Defensive Applications Potential need to file Objection Proceedings against speculative gTLD applications in defense of affected communities or the public interest. Estimate is based on the hypothesis that 2 arbitration proceedings must be initiated with an expected cost of USD 50,000 per proceeding. By comparison, 3 objection proceedings were necessary for .sport in 2012/2013. This item also provides for the likely need of one purely defensive TLD application (the application fees considered under new gTLD Application fees item involve defensive considerations as secondary motives for action).	2022 or later	275,000
Technical and process changes resulting from new ICANN requirements published in 2020 Significant change requirements and expenses result from the widely expected security-related recommendations of ICANN's Second Security, Stability, and Resiliency (SSR2) Review Team Final Report published in January 2021 (preliminary reports were published earlier). Some of these governance and process requirements arise from recent technological changes, such as DNS over HTTPS (DoH).	2021-2023	100,000
	Total USD	**1,450,000**

Envelope 4: Community-based Content Ecosystem Pilot for dotSport

The cost of setting up a website is still prohibitive for most users. By comparison, the initial cost of setting up social media accounts is negligible, but the holder of such an account must allow personal tracking of all visitors to their content. The No-Tracking Content Alternative is an integrated data and protocol architecture for scalable content generation without relying on personal tracking of viewers. CORE has built the first elements over 2019-2020 in the form of the web-reflector and athlete programs for the .sport TLD. The .sport extension is based on a strong community-based registration policy and is operated by the international sport federations' umbrella organization GAISF.

CORE provides technical services for .sport. In doing so, CORE is working with GAISF and other organizations recognized by the International Olympic Committee. The existence of a strong, community-based governance mode anchored in the long-established institutions makes the .sport extension an ideal environment to prove the economic viability of a sustainable approach to highly-scalable content provision.

Scope for Envelope 4: Community-based Content Ecosystem Pilot for dotSport	Work Timeline	Amount USD
Athlete.sport program Specification of terms and definitions of registry interactions for athlete-owned domain names benefitting from preferential terms for athletes and teams of athletes. While all sport practitioners are eligible as athletes under this program regardless of affiliation with any federation, the program's objectives also include a design that facilitates interaction with, and benefits offered through, international sports federations as well as their national federations and their clubs. One key use case is the ability of federations to carry personal athlete pages on their own web site infrastructure, by displaying the respective athlete's page under the athlete's own domain name.	2020-2022	20,000
My.sport Integrated Reference Platform The development of my.sport as a reference content management platform began in 2019 as a proof-of-concept project to identify the best approach to achieving an integrated user experience while maintaining portability and free choice of service providers at all levels. One key objective of the My.sport platform is to encourage development by third-party developers of their own platforms, so as to foster an ecosystem bringing innovation and choice to athletes and their communities.	2019-2023	25,000

Sport Widget API Specification The Sport Widget API Specification will define visual objects that can be displayed on athletes' web pages at the discretion of the respective athlete, without requiring any development specific to a given widget on the content management platform. The widgets are designed to automatically update content selected by the athlete and can be operated on a commercial basis or on a community service basis. The widgets are thus intrinsically portable and can be maintained by an athlete even after changing service providers in charge of domain, hosting or content management. In particular, the specification is based on a no-tracker policy: the provider will get statistical information as well as information about the sport-related credentials of the host of the page, but will not get any data allowing the identification of the page visitors.	2020-2021	15,000
Web Reflector Platform for International Sports Federations First instance developed in 2018/2019 providing content for proactively-registered domain names covering international federations' sports disciplines vocabulary in 30 languages. The platform requires further development for improved linkage with athlete pages, improved linkage to governing bodies and improved content in the various languages. For this purpose, the existing multi-language / multi-author content management system of the Web Reflector Platform is to be enhanced with a framework allowing delegation of authoring capability to representatives of national sports federations. The development will continue to focus on integration with Wikipedia.	2018-2022	25,000
	Total USD	**85,000**

Envelope 5: No-Trackers Ad-Exchange Pilot for dotSport

The development of a No-Tracking Content+Ad Exchange is arguably the most significant and far reaching effort undertaken by CORE. Ad Exchanges (advertising exchanges) have existed for over 20 years on the Internet. On an ad exchange, instant auctions are held each time a user visits a web page or scrolls to a new item on a smartphone app.

Most ad auctions are based on the identification of the viewer. Typical advertising engines effectively require the betrayal of the identity of the viewer, and the disclosure of information about the viewer, including the viewer's browsing history, to invisible and unaccountable market participants.

Once transmitted, this information cannot be taken back and will be merged with other data obtained by such actors. One ultimate effect is that originally anonymized personal information can be de-anonymized by hidden actors, while the parties visible to the user are shielded from liability.

The purpose of this envelope is to demonstrate the financial viability of an advertising that avoids the personal targeting paradigm altogether and is strictly based on the context of the content. The project name is "Strictly-by-Context AdEx".

As of 2020, most Internet advertising is based on instant auctions of individual ad impressions. However, virtually all of these require the highly intrusive personal tracking of page visitors. As such, they are potentially unsustainable for page hosts, page visitors and advertisers alike: page hosts are forced into a conflict of interest with respect to their visitors; page viewers are potentially exposed to malicious targeting as the personal tracking data leaks out to bad actors and cannot be reliably anonymized. Advertisers face the dilemma of seeing their own marketing intelligence sold to their competitors by their advertising intermediaries.

This situation calls for the creation of a reference no-trackers ad exchange based solely on contextual data supplied by the page host. Because no personal data or identifiers at all are supplied to the advertising exchange, it is intrinsically sustainable and economically sound for media, advertisers and intermediaries.

Scope for Envelope 5: No-Trackers Ad-Exchange Pilot for dotSport	Work Timeline	Amount USD
No-Tracking Ad-Exchange API Specification Definition of the messages exchanged between the web pages and the Ad Exchange	2021-2022	25,000
No-Tracking Ad-Exchange Combo Widget Specification Definition of link between content widgets whose provision is funded by ad revenue, and the corresponding ad widget displayed on the same page.	2021-2022	25,000
Reference implementation Server Side Implementation of the API on the Ad Exchange server side. The my.sport platform will link to this end point; other platforms can link to it too.	2021-2022	30,000
Reference implementation Host and Viewer Side Implementation of user configuration tools allowing the selection and activation of ads by the athlete on my.sport, as well as display of the ads based on interaction with the Ad exchange.	2021-2023	25,000
Reference implementation Advertiser/Sponsor Side Implementation of the advertiser/sponsor-facing configuration and management resources	2022-2023	35,000
	Total USD	**140,000**

Envelope 6: Transparency, Attestation and Public Access to Objective Information

In order to support transparency and attestation of trustworthiness, users with or without technical knowledge must be able to check domain registrations. Recent developments, such as the replacement of the Port-43 Whois Protocol with RDAP and GDPR have made it more

difficult for lay users to obtain information. The repurposing of the existing .whoswho extension allows users to obtain information on any browser, using a simple URL.

Scope for Envelope 6: Transparency, Attestation and Public Access to Objective Information	Work Timeline	Amount USD
Control and governance of .whoswho extension Moved from Envelope 6 to become sole item of Envelope 7, following up on feedback provided in the Extraordinary Plenary of June 21, 2021. As a result of this change, Envelope 6 is reduced by USD 360,000, which is the same as the total amount of Envelope 7.	See Envelope 7	0
DNSSEC Systematic use of DNSSEC for all zones based on <tld>.whoswho . In the event that .whoswho cannot be used, a substitute suffix, such as ".core.info", is used instead.	(base services completed as of 2020)	1,000
DNS Record Lookup Ability to look up DNS records directly from the .whoswho lookup. Basic functionality has already been implemented; required additions include subdomain DNS queries, the inclusion of the query parameters in the short URL, follow-on links to syntax and integrity verification sites. In the event that .whoswho cannot be used, a substitute suffix, such as ".core.info", is used instead.	2020	1,000
Downloadable Snapshot Report Tool Ability for viewers to download a WhosWho Domain Data Snapshot. Intended in particular for use by legal and IP communities. In the event that .whoswho cannot be used, a substitute suffix, such as ".core.info", is used instead.	2023	9,000
Wildcard certificates per *.tld.whoswho Required to avoid the potential unexpected display of an error message. Users should be able to simply add ".whoswho" at the end of any domain name in a URL starting with "https://". In order to ensure that each URL composed of a domain name plus the suffix ".whoswho" will work with HTTPS, wildcard certificates are necessary. (In the absence of such HTTPS support, when the URL is called using the "https://", the browser displays an error message instead of the web page.) Bi-monthly renewal of free Let's Encrypt or similar wildcard certificates requires an automated authentication infrastructure that must be purpose-built for the .whoswho project. In the event that .whoswho cannot be used, a substitute suffix, such as ".core.info", is used instead.	2021	5,000

RDAP retrieval and display RDAP is the newly standardized protocol replacing the traditional Port-43 Whois protocol. It is mandatory for all gTLDs, though not for ccTLDs. As RDAP is based on HTTP, it can be retrieved by the user's browser directly from the original source (i.e. the registry and/or the registrar). The proof-of-concept has been working since Q2 2020 with consistently high response speed and availability. Remaining work involves developing a more user-friendly basic layout of RDAP information. One key focus for improvement is the unambiguous highlighting of the published registrant (domain holder) information in a way that lay users can understand as reflecting ownership and accountability. In the event that .whoswho cannot be used, a substitute suffix, such as ".core.info", is used instead.	(retrieval and basic display completed as of 2020) 2021	5,000
Whois retrieval The proof-of-concept version in operation since Q2 2020 automatically displays Port-43 Whois where available. Layout and readability improvements are still needed, as are outreach efforts to ccTLD registries that do not offer RDAP. In the event that .whoswho cannot be used, a substitute suffix, such as ".core.info", is used instead.	(completed as of 2020)	2,000
Platform scalability based on containers (Docker) The proof-of-concept version is based on minimal resources in the form of traditional web servers. In order to achieve scalability or higher rates of usage, the container model is ultimately the most cost-effective solution.The same model can be applied to other projects. In the event that .whoswho cannot be used, a substitute suffix, such as ".core.info", is used instead.	2022	5,000
Multi-domain lookup in a single short URL Multi-domain lookup syntax based on the example tokyo2021.sport.whoswho/..com..org..tokyo2020.com In the event that .whoswho cannot be used, a substitute suffix, such as ".core.info", is used instead.	2021-2023	4,000
Channel-constrained advertising engine Channel-constrained advertising engine, used to advertise services of participating registrars and resellers (including CORE members and partners) and on the data display about domains under management by those registrars. If a domain is sponsored by a non-participating provider, the advertising space is used for CORE's public-interest awareness campaigns "Mind the Internet" and "Mind the Domain", designed to raise domain holder awareness for best practices and end-user awareness and educational resources for safe Internet browsing. In the event that .whoswho cannot be used, a substitute suffix, such as ".core.info", is used instead.	2021-2023	4,000
Public-interest campaign on checking domain veracity and accountability Public-interest campaign on checking domain veracity and accountability In the event that .whoswho cannot be used, a substitute suffix, such as ".core.info", is used instead.	2021-2023	4,000

TLD properties data sheets under <tld>.whoswho CORE has an extensive database with detailed information about the properties of TLD. A significant part of that data - such as TLD's particular logic of expiration or transfer policies, its eligibility and nexus requirements or any special registration data collected or published by the respective registry - is of interest to the public at large. The data is to be displayed along with the IANA data currently shown and can later be combined with data standardized computer and human-readable policy data published by the registry as and when such standards come into existence. In the event that .whoswho cannot be used, a substitute suffix, such as ".core.info", is used instead.	2021-2023	4,000
TLD rating Development of an objective methodology for a TLD (or public suffix) rating visible to the public at large, reflecting the protection internet users can expect from the security policies of the respective registry. The rating and the methodology can then be added to the <tld>.whoswho pages. One key objective of this effort is to create an environment in which registries have an incentive to go beyond paying lip service to security and invest in genuine trust-enhancing practices.	2021-2023	10,000
Domain security rating Development of an objective methodology for a domain rating visible to the public at large. Contrary to the TLD or public suffix rating, it reflects the properties of an individual registered domain.	2022-2023	4,000
Domain abuse complaint mechanism Ability for users to go directly to existing complaints submission tools and have relevant information automatically prepared. Needed as very few lay users understand how to submit complaints for fraudulent domains. In the event that .whoswho cannot be used, a substitute suffix, such as ".core.info", is used instead.	2021-2023	4,000
Domain abuse lookup via existing blacklists and security checking tools Domain abuse lookup via existing blacklists In the event that .whoswho cannot be used, a substitute suffix, such as ".core.info", is used instead.	2021-2023	4,000
Trademark Clearinghouse voluntary record publication Enabling holders of trademark clearing house records to have their SMD strings published under <string>.tmch.whoswho . To obtain publication, the holder of a the SMD file submits a registration for a virtual domain in the format yyyy-mm-dd.<string>.tmch.whoswho , where yyyy-mm-dd is the validity start date of the SMD file. If more than one SMD holder has a record for the same string, all are listed on the URL <string>.tmch.whoswho . Where possible, as a convenience, <string>.whoswho redirects to <string>.tmch.whoswho . If the SMD record is combined with a TMCH Trademark Registry Exchange (TREx) record, that information can be carried at the	2021-2023	5,000

discretion of the respective trademark holder. In the event that .whoswho cannot be used, a substitute suffix, such as ".core.info", is used instead.		
Domain Attestation Framework (DAF) White Paper White paper to propose a standardized syntax for assertions made via DNS zone files. One of its purposes is to serve as a foundation for the Optional Attestation Frameworks for Authorization, Accountability, Endorsement and Trustworthiness. As the syntax has many possible future applications, expert advice and involvement are needed for the design of the syntax.	2021-2023	30,000
Domain Attestation Framework (DAF) Standardization Effort Funding for expert authoring of draft standard documents	2021-2023	9,000
Verified Link to Legal Entity Identifier (LEI) The Legal Entity Identifier (LEI) is a 20-character, alpha-numeric code based on the ISO 17442 standard developed by the International Organization for Standardization (ISO). Issuers of LEIs are accredited by the Global Legal Entity Identifier Foundation (GLEIF, see https://gleif.org). The Verified LEI Link Project will enable LEI holders to link their domains to their LEI and show the link, as well as proof of its veracity, to the public. In the event that .whoswho cannot be used, a substitute suffix, such as ".core.info", is used instead.	2021-2023	9,000
	Total USD	**119,000**

Envelope 7: Control of .whoswho TLD by CORE

The purpose of the Domain Lookup by .who**s**who Project is to help rebuild the foundations of transparency and trust that characterized the early DNS but were lost due to growth of the Internet. A proof-of-concept installation has been available since mid 2020 based on informal cooperation between CORE and the .whoswho registry.

The .whoswho service allows any Internet user to find the official registration information about a domain name by simply adding ".whoswho" after the domain name, using a normal Internet browser. For instance, by typing *eurovision.tv*.whoswho, or *who.int*.whoswho, the user can find information about eurovision.tv or who.int . As such, the .whoswho service already allows the lookup of hundreds of million domain names. Along with registration information, the tool also provides useful DNS configuration information, such as whether and how a mail server or a web server have been associated with the domain. In the near term, this will be expanded to provide information presented in a clear way a lay user can understand, combined with access to more advanced information for use by expert users.

The service also provides information about internet extensions. For instance, by typing sport.whoswho, or swiss.whoswho or com.whoswho, etc., the user can find information about .sport or .swiss or .com, etc. In the near term, this will be expanded with objective information about Internet extension (such as the registry's eligibility policy or domain holder identification policy). The simple lookup paradigm as a whole can easily become part of the public's habits

under the name "**domain.whoswho**" (with matching public educational and outreach material available on that domain).

The .whoswho lookup is needed to help ordinary users check if they can trust the sites they visit. They currently have no credible way to do so. Furthermore, it is practical for lay users and experts alike. It also fills a new void caused by RDAP (RFC 7483 published in 2016). RDAP replaces the old Whois protocol (RFC 812 published in 1982). But the Whois was built for man-to-machine interaction, while RDAP is a machine-to-machine protocol. *Contrary to a Whois server, an RDAP server has no control over the presentation of the information seen by the user. It cannot even control which elements of the information are displayed at all. Most websites displaying RDAP information hide the bulk of the information supplied - ICANN's own lookup.icann.org being one such example. This also blocks specialized types of information - for instance, a validation status flag as used in .swiss. Such items will not be displayed unless the user's viewing tool has been expressly configured to display them.*

The Port-43 Whois, combined with best practices and ICANN rules, was de-facto both a presentation standard and a transmission standard. RDAP is only a transmission standard. Therefore, one central role of the .whoswho lookup is to create and continuously improve a presentation standard for registration information. Additional information is key for registries or registrars that certify the trustworthiness of domains. The .whoswho TLD is thus a means of making that certification publicly visible in a way that a typical Internet user can understand.

Running the .whoswho lookup as a neutral service lies at the center of CORE's statutory purpose of improving the DNS as a critical resource held in the public trust. The visibility created through the project is a means of action for all the other activities of CORE, be it the neutral COREhub registrar, the GatewayNG registration channel platform, the Tango registry system, or the specialized purposes and strong policies of community-based internet extensions for which CORE provides technical services (.cat, .swiss, .sport, .radio, etc.)

Scope for Envelope 7: Control of .whoswho TLD by CORE	Work Timeline	Amount USD
Control and governance of .whoswho extension Cost of obtaining the assignment of the .whoswho registry agreement to CORE. Negotiations with the current operator of .whoswho were conducted in 2020 subject to ratification in accordance with CORE's Articles of Association and due diligence review by CORE staff. If the .whoswho TLD is available and controlled by CORE as a neutral entity dedicated to serving the interests of the Internet Community at large, a plurality of items in Envelopes 1-6, in particular those related directly or indirectly to public access to objective information, can be achieved in a way that is easy to be shared, remembered and understood by, virtually all levels of Internet literacy of Internet users. A contrario, in the absence of an ability to use the .whoswho TLD to overcome current challenges related to access and usability of objective public information on domain names, these projects, while still viable and useful, have their public benefit potential reduced by an aggregate margin that largely outweighs the cost of obtaining the assignment of	2020 (if ratified)	360,000

the .whoswho registry agreement to CORE Association.		
	Total USD	**360,000**

Note: Envelope 7 has been constituted separately as a follow-up to feedback from the Extraordinary Plenary of June 21, 2021. The purpose of this change is to adjust the granularity of the budget decision-making process and enable CORE members to express focused mandates for action. It is important to keep in mind, however, that all the envelopes are intrinsically linked and that the effort defined in each envelope benefits from those of the other envelopes.

This is particularly relevant in the case of the newly separate Envelope 7. Thanks to the use of the .whoswho TLD to construct lookup strings, the branding of the lookup is more neutral, more purpose-specific, more memorable, easier to understand and easier to use for the lay user than any other approach.

Furthermore, the domain.whoswho project goes a long way toward outreach and promotion of the values of CORE Association.

The channel-constrained advertising engine (see Envelope 6) acquires considerable practical advantages for participating providers if the lookup URLs are neutrally branded as ".whoswho". Participants can display their logo and corporate service motto in conjunction with registration objects they handle on behalf of their customers. The list of project participants automatically includes CORE members and partners. The branding in .whoswho thus increases the appeal to new project participants from outside of CORE Association while supporting the interest of the membership, in a process that is open, fair, reasonable and non-discriminatory to CORE members and non-members alike. This enables CORE to welcome new members and to serve the shared interests of CORE's membership.

Finally, future extensions of the proposed online attestation and corroboration paradigms benefit from the available operation of a lookup string as a domain name because DNS pointers can emanate from them. This facilitates instant machine-based analysis, including the computation of domain trustability graphs, while ensuring that the same information can easily be read by humans.