New gTLD Program
Explanatory Memorandum

A Model for a High Security Zone Verification Program

Date of Publication: 2 October 2009

Background - New gTLD Program

Since ICANN was founded ten years ago as a not-for-profit, multi-stakeholder organization dedicated to coordinating the Internet's addressing system, one of its foundational principles, recognized by the United States and other governments, has been to promote competition in the domain-name marketplace while ensuring Internet security and stability. The expansion of the generic top-level domains (gTLDs) will allow for more innovation, choice and change to the Internet's addressing system, now represented by 21 gTLDs.

The decision to introduce new gTLDs followed a detailed and lengthy consultation process with all constituencies of the global Internet community represented by a wide variety of stakeholders – governments, individuals, civil society, business and intellectual property constituencies, and the technology community. Also contributing were ICANN's Governmental Advisory Committee (GAC), At-Large Advisory Committee (ALAC), Country Code Names Supporting Organization (ccNSO), and Security and Stability Advisory Committee (SSAC). The consultation process resulted in a policy on the introduction of New gTLDs completed by the Generic Names Supporting Organization (GNSO) in 2007, and adopted by ICANN's Board in June, 2008. The program is expected to launch in calendar year 2010.

This explanatory memorandum is part of a series of documents published by ICANN to assist the global Internet community in understanding the requirements and processes presented in the Applicant Guidebook, currently in draft form. Since late 2008, ICANN staff has been sharing the program development progress with the Internet community through a series of public comment fora on the applicant guidebook drafts and supporting documents. To date, there have been over 250 consultation days on critical program materials. The comments received continue to be carefully evaluated and used to further refine the program and inform development of the final version of the Applicant Guidebook.

For current information, timelines and activities related to the New gTLD Program, please go to http://www.icann.org/en/topics/new-gtld-program.htm.

Please note that this is a discussion draft only. Potential applicants should not rely on any of the proposed details of the new gTLD program as the program remains subject to further consultation and revision.

Table of Contents

1. Executive Summary

1.1 Purpose

This draft *concept paper* introduces the concept for a program that is designed to provide a structured approach to improve internet community trust and to improve the overall security of the domains registered within TLDs that volunteer to participate in the program. In its current state, the document is in "strawman" format, which means that it provides a framework that describes a voluntary high security zone program for Registrars wishing to self-identify as a "high-security" TLD. This document is based on input from ICANN stakeholders that was gathered during the feedback process for the establishment of new TLDs, as well as examination of other certification-type programs. It includes input from internationally recognized control and certification standards such as the AICPA/CICA Trust Services and the ISO/IEC 27000 series. The paper is intended to solicit community feedback related to the utility and features of such a High Security Zone Program. Based on community input, ICANN believes this concept should be considered. As a next step, a multi-stakeholder working group will be initiated that will be tasked with establishing a proposed implementation plan, with the intent to build a fully functional program. For further information on the working group, please refer to section 3.1 Governance below.

1.2 Overview

For the purpose of this concept paper, the High Security Zone Verification Program ("Security Verification Program") or ("Program") has one level. The benefit of Security Verification is that it allows for an enhanced level of trust for the Internet users within a Security Designated TLD. Trust is established by allowing TLD Internet users to see, *through an appropriate seal*, that a Security Designated TLD has achieved "Security Verification". By achieving Security Verification, the TLD will have demonstrated that it has implemented the required control environment defined by this Program, and that the required controls were operating effectively during a period of review. The Security Verification Program will require the Registry to both implement controls and to undergo an audit per the requirements of this Program. The balance between benefit (enhanced trust) and cost constitutes the key business decision that a TLD registry will use as the basis to determine if Security Verification is an appropriate business process to pursue.

Security Verification: Security Verification provides an enhanced level of trust and security over the baseline that gTLD registries are nominally expected to provide when standard contractual provisions are met. The processes required to achieve Security Verification can greatly increase the trust level for all consumers of information within the TLD. It includes verification of Registry operations and supporting Registrar operations. It also builds upon the assumption that Registrars will be required to perform procedures to authenticate the accuracy of Registrant information at the time of domain registration. This further assumes that (a) the Registries will be able to select through objective criteria, the Registrars that they do business with to those Registrars whose operations maintain an appropriate control structure from Registry to Registrant and that (b) Registries will structure their Registrar contracts to require implementation of specific controls required by the Program. The controls necessary to support Security Verification would also be assessed through an independent audit by an approved 3rd party. The audits will occur on a periodic basis, to prove that the controls in place at the Registry operator and its contracted Registrars are continuing to operate effectively. Results of the audits will be

provided for final review. This allows issue of a public assertion (i.e., a *seal*) that the designated TLD operator was indeed operating with the necessary enhanced security controls required to achieve Security Verification.

1.3 Scope

The Security Verification Program applies to a proposed set of activities necessary to support an enhanced level of Internet user trust for Registry and Registrar operations for a Security Designated TLD. The draft framework focuses on the controls necessary to reduce the potential for malicious conduct, including fraud and other criminal activities, for Registries that elect to pursue proof of Security Verification. Other considerations, such as controls to address intellectual property concerns, could be added as components for future consideration in the lifecycle of the program. This document provides potential draft requirements to achieve Security Verification including criteria topics, but does not endeavor to be comprehensive in scope nor is it intended to address detailed implementation of each criteria topic at this time.

The scope is limited to the internal controls ("controls")[1] and activities at the Registry and Registrar operations level. The Security Verification Program is intended to provide reasonable, but not absolute, assurance that the designated TLDs have implemented effective operating controls to meet the Security Verification Program criteria. The combination of clearly defined program criteria and periodic independent reviews/audits of their effectiveness will therefore provide an increased and persistent level of trust. It should also be noted that controls and activities involve human action, which can introduce possible errors in processing or judgment. In addition, controls and activities can potentially be overridden by collusion among actors or coercion by management. Because the effectiveness of specific controls is subject to these inherent limitations, errors or fraud may occur and not be detected by the Security Verification Program. We hope to minimize the number of such instances through aggressive compliance oversight of designated TLDs. Due to the risks involved measures will be needed to limit liability to ICANN. If established, ensuring public awareness of the limitations of the program in terms of not providing guarantees about the presence of malicious activity within a TLD must also be addressed.

2. Positioning

2.1 Business Opportunity

The introduction of a new Security Verification Program provides a significant opportunity for TLD Registries to demonstrate the effectiveness of their controls to stakeholders, and to establish an enhanced level of trust for certain Registrants, by covering Registrar operations where vetting/authentication of Registrant data is required. Security Verification represents a business opportunity for TLD Registries and associated Registrars that desire to establish an enhanced trust model for the domains within their TLD. The overall concept is to provide a business benefit for their Registrants. This Security Verification is likely to be an attractive option for TLDs:

[1] A process effected by an organization's structure, work and authority flows, people and management information systems, designed to help the organization accomplish specific goals or objectives.

- Who's business model would benefit from increased trust and control; and/or
- Have regulatory pressure or requirements for enhanced trust and control.

Expansion of the DNS namespace to include new TLDs also presents an opportunity to enhance the security, stability, and resiliency of the domain name system. It is important to keep in mind that TLDs are simply namespaces; in and of themselves, a namespace presents limited value beyond the inherent marketing oriented value in the string itself. However, when a namespace administrator manages a TLD as a policy domain with specific admission and operational standards, the resulting namespace may exhibit improved SSR characteristics over time. This value will be promoted through a voluntary certification program for TLDs that allows the Registry operator to assert unique aspects of its policy domain including admission policy and operational standards.

A TLD that elects to go through the Security Verification Program may result in a namespace with valuable properties:

- *Operated by a reputable organization or designated representative of the TLD string.* This business level assurance or recognition should prove beneficial when the DNS or security community calls upon the Registry operator to assist in responding to a significant incident involving domain names.
- *High operational quality*. The competence in operations demonstrated through the Security Verification Program provides confidence that the Registry operator is able to respond to threats to the security, stability, and resiliency of the DNS.
- *Published admission policies for second level domains and a reliable "thick" Whois.* These policies are consistent with transparency and accountability objectives that the community seeks to achieve.
- *Strong ability to investigate and make assertions about the second level domains.* The program provides confidence to Registrants and Internet users that Registry and Registrar operators will work in a coordinated and effective manner in response to disputes and complaints (e.g., malicious conduct) involving the Registry's domain names .
- *Continuity of trust from Registry to Registrant*. The Security Verification Program provides confidence to Registrants and Internet users that Registry and Registrar operators work together to maintain the level of trust the program seeks to achieve.
- *Strong, multi-factor registrant authentication throughout the namespace.* The program seeks to greatly reduce or mitigate opportunities for impersonation and/or malicious conduct in the domain registration and DNS configuration processes.

3. Elements of a High Security Zone Verification Program

This section describes the key elements proposed to support the rollout of a Security Verification Program. As the Security Verification Program continues to be evaluated and improved, this section is likely to be modified to support additional elements and to provide more detail for the existing elements.

3.1 Governance

This section briefly describes the Security Verification Program's Governance structure. A successful Security Verification Program requires appropriate ownership and a functional and active governance body. The governance body is primarily responsible for creating and managing the processes and relationships that allow for good decision making necessary to create, support, and enforce the Security Verification Program. To accomplish this goal, the governance body will be formed by a group of individuals or organization(s) that will provide oversight and stewardship; set direction on issues such as appeals, grandfathering, and information disclosure; and evaluate the Security Verification Program's overall effectiveness.

For the purposes of this concept paper, the general governance structure below provides a strawman perspective on how the governance structure may be designed. It is critical to note that this structure is simply a suggested beginning approach, designed to provide a starting point for governance body discussions, decisions, and finalization. Overall, the structure, participants, and responsibilities are likely to change significantly from this initial concept.

Illustrative example Governance Body key stakeholders:

- *Program Sponsor* – The program Sponsor will be the overall sponsor of the High Security Zone Verification Program. To support this, a "Security Verification Program Working Group" will be created. Responsibilities of program ownership include, but are not limited to, setting program criteria, publishing appropriate documentation and guidance, providing a system of record for designated entities, sponsoring a working group, and providing adequate personnel and tools to enable effective operation of the program. Many of these tasks will be accomplished through the working group members, as representatives to the program.

- *Security Verification Program Working Group* – A "Security Verification Program Working Group" will be created to craft an appropriate charter for working group activities and to enhance and manage overall program direction. In general, the working group is committed to supporting ownership of the TLD Security Verification Program. They will assist in many aspects of the program, including setting standards and guidelines for the program, providing necessary program oversight, evaluating the assessments to grant actual Security Verification, and sponsoring community and public involvement. Some of the key working group representatives should include the following:

    - *Registry/Registrar Community* – Key representatives of the Registry and Registrar community will be participants in the working group. This allows for the Registries and Registrars to have a voice in the direction of the program through active participation. This will help achieve a better quality program that is reasonable, appropriate and effective for the community.

    - *Program Partners* – To help broaden the view of the program, key partners should be considered for membership in the working group. These may include industry focus groups, other certification bodies, web application vendors, security experts, tool vendors, etc. Inclusion of partners will allow for a

smoother interaction with other similar industry programs, will help in the appropriate response to key industry concerns and will help allow for the inclusion of key program components (seal, etc.) in various technology tools.

- *Security Verification Program Auditors/Assessors* – A critical working group perspective will come from the groups that will perform actual Security Verification Program control assessments. This representation will help the working group determine specific needs, areas for improvement and key metrics around the assessment activities.

Actual membership and structure of the governance body should be defined and modified as the Security Verification Program is further developed. It is likely to change as the program is fully developed but should maintain the overall goals of program ownership, communication, measurement, and success.

3.1 Program Requirements and Standards

This section contains details about the Program's core requirements. They are represented as a collection of principles, objectives, and criteria that form the basis of controls designed to improve TLD security and trust. When fully completed, each criteria topic will also have one or more illustrative control examples that provide guidance for an appropriate control necessary to meet the criteria requirements. In the current concept paper, this section is a placeholder designed to demonstrate overall structure. Further analysis, design, and documentation must occur to craft an effective body of controls.

This version of the concept paper offers sample criteria topics. These are expected to serve as the bases for further discussion and are considered to be necessary to establish actual final criteria, criteria language, and criteria definition.

Many of the criteria topics listed below are also requirements of all gTLD applicants. They continue to be requirements of the Security Verification Program and they will be subject to regularly scheduled assessment. Compliance for gTLD's that do not elect to pursue the Security Verification Program will continue to be monitored by ICANN as a function of ICANN's existing compliance program. For additional information regarding assessments required for Security Verification, please refer to sections 3.3.2 to 3.3.6 of this concept paper.

3.1.1 Program Principles, Objectives and Sample Criteria

PRINCIPLE 1: *The Registry maintains effective controls to provide reasonable assurance that the security, availability, and confidentiality of systems and information assets supporting critical registry IT (i.e., registration services, registry databases, zone administration, and provision of domain name resolution services) and business operations are maintained by performing the following:*

- *defining and communicating performance objectives, policies, and standards for system and information asset security, availability, confidentiality, and privacy;*

- *utilizing procedures, people, software, data, and infrastructure to achieve defined objectives in accordance with established policies and standards; and*
- *monitoring the system and information assets and taking action to achieve compliance with defined objectives, policies, and standards.*

No.	Topic	Objective	Possible Criteria Topics
1.1	Registry IT Infrastructure Security	Key elements of the IT components that support the TLD infrastructure are secured and appropriately protected from unauthorized physical and logical access.	• Security management • Personnel security • Physical access control • Media storage and disposal • System acquisition and development controls • Security incident management controls • Security incident response and reporting • Interface controls • System access management • Network security • Application security • Encryption requirements • Periodic vulnerability testing and response exercises • System software release process • Name resolution service management controls (e.g., DNS zone integrity and name server availability monitoring, …) • DNSSEC deployment plan • Secure communications channels (authenticated, encrypted connections with registrars) • Information asset management (database accuracy/integrity/availability services for zone, registration and other customer data)
1.2	Registry IT Infrastructure Availability	TLD services are available for use per contract or commitment.	• Service level agreements • Whois service availability • Whois service performance level • Whois service response times • Whois accuracy and completeness • Availability monitoring • Registration and transaction data escrow including escrow schedule, specifications, transfer, and Security Verification • Disaster recovery and business continuity plan (failover practices, including plans to sustain name resolution service in the event of a business failure) and exercises • Environmental controls (power and air conditioning, fire protection, generators) • Cabling security controls

No.	Topic	Objective	Possible Criteria Topics
1.3	Confidentiality and Privacy of Sensitive Data	Information owned, managed or transferred through the TLD that has been designated as confidential is protected as committed or agreed. Personal information collected by the TLD operator is collected, used, retained, disclosed, and destroyed appropriately, in line with relevant data protection laws per the jurisdiction of the registry operator.	• Appropriate classification of confidential and personally identifiable information • Data collection, use, retention, access, and disclosure policies • Data at rest and in transit • Third party access to information • Encryption requirements • Management controls for signing keys • Physical and logical access controls • Segregation of duties • System monitoring • Personal security controls

PRINCIPLE 2: *The Registry maintains effective controls to provide reasonable assurance that the processing of core Registry functions are authorized, accurate, complete, and performed in a timely manner in accordance with established policies and standards. The identity of participating entities is established and authenticated.*

No.	Topic	Objective	Possible Criteria Topics
2.1	Registry Security Verification	Registry operator credentials are made available to substantiate the identity of the legal entity that operates the TLD.	• Vetting of REGISTRY organization, including – Background of principals – Verifiable address – Verifiable e-mail address – Verifiable telephone numbers – Articles of incorporation – Certificate of formation – Charter documents – Business license – Doing Business As (i.e., assumed name) – Registration of trade name – Partnership papers – Business license • Insurance coverage • Financial capabilities • Revalidation requirements • Screening processes for employees
2.2	Registrar Security Verification	The identity of the Registrar is designated and established prior to commencement of operations	• Vetting of REGISTRAR organization topics noted in 2.1 • Registrar accreditation status • Revalidation requirements
2.3	Registry Processing Integrity	TLD data is consistent and correct at the TLD Registry level.	• Domain name registration and maintenance • Maintenance, accuracy, completeness, and integrity of public Whois data • Vetting of new registrar • Ongoing monitoring processes • Registrar data QA/quality review (and escrow data audit results)

No.	Topic	Objective	Possible Criteria Topics
			• Dispute resolution process
2.4	Anti-abuse Policy and Enforcement	Establish effective controls to reduce malicious conduct by Registrars and Registrants	• Anti-phishing and anti-spoofing controls for new TLDs • Independent third party rating(s) from reputable anti-phishing and anti-malware analysts and laboratories • SLA based on percent of malicious domains per "unit measure" of registrations (e.g., 1000, 5000, 10,000 domains) • Orphaned name server policy (statement of what actions will be taken to identify and correct orphaned name servers) • Abuse points of contact with a documented response process that is timely and auditable • Definition of malicious use (conduct), explicit prohibition of malicious conduct in registrant terms of service agreement • Rapid Domain Suspension process • Thick Whois process and support • DNSSEC & IPv6 deployment plan • Real-time zone monitoring (e.g., for suspicious activity, e.g., fast flux) • Monthly reports of malicious activity reported to registry (such as phishing and botnets) and commitment to address if results are high (relative to other registrars who do business with this registry)

***PRINCIPLE 3**: The Registry shall maintain effective controls to provide reasonable assurance that the processing of core Registrar functions by its Registrars are authorized, accurate, complete, and performed in a timely manner in accordance with established policies and standards. The identity of participating entities is established and authenticated.*

No.	Topic	Objective	Possible Criteria Topics
3.1	Registrant Security Verification	Registrant identity is verified and established prior to provisioning of domain name by the Registrar.	• Vetting of organization topics noted in 2.1 • Authority of Registrant to register in the TLD • Commercial users exempt from Proxies/Anonymous Registrations (applicant must provide proof that the applicant is a natural person, organization must show cause or justification for anonymity)
3.2	Registrar Processing Integrity	Data is consistent and correct at the Registrar level.	• Registrar authenticating new registrants through agreed processes • Registrar confirmation that registration data are accurate and complete • Registrar monitoring registration data for accuracy and completeness • Registrar authentication of registration data for each transaction • Registrar confirmation of change in registration data • Rejection/suspension of registration data with cause (incomplete, false/inaccurate) • Thick Whois • Registrar removal of registration data

No.	Topic	Objective	Possible Criteria Topics
			• Ongoing monitoring processes • Periodic QA review of registrant data • Takedown process and timeliness objectives (e.g., MTTR)

3.2 Program Assessment Methods

This section describes the process that TLD Operators would undergo as a component of periodic compliance assessment. It demonstrates that the TLD Operators are consistently implementing the necessary controls for Security Verification and allows enforcement of the required business practices defined under the requirements of the Security Verification Program.

3.2.1 Circumstances of Assessment

The circumstances of assessment shall be determined by the governance body based on a variety of factors including, but not limited to, the applicable operator trust model as defined in section 1.2 of the Security Verification Program. Requirements for compliance, where applicable, shall be disclosed within the operator application. A compliance assessment is not required to be completed by TLD operators, unless they are seeking Security Verification.

3.2.2 Type of Assessments

3.2.2.1 Point-in-time Readiness Assessment

Point-in-time readiness assessments can occur prior to TLD operation commencement (during the TLD evaluation process) or can occur after the TLD has been in operation. To accomplish a readiness assessment, the TLD operator successfully completes an initial point-in-time readiness assessment against the compliance criteria, or a point-in-time readiness assessment audit against equivalent audit procedures approved. The purpose of this assessment is to establish that the TLD operator has designed and established appropriate technical and procedural controls for operations.

3.2.2.2 Periodic Assessment of Operations

To maintain Security Verification, the TLD operator periodically completes a full or limited scope audit of operations to demonstrate continuing compliance with the requirements of the compliance criteria. The purpose of this assessment is to evaluate not just whether the TLD operator has policies and procedures, but whether the TLD operation consistently followed those policies and procedures to meet the Security Verification Program criteria over a period of time.

3.2.3 Frequency of Assessments

The point-in-time readiness assessment shall be performed by an operator only once prior to commencement of operations or when electing to achieve a Security Verification for the TLD. The point-in-time readiness assessment is the required first step toward achieving Security Verification. Once the point-in-time readiness assessment is passed, a second review is necessary, to validate that the processes, controls and procedures reviewed in the point-in-time readiness assessment are operating as planned over a specified (yet to be determined) period of time. If deficiencies are identified during the review, they would be communicated to the Registry. The Registry would have a short period time to resolve the problem before any compliance action is taken. Finally, in order to maintain

proof of a functioning control environment, full recertification audits shall be performed on a recurring biennial basis.

3.2.4 Identity and Qualifications of Assessor

Compliance assessments may be performed by a qualified independent third-party.

Third-party assessors may either be accredited under a new compliance accreditation program or may be specifically approved on a case-by-case basis. Third-party assessors shall possess the following minimum qualifications as set forth below:

1. Be an independent firm that has proficiency in examining information security tools and techniques, information technology and security auditing, and the third-party attestation function. Consideration should be given to the auditors' accreditation. Appropriate international accreditation should be added to this section as the Security Verification Program is matured; and
2. Be approved as an Assessor.

3.2.5 Assessor's Relationship to Assessed Entity

The compliance assessor shall be a firm which is independent from the entity being audited. The program governance body shall, in its sole discretion, determine whether a compliance assessor meets this requirement. Actual independence rules will need to be created and published as a step in the overall program development.

3.2.6 Topics Covered by Assessment

The scope of the assessment shall include the topics included in the defined Security Verification criteria or equivalent. In cases where the Registry operator has already successfully completed an assessment based on an alternate standard (e.g., ISO 27001), determination of the partial or full equivalency of previously evaluated criteria to the Security Verification criteria may be made by the program governance body. The details of program overlap with similar standards can be determined once Section 3.2 has been fully agreed upon.

3.2.7 Reporting Requirements

3.2.7.1 Type of Report

Compliance assessment results presented within the audit report to the governance body shall follow a standardized format with the expectation that minimal customization may be required, in some cases, in order to comply with appropriate local and/or industry professional auditing standards and guidelines.

Standard components of the report shall include the name of the firm performing the assessment and issuing the report, the period of time evaluated, the scope of the assessment and the locations inspected, evaluation criteria used during the assessment, the assessor's opinion regarding the operator's achievement of the identified criteria, any exceptions that were noted that caused the operator to not successfully achieve one or more of the evaluation criteria, and the professional standards followed by the firm in providing the opinion.

3.2.7.2 Communications of Results

The audit compliance report shall be submitted to the governance body for evaluation in accordance with the frequency noted in section 3.3.3 of the Security Verification Program.

3.2.8 Evaluation of Results and Handling of Deficiencies

The governance body is responsible for evaluating the results of compliance assessments and for determining whether operators are in compliance with the Security Verification Program requirements. In instances where a TLD operator is not in compliance with the requirements of the Security Verification Program, the governance body can remove the TLD operator's Security Verification Seal (*see* 3.5.2 re Security Verification Seal), procedures shall be developed for making and implementing such determinations. It should be noted that Security Verification is separate and distinct from contractual TLD obligations. Security Verification may be revoked through the removal of the Security Verification Seal, but this does not have a direct impact on the actual operation of the TLD. Additional consideration for these circumstances is beyond the scope of this document, but should be an area of focus for further program development.

3.3 Preparation, Training, and Remediation Activities

New and existing TLD operators may consider achieving Security Verification for their operations to demonstrate their commitment to current commonly-accepted and generally recognized good security practices. A considerable amount of work and effort might be required inside their existing framework to achieve Security Verification. It will be critical for their success to make use of the existing and new informational materials that the program will provide.

As part of the Security Verification Program, supporting guidance to TLD operators through program documentation will need to be created, that addresses topics that include the following:

- Defining how to review the existing framework
- Defining the scope and boundary of the planned Security Verification process
- Defining components, processes, and related terms in order to fulfill the relevant Security Verification domains
- Defining the required maturity of the components and processes, and their priorities
- Defining a clear and simple reporting documentation
- References to or inputs from best practice guidelines (i.e., WebTrust, etc.)
- A representative project plan for implementation
- Defining the overall life cycle of the Security Verification (i.e., plan-do-check-act)

Such guidance would be published with the launch of the program and would be available at www.icann.org. In addition, such topics may be presented at periodic ICANN meetings for purposes of awareness and training.

On a periodic basis post-launch, ICANN could facilitate sessions at ICANN meetings that address topics such as:

- Defining a compliant documentation structure;
- Roadmap on how to gradually improve the existing components; and
- Common identified gaps and potential solutions to fix them.

3.4 Administrative Practices

This section is designed to create a structure of areas that will need to undertake to support a new Security Verification Program. Each area includes a brief description of the systems, activities, and processes that must be in place to appropriately support a Security Verification program.

3.4.1 Build and maintain accurate system of record for Security Verification

A system of record will be created to host and maintain an authoritative list of Security Designated entities. Controls will be established to ensure that entities are appropriately registered within the Security Verification Program tracking system and the Security Verification Program tracking database is regularly updated to reflect the most current Security Verification status of entities. The authenticity of Security Verification status is to be validated prior to making any status updates within the Security Verification Program tracking system. The system will be designed to include strong security and privacy controls to protect the integrity of hosted information.

3.4.2 Security Verification Seal

A *Security Verification Seal* will be designed that would represent a TLD operator's commitment to a high level of operational quality and security assurance in its services. To obtain the Seal, the operator undergoing the audit must successfully meet all the applicable requirements associated with the Security Verification Program as demonstrated by an opinion presented by an independent assessor. The Security Verification Seal will demonstrate that the operator has passed a rigid, professional inspection and assessment of its services, and that the quality and integrity of its services has been validated and assessed by an independent group of professionals.

An authorized Security Verification Seal enables an operator to use the logo on its website. The Security Verification Seal will be a unique design. ICANN will have exclusive ownership of the trademark and all rights with respect to its use. Misrepresentation and/or misuse or display of the Security Verification Program Seal will be strictly prohibited by and will result in legal action taken, or cancellation of right to display Seal or be considered a Security Designated TLD.

3.4.3 Verification, Tracking, and Communication of Program Status

Once the Security Verification Seal has been obtained, the TLD operator will be able to continue displaying it on its website, provided that the auditor updates its assurance examination of the operations of the TLD operator on a regular basis and presents, if warranted, a renewed "pass" decision within its audit opinion. The interval between assessments will depend on the nature and complexity of the TLDs operations, the frequency of significant changes to their operations, the nature and number of any

previously identified audit issues, and the professional business judgment of the governance body.

Status of TLD operator compliance and TLD compliance expiration dates will be tracked and communicated to all security designated entities. The tracking process will include automatic reminders prior to expiration of the Security Verification Seal, follow-up procedures for TLD operators who miss the deadlines to complete the Security Verification requirements, and an exception management policy.

During the period between audits, it is the responsibility of the TLD operator to inform the Security Verification Working Group and its auditor of any significant changes to the TLD operator's business policies, practices, and controls, particularly if such changes affect the TLD operator's ability to continue to meet the Security Verification Program principles and criteria. Such changes may trigger the need for an assurance update, or in some cases, removal of the Security Verification Seal until an updated assessment can be made by an auditor.

4. Emerging Issues

This section briefly describes important areas that require further community consideration, discussion, and proposed elements for inclusion in the program. As the Security Verification Program continues to be evaluated and improved, the issues noted in this section are expected to be resolved.

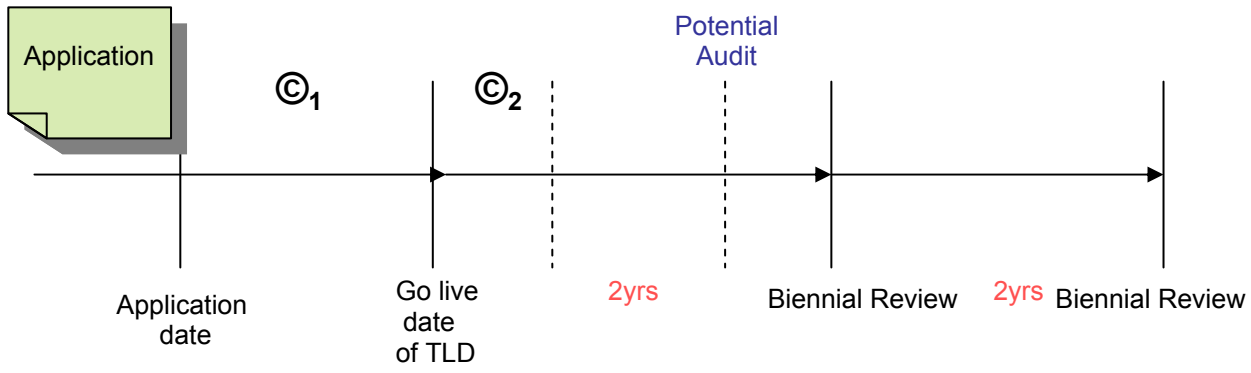
- *Limitation of Liability* – Key issues and resolutions around issues of liability related to the program will need to be identified and resolved.
- *Incentives* – Potential incentives (beyond market value) should be considered as a component of the program.
- *Background Checking* – The ability to obtain valid background checks in a global implementation will need to be examined.
- *Assessor Requirements* – Full requirements to become a Security Verification Program Assessor will need to be developed and published. Requirements will also need to define assessor independence.
- *Metrics and Reporting* – Development of standardized metrics and report templates designed to report compliance to the governance body, management team, the Board, and the Internet Community. These reports and metrics would be published.
- *Anticipated Fees* –At this stage in development, fee structure for the program has not been decided. It is anticipated that Registries wishing to pursue Security Verification will be required to pay fees for the evaluation of operation of controls in their environment. The fees will be revenue neutral and will likely be paid to a third party directly.

Appendix A: Program Timelines

This section outlines an overall timeline for the Security Verification process. In this draft, it represents the key activities, gates, and relative timeframes for execution of various program components. The timeline will continue to be refined as this draft is communicated and updated with content. Currently, two models are presented, as figure 1 and figure 2 respectively.

The model in figure 1 below represents the Security Verification process for a TLD that elects to verify prior to delegation (known as "going live" or "go live") with their TLD. Elements of the Security Verification Program will be coordinated prior to the "go live" date. The model in figure 2 below represents the Security Verification process for a TLD that has been in operation, but wishes to establish Security Verification for the TLD.

Figure 1: Timeline for Security Verification of TLD Operators Prior to "Going Live" (currently relative timeframes)



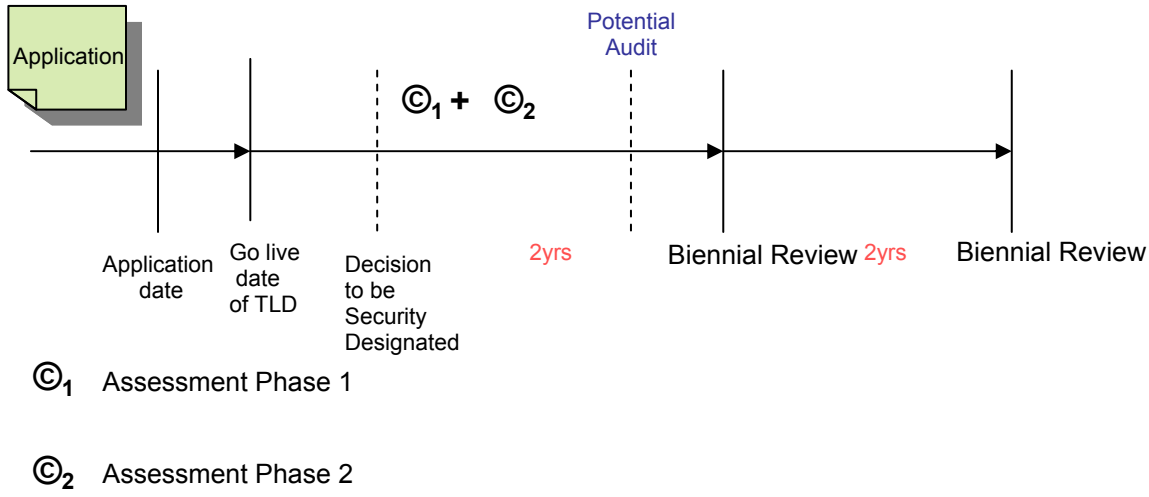
©1 Assessment Phase 1

©2 Assessment Phase 2

A TLD operator elects to obtain Security Verification prior to the completion of its application. Figure 1 above represents the relative process and timeline for the Security Verification. This process begins once the application is received and has two phases: Phase 1 and Phase 2.

- **Phase 1 –** The purpose of this phase of the assessment is to establish that the TLD operator has designed and established appropriate technical and procedural controls for operations, in line with the requirements set forth in the Security Verification Program.
- **Phase 2 –** After the registry has been approved and starts operation, a reasonable period of time will be given for it to implement all the pre-approved processes and controls There would then be a second review that would test the processes/controls/procedures documented in Phase 1 to validate they are operating as planned. If deficiencies are identified, they would be communicated. The Registry would have a short period time to resolve the problem before any compliance action is taken.

Figure 2: Timeline for Assessment of TLD Operators After "Going Live"
(currently relative timeframes)



In this case, the Security Verification does not take place upfront, but at a later date. Phases 1 and 2 will be combined together.

A TLD operator elects to obtain Security Verification anytime after the completion of its application. Figure 2 above represents the relative process and timeline for the Security Verification. This process begins once the application is received and has two phases: Phase 1 and Phase 2.

- **Phase 1** _ The purpose of this phase of the assessment is to establish that the TLD operator has designed and established appropriate technical and procedural controls for operations, in line with the requirements set forth in the Security Verification Program.
- **Phase 2** _ Phase 2 of the review tests the processes/controls/procedures documented in Phase 1 to validate they are operating as planned. A reasonable period of time will need to be established, for the Registries controls to operate, so that they can be reviewed in operation. If deficiencies are identified, they would be communicated. The Registry would have a short period time to resolve the problem before any compliance action is taken.

Subsequent to successful review and based on risk factors (e.g., complaints from registrars or on a random basis), it may be desirable to perform another review of the TLD operator during the designated period to test ongoing compliance with the agreed to processes/controls. Any deficiencies would be communicated. The TLD operator would have a short period of time to resolve the problem before any compliance action is taken.

All Security Designated TLDs should be considered for re-review on a biennial period.