DRAFT WORKING PAPER

Best Practices for Electronic Collateral Registries

Prepared by

NatLaw

MARCH 29, 2019

BEST PRACTICES FOR ELECTRONIC COLLATERAL REGISTRIES

CONTENTS

I. INTRODUCTION

A. BACKGROUND

This Working Paper on Best Practices for Electronic Collateral Registries has been produced as part of the **Best Practices in the Field of Electronic Registry Design and Operation project** (BPER project, or the Project). The BPER project is a joint undertaking between the UNIDROIT Foundation, the Harris Manchester College Commercial Law Centre at the University of Oxford and the Global Business Law Institute at the University of Washington.

The purpose of the BPER project is to develop a framework to establish and evaluate best practices in electronic registration, both as a guide to registrars and those involved in such registration, especially in the context of various risks that may affect the registrar's liability. Electronic registries have emerged as a main element of systems in many contexts (including commercial contexts) that collect, store, and disseminate data, and, in some cases, establish and transfer property rights. Establishing best practices for their design and operation is, therefore, of major importance.

The Project initially emerged out of the Cape Town Convention on International Interests in Mobile Equipment, which provides for the establishment of international registries for interests in different categories of assets. Article 28 of the Convention sets out a standard for the responsibility of registrars for losses resulting from a 'malfunction' caused by 'inevitable and irresistible' events but also provides a defence where 'best practices in current use' in the field of electronic registry design and operation, including those related to back-up, systems security and networking, have been followed. However, 'best practices in current use' in electronic registries is not defined by the Convention, nor have international parameters been set forth.

To assess best practice, the Project has identified Critical Performance Factors (CPFs) against which electronic registries can be measured. The relevance and weight of each CPF is expected to vary depending on the particular registry being evaluated.

The Project has been progressed through expert meetings and papers. The first two academic workshops were held at Harris Manchester College in March 2016 and March 2017 respectively. It is anticipated that further work will be done, both on expanding the BPER project's consideration of best practice for collateral registries, as well as expanding the analysis to evaluate best practice for other types of electronic registries.

The BPER project is supported by Aviareto, a Dublin-based joint venture between SITA and the Irish Government which operates the International Registry of Mobile Assets, as established under the Aircraft Protocol to the Cape Town Convention.

B. WORKING PAPER OBJECTIVES

This Working Paper examines 'best practices' in current use in the field of electronic registry design and operation, focusing specifically on electronic collateral registries. Throughout, the term 'collateral registry' encompasses filing systems, registries for notices of security rights, and similar publicity mechanisms that perform the following two core functions. First, they allow secured creditors and other claimants to make registrations (submit notices for registration) to render their security interests and other rights effective against third parties ("perfection"); and, secondly, they provide information to searchers who may be the same secured creditors and other claimants, but also prospective buyers of assets. Thus, this Working Paper aims to identify 'best practices' that exclude or mitigate the risks and liabilities faced by collateral registries in performing these two core functions, and coextensively realize a system suitable for all its users, regardless of their sophistication.

To fulfil the two aforementioned core functions, data stored in a collateral registry must be secure against all types of threats.[1] Overall, data access and other registry services should, ideally, be:

- Highly available, such that the registry experiences no unscheduled downtime (e.g. 99.999% uptime, also known colloquially as the "Five 9's");
- Capable of addressing natural or human-caused accidents and disasters, such as fires or floods;[2]
- Protective against the insidious risks posed by human negligence: operational errors, complacency, and false assumptions about technology;
- Highly redundant, such that there is no single point of failure (SPOF) and that failure of one or more components and/or datacenters does not make the entire registry inoperable;
- Fully recoverable in the event of a disaster, such that a catastrophic event (e.g. fire, flood, war, terror attack, etc.) impacting one datacenter does not lead to any data loss and a backup or backups can be semi-automatically or automatically provisioned with minimal downtime (e.g. Recovery Time Objective (RTO) and Recovery Point Objective (RPO) of 0);
- Immutable, such that all entries are tamper proof and that any and all changes can be tracked forensically and verified independently;

[1] See IFC, Secured Transaction Systems and Collateral Registries (2010), at 71, https://www.ifc.org/wps/wcm/connect/c5be2a0049586021a20ab719583b6d16/SecuredTransactionsSystems.pdf?MOD=AJPERES (last accessed March 26, 2019).
[2] *Id.*

- Secure against internal and external threats, such unauthorized access, tampering, and attacks involving malware and/or denial of service attacks are not possible; [3]
- Horizontally and dynamically scalable, such that computing and storage resources can be scaled automatically in response to large peaks in system activity and as such, ensure the system does not slow down or cease operation due to overload;
- Configured to provide adequate monitoring and logging, such that all errors, downtime, and access events are recorded for review and analysis in real-time and/or in the future.
- Configured for proper access control policies/procedures; and
- Capable of providing a high level of confidentiality to ensure that information is not disclosed to an unauthorized person, process or device.

Most collateral registries today operate exclusively electronically. Nevertheless, there are also some registries that provide for manual processes that require submission of notices in writing and subsequent storage in electronic databases (e.g., some UCC filing offices in the United States). Moreover, the UNCITRAL Legislative Guide on Secured Transactions contemplated the possibility of hybrid collateral registries that permit both electronic and manual access. The Guide also provides for the liability of the registry for loss caused by an error or omission in the information entered by the registrar into the record. This Working Paper does not take into account the risks associated with 'manual processes' of hybrid and 'paper-based' registries that allow the submission of registrations in a paper format as an alternative to direct electronic access.

This Working Paper identifies critical performance factors (CPFs) necessary to secure registry data and ensure that registry functions are available while maintaining access control and confidentiality of data stored in registry databases. By exploring international standards and guidelines that address risks to registry performance, this Working Paper seeks to identify best practices for the design and operation of collateral registries. Following best practices is important, not only for collateral registry performance and reputation, but also to mitigate registry liability.

The collateral registry that is the focus of this Working Paper should be understood more broadly than a registry for notices of security rights as envisaged in the UNCITRAL Model Law on Secured Transactions. It also encompasses electronic registries established for the electronic registration of notices relating to a specific type of transaction, such as finance leases.[4] Having in mind a broader focus of the overall project, the recommendations and the analysis below may equally apply to registry

[3] Rob Cowan & Donal Gallagher, The International Registry For Aircraft Equipment—The First Seven Years, What We Have Learned, 45 UCC L. J. 225, 249 (2014), https://www.aviareto.aero/wp-content/uploads/2015/03/UCCLJ-Volume-45-No3-Cowan-Gallagher.pdf (last accessed Feb. 8, 2019).
[4] Several countries have established such registries, including Jordan and Palestine.

systems functionally similar to collateral registries, including car registries, intellectual property registries, and companies registries that in many jurisdictions register security rights, in addition to performing other functions. However, some of these recommendations may need to be adapted to private registries, such as those maintained by companies for the issuance of securities, securities intermediaries that keep records of account holders and financial assets, systems for the issuance and transfers of electronic equivalents of documents of title, chattel paper and instruments. For instance, a different confidentiality standard may apply to such systems since they are not commonly accessible to third-party searchers.[5]

The purpose of this Working Paper extends beyond the mere identification of the best practices required by Article 28 of the Cape Town Convention to shield the International Registry from liability for malfunction. It seeks to provide guidance to the designers and operators of collateral registries more broadly. Many international instruments generally refer to liability for certain actions, omission and failures in connection with various registry functions, but do not detail any measures that may prevent or mitigate the risk of such occurrences. Many domestic policymakers and legislators opt for full immunity of the registry from any liability in the absence of clear guidance on the various aspects of liability. This Working Paper also aims to assist domestic reform initiatives that seek to establish collateral registries.

More broadly, this Project aspires to establish a 'functional framework' by identifying the core elements and functions of registries for which the recommendations would be suitable. For instance, one such element is the administrative function of the registry that does not entail verification of the information submitted by the registrant. Another element may be some legal effect that a registration produces, such as with respect to making the right effective against third parties upon registration. The development of this 'functional framework' may take into account the UNCITRAL Model Law on Electronic Transferable Records that contemplates a centralized registry to give public notice of transactions involving transferable documents in electronic form (e.g., an electronic warehouse receipt). A warehouse receipts registry where the issuance and transfer of electronic warehouse receipts is registered is one such example of a registry system that is functionally similar to collateral registry, but for which this UNCITRAL Model Law does not provide any guidance as to the technical parameters to be implemented to properly perform the functions contemplated therein. Finally, the lessons drawn from this Working Paper should be adaptable for the use of credit referencing systems that complement the functions of collateral registries within the broader credit infrastructure.

[5] See further Charles W. Mooney, Jr., FinTech and Secured Transactions Systems of the Future, 81 Law & Contemp. Probs. 1, 8-10 (2018).

C. LEGAL RELEVANCE OF BEST PRACTICES

Collateral registries are established and operate pursuant to: i) international conventions (e.g. the International Registry under the Aircraft Protocol to the Cape Town Convention); ii) federal laws (e.g. the Australian Personal Property Securities Register); iii) state/provincial laws (e.g. the Canadian Personal Property Security Interests Registries); or iv) laws that contemplate multiple registries, typically located in counties (e.g. under the 2011 OHADA Securities Act).

Generally, applicable legislation mandates that the operator of the registry ensure the provision of prescribed services/core functions. Failure to perform some of those functions may trigger liability of the operator/Registrar. However, legislation may or may not provide clear rules detailing the consequences of registry failures. In some States, the registry may enjoy 'full immunity' from any sort of failure allocating the function to mitigate any risk of loss to its users while in others the registry may be liable for some failures. Many States that have recently implemented collateral registries choose the 'full immunity' approach that has caused a concern among the financial sector community that would preclude any claims against the Registrar in case of a loss sustained by inadequate performance of the system erecting a disincentive to the deployment of the reformed framework in practice. In contrast, other regimes subject registries to a variety of liability standards.

As mentioned above, some registries' processes are manual, but most registries today operate exclusively electronically. Recommendation 56 of the UNCITRAL Legislative Guide on Secured Transactions contemplates a hybrid access and for the liability of such a system, it provides the following:

> "The law should provide for the allocation of responsibility for loss or damage caused by an error in the administration or operation of the registration and searching system. If the system is designed to permit direct registration and searching by registry users without the intervention of registry personnel, the responsibility of the registry for loss or damage should be limited to system malfunction."

Differently, the Cape Town Convention (CTC) in Article 28 provides:

> "the Registrar shall be liable for compensatory damages for loss suffered by a person directly resulting from an error or omission of the Registrar and its officers and employees or from a malfunction of the international registration system except where the malfunction is caused by an event of an inevitable and irresistible nature, which could not be prevented by using the best practices in current use in the field of electronic registry design and operation, including those related to back-up and systems security and networking."

Article 28 thus provides for:

1) liability for error or omission by the Registrar or its officers;
2) liability for malfunctioning caused by 'ordinary events' which are not of an inevitable or irresistible nature; and
3) no liability for system malfunctioning caused by an event of an inevitable and irresistible nature if such malfunctioning occurred despite the adoption of 'best practices' in the design and operation of electronic registries.

The CTC establishes that the 'Registrar' owes compensatory damages for losses stemming both from errors or omissions of its employees and malfunction caused by events that are neither inevitable nor irresistible in nature. This liability is strict: it arises regardless of fault, negligence or malice, and cannot be excluded or limited. By contrast, for losses stemming from events that are inevitable and irresistible in nature, the Registrar is spared liability if it can show that it had adopted 'best practices' in current use in the field of electronic registry design and operation.

The liability matrix articulated by Art. 28 of the CTC markedly incentivizes the adoption of 'best practices'. The Registrar will seek to implement such practices to escape liability for losses stemming from events that are inevitable and irresistible in nature. Furthermore, the Registrar will want to implement 'best practices' to avoid human errors or omissions, and to prevent malfunctions due to non-inevitable natural events, as liability for losses stemming for such events is strict.

In the context of the third type of liability, the relevant 'best practices' contemplated by the CTC include those related to:

a) back-ups;
b) system security; and
c) networking.[6]

In the context of design and operation of a registry, the liability can therefore arise from events in three domains:

a) errors or omissions by the International Registry officers and contracted third parties (operation only);
b) hardware failure (design and operation); and
c) software failure (design and operation).

Examples of avoidable malfunctions include: i) human error by an officer manually entering a court order to discharge a registration; ii) hardware failure causing a malfunction that could have been prevented by implementing a design incorporating

[6] It may be questioned whether and how networking relates to the International Registry at all.

redundant hardware; and iii) a malfunction resulting from a software programming error that could have been discovered by off-line system testing prior to deployment.

Consider the hypothetical example of a major software vendor that issues a critical update to its widely used software in response to cyberattacks that exploit a previously unknown software vulnerability to gain unauthorized access to data. The registrar receives notification of the update before the registry is affected but fails to install it before a cyberattack accesses, downloads, modifies, and deletes data stored in the registry database. The cyberattack was enabled by a software design fault (domain c) that (for purposes of this example) could not have been prevented even if the registrar followed best practices before the vulnerability was made public. However, failure to take practicable preventive measures following publicity of the vulnerability may well be an error or omission and failure to follow best practices (i.e. by not following the software provider's advisory to install the critical software update). Therefore, in this example, where the registrar could have prevented the cyberattack by promptly installing the software update, the registrar may be subject to the first type of liability for harm caused by the cyberattack.

The worst-case scenario is one in which a system error or inadequacy (e.g. in the implementation of the process for authenticating registrants) is not discovered until identified by an expert witness during legal proceedings.[7] Such an event could raise uncertainty regarding all registrations.[8]

The CTC does not define or further describe the meaning of 'best practices', leaving this standard undefined. Similarly, domestic secured transactions laws do not provide any or clear liability standards. The objective of this Working Paper is to clarify the meaning of 'best practices' in the context of electronic collateral registries, as the liability of this kind may arise in the context of any electronic collateral registry. In doing so, this paper draws on the earlier work of the BPER Project.[9]

D. RESEARCH OBJECTIVES

The Project previously identified ten *critical performance factors* (CPFs) to securing and maintaining the integrity of electronic registries, defined as essential functions and attributes of a registry, but not limited to collateral registries. A CPF may be any technical feature or system attribute without which a registry is unable to perform its

[7] Cowan & Gallagher, *supra* note 3, at 249.
[8] *Id.*
[9] *See* Aaron Ceross, *Practices in Electronic Registries*, (Interim Report, Spring 2018), this report was conducted within the framework of the "Best Practices in the Field of Electronic Registry Design and Operation" Project sponsored by Oxford University, *see* https://www.law.ox.ac.uk/research-subject-groups/best-practices-field-electronic-registry-design-and-operation (last accessed Feb. 28, 2019).

core functions at a level that meets the reasonable expectations of the relevant market participants.

This Working Paper refines the definitions of these CPFs and identifies additional CPFs. It also expands on previously suggested standards and practices that can be adopted to reduce the risk of malfunctions and related liability. Finally, this paper suggests a CPF hierarchy of priority for risk management. These modifications are partly driven by the present focus on electronic collateral registries.

Table 1: Previously identified CPFs and revised definitions specifically adapted for collateral registries (in alphabetical order)

CPF	**Previous Definition**	**Revised Definition**
1. Accessibility	Property of being able to obtain the use of a resource.[10]	(no change)
2. Authentication	Property that an entity is what it claims to be.[11]	Process of verifying that an entity is what it claims to be.
3. Availability	Property of being accessible and usable upon demand by an authorized entity.[12]	(no change) Additional support by CNSSI.[13]
4. Confidentiality	Property that information is not made available or disclosed to unauthorized individuals, entities, or processes.[14]	Property that information is not made available or disclosed to unauthorized persons.[15]
5. Disposition (Disposal)	Processes implementing records creation, retention, and transfer decisions.[16]	Processes implementing disposal of records: retention, archiving, destruction or transfer decisions.[17]

[10] *See* ISO/IEC 2382:2015 Information technology — Vocabulary.
[11] *See* ISO/IEC 27000:2016 Information technology — Security techniques — Information security management systems — Overview and vocabulary.
[12] *Id.*
[13] *See* CNSSI-4009, Committee on National Security Systems (CNSSI) (2015) at 11, https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf (last accessed Feb. 8, 2019).
[14] *See* ISO/IEC 27000:2016 Information technology — Security techniques — Information security management systems — Overview and vocabulary.
[15] *Id.*
[16] *See* ISO/IEC 27040:2015 Information technology — Security techniques — Storage security.
[17] *Id.; See also* BS ISO 15489-1:2001(E) Information and documentation — Records management, § 3.9, defining disposition as the "range of processes associated with implementing records retention, destruction or transfer decisions."

6. Integrity	Property that data has not been altered or destroyed in an unauthorized manner.[18]	(no change) Additional support by CNSSI.[19]
7. Interoperability	Capability to communicate or transfer data in a manner that requires little or no knowledge of the unique characteristics of the data units.[20]	Ability to communicate with, or transfer data among other systems (e.g. other registries) in an automated manner that does not require the user to be familiar with the operation of the other systems.[21]
8. Reliability	Ability of a system or component to perform its required functions under stated conditions for a specified period of time.[22]	Ability of a system to perform its required functions for a specified period of time.[23]
9. Retention	Property of preserving data in a system for a length of time.[24]	Property of preserving data in a system for a specified period of time.[25]
10. Validation	Confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled.[26]	(no change) Additional support by ISO 9000 and CNSSI.[27]

[18] *See* ISO 16175-2:2011 Information and documentation — Principles and functional requirements for records in electronic office environments — Part 2: Guidelines and functional requirements for digital records management systems.
[19] *Id.; see also* CNSSI-4009, Committee on National Security Systems (CNSSI) (2015) at 41, https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf (last accessed Feb. 8, 2019).
[20] *See* ISO/IEC 2382:2015 Information technology — Vocabulary.
[21] *See Id.* at 2121317, defining interoperability as the "capability to communicate, execute programs, or transfer data among various functional units in a manner that requires the user to have little or no knowledge of the unique characteristics of those units."
[22] *See* ISO/IEC 27040:2015 Information technology — Security techniques — Storage security.
[23] *Id.*; *see also* ISO/IEC 2382:2015 Information technology — Vocabulary, at 2123024, defining reliability as, "ability of a functional unit to perform a required function under given conditions for a given time interval."
[24] *See* ISO/IEC 2382:2015 Information technology — Vocabulary.
[25] *Id*.
[26] *See* ISO/IEC 27000:2016 Information technology — Security techniques — Information security management systems — Overview and vocabulary.
[27] *See* ISO 9000:2015 - Quality management systems – Fundamentals and vocabulary, ISO (Sep. 2015); *and see* CNSSI-4009, Committee on National Security Systems (CNSSI) (2015) at 130, https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf (last accessed Feb. 8, 2019).

E. SPECIFIC RELEVANCE OF THE CPFS TO COLLATERAL REGISTRIES

The revised definitions are tailored to collateral registries. This section amplifies the new definitions and explains the basis for their revision.

1. Accessibility

Definition: Property of being able to obtain the use of a resource.

The Project's previous definition of Accessibility is carried over without modification. Accessibility refers to providing means of access. This is generally accomplished by accessibility via the internet. Moreover, to ensure transparency, access to a collateral registry should not be subject to restrictions that require persons who wish to submit a registration or conduct a search to provide justifications for their actions to either the Registrar or other authority. However, this does exclude the implementation of measures and processes that address abuses and wholly unauthorized entries.

In the context of collateral registries, it should be noted that this definition does not address the cost of using the registry services, such as for registering and searching. The Aircraft Protocol requires the International Registry to recover the "reasonable costs" of establishing and operating the registry by charging fees for its services.[28] Accessibility should be regarded as encompassing the element of cost – any fees must be set at a level that facilitates accessibility.[29] Accessibility must be both technically and economically practicable to encourage use of the registry.[30] For example, some economies are developing an off-line version of its registry for use in remote areas without internet access. Registrations would be uploaded at the end of the day from a location with internet access. This would provide Accessibility to users that otherwise would not have access despite the registry meeting its goal of 24-7 (on-line) Availability.

Other means of accessibility include the ability to accept registrations through application programing interfaces (APIs) or transmitted directly to the registry without the need to interact via the registry website. IACA (the International Association of Commercial Administrators) supports a standard XML (Extensible Markup Language)

---

[28] *See* Aircraft Protocol Art. XX(3), "[Fees to be charged for the services and facilities of the International Registry] shall be determined so as to recover the reasonable costs of establishing, operating and regulating the International Registry and the reasonable costs of the Supervisory Authority associated with the performance of the functions, exercise of the powers, and discharge of [its duties]."

[29] *See* U.N. COMM'N ON INTN'L TRADE LAW, UNCITRAL LEGISLATIVE GUIDE ON SECURED TRANSACTIONS, U.N. SALES NO. E.09.V.12 (2010) at 158.

[30] *See* Marek Dubovec, *UCC Article 9 Registration System for Latin America*, 28 ARIZ. J. OF INT'L & COMP L. 117, 137 (2011).

format recommended for transmitting electronic registrations to UCC registries (filing offices).[31]

2. Authentication

Definition: Process of verifying that an entity is what it claims to be.

The Project's previous definition of Authentication was refined to clarify that this is a process employed by the registry rather than a property. As a practical matter, authentication of a collateral registry user involves multiple processes employed at each stage of a user's interaction with the registry. These include, among others:

a. Upon initial creation of an account by a user that wishes to submit registrations. Examples of authentication techniques include:
    i. Verifying the existence of a company, as well as the accuracy of its name, against a government business registry.
    ii. Verifying an individual's ID against a national ID database.
    iii. Verifying that a user acting on behalf of an organization is authorized by that organization to use registry functions on behalf of the organization (for example, an employee of a financial institution creating an account on behalf of that institution in order to submit registrations).

    In some instances, such verifications require manual efforts by registry staff, such as contacting the institution represented by the user.

b. Upon login by a user that has already established an account. Examples of widely used authentication techniques include requiring the use of strong passwords and two factor authentication (e.g. requiring confirmation of receipt of a text message or email to authenticate a login attempt). The International Registry verifies the user's identity via a digital certificate issued by a Certificate Authority using Public Key Infrastructure (PKI) technology.[32] PKI uses industry standard protocol (Secure Sockets Layer (SSL) and Transport Layer Security (TLS)) to establish secure communications that, i) authenticates users and machines with digital certificates issued by trusted third parties; ii) encrypts communications and data transmissions by using a secret private key and a mathematically related public key; and iii) assures non-repudiation (i.e. provides proof of the origin and integrity of the

[31] *XML Technical Specifications for Uniform Commercial Code Filings Revised Article 9 - Version 4.00*, IACA (2019), https://www.iaca.org/secured-transactions/xml-technical-specifications/ (last accessed Mar. 12, 2019).
[32] Cowan & Gallagher, *supra* note 3, at 230.

transmitted data).[33] Different levels of authentication have been used by established collateral registries.

Nevertheless, the registry should not undertake excessive authentication of the identity of the user but be required to retain information about the identity of the registrant (see Recommendation 7 of the UNCITRAL Registry Guide).

3. Availability

Definition: Property of being accessible and usable upon demand by an authorized entity.

The Project's previous definition of Availability is suitable for collateral registries and is carried over without modification. In general, electronic collateral registries should be accessible 24 hours a day, every day of the year. In practice, occasional downtime will be necessary for scheduled maintenance and updates, and the inevitability of technical and security interruptions. The International Registry regulations provide that, "[t]he International Registry shall be accessible 24 hours a day, 7 days a week, except if precluded by maintenance performed outside peak periods, or technical or security problems, as set out in the Procedures." [34] Recommendation 5(b) of the UNCITRAL Guide on the Implementation of a Security Rights Registry (UNCITRAL Registry Guide) also provides for a continuous operation of a registry.

4. Confidentiality

Definition: Property that information is not made available or disclosed to unauthorized persons.

The Project's previous definition is suitable for collateral registries but was slightly refined. The words "processes" and "individuals" were dropped, because all end users of the confidential information are encompassed by the word "persons." Examples of confidential data contained in a collateral registry include i) those in accounts of users; and ii) statistical information, such as details about the secured obligation, the interest rate or a loan amount that registrants must provide in registrations.[35] Notably, confidential data falling under ii) may be collected by the Registrar for statistical purposes and subsequently disclosed to the public in aggregated form. The

[33] *See* https://docs.oracle.com/cd/B10501_01/network.920/a96582/pki.htm (last accessed Mar. 8, 2019).
[34] For example, *see* Regulations and Procedures for the International Registry § 3.4, ICAO (2016).
[35] For example, *see* Regulations and Procedures for the International Registry § 4.1, ICAO (2016), "Each registry user entity may elect to exclude from the information generated by a search under Section 7.6 its physical address and administrator's telephone number, and in the case of a natural person, his/her date of birth."

confidentiality level of the latter differs since that information included in individual registered notices is aggregated and may be publicly shared. Furthermore, general data protection regulations may apply to personal information.

Regulators generally do not specify the level and detail of necessary security measures. In this respect, the processes and measures adopted by credit registries (a type of credit referencing systems) might provide useful reference points, despite the higher level of confidentiality required for the data generally stored therein (e.g., the core data in credit referencing systems is accessible only to authorized users). In addition to requiring data integrity (see *infra*), data protection regulations generally require that the registry take active steps to protect against data misuse or theft.[36] Active steps include implementing IT security; screening and educating personnel about confidentiality policies; restricting database access to authorized personnel; and implementing staff disciplinary rules regarding information misuse and other breaches of security.[37]

Other critical methods of ensuring confidentiality include encryption of data in transport and data at rest to ensure no unauthorized parties can view confidential data, as well as proper permissions and entitlements for access to data, including Access Control List (ACL) and Role Based Access Control (RBAC) frameworks and policies.

5. Disposition

Definition: Processes implementing disposal of records: retention, archiving, destruction or transfer decisions.

The Project had previously defined disposition broadly to include: "records creation, retention, and transfer." The definition has been refined to conform with standards such as ISO 15489-1:2001(E) Information and documentation — Records management, § 3.9, which defines disposition as the "range of processes associated with implementing records retention, destruction or transfer decisions." Records creation is not included in the refined definition because disposition refers to processes and policies related to the disposal of records (including archiving, deleting, or transferring). Therefore, disposition does not create new records (other than in an activity log or in the sense that archiving inserts records into an archive).[38] While the "add-only" retention policy is of prime importance with regard to registrations before their natural lapse, it is also prudent beyond that period (for example for liability purposes). Nonetheless, general retention of records law may require the complete deletion of certain records from the database

[36] *Credit Reporting Knowledge Guide 2018*, World Bank, IFC (forthcoming 2019), at 45.
[37] *Id.*
[38] Collateral registries should follow an "add-only" policy that "only permit[s] documents to be added to the record, but never removed. *See* Secured Transaction Systems and Collateral Registries, *supra* note 1, at 71.

(including any backup or archived copies). For example, this may apply to certain personal information required for an individual to create a user account in the registry.

6. Integrity

Definition: Property that data has not been altered or destroyed in an unauthorized manner.

The Project's previous definition of Integrity is carried over without modification.

Integrity of registry data lends evidentiary weight to registrations – an important factor for efficiently resolving disputes.[39] Parties should not have grounds to dispute the status, time, or content of registrations.[40] Ensuring Integrity is an ongoing obligation that requires regular reviews and updates of security measures in light of emerging threats.

Integrity relates not only to the data submitted by registrants, but also any data associated with registrations by the registry system. For instance, all registrations and/or state changes in the registry should be timestamped and ordered chronologically. Such timestamps should be cryptographically secured so as to prevent any tampering with the order in which transactions and state changes occur. A forensic audit trail of chronologically ordered events should be maintained. Proper mechanisms should also be in place that prevent race conditions. A race condition occurs when two or more threads can access shared data and they try to change it at the same time.

The World Bank's recommendations for credit registry data security may be taken into account in the context of collateral registries, and include, among others:

i) authentication (*see supra)*;
ii) maintaining and monitoring database access logs;
iii) cybersecurity measures to protect the database from hackers and malware attacks;
iv) continuous monitoring of threats and ensuring up-to-date protection against them;
v) maintaining database backups including continually updating backups stored offsite;
vi) ensuring appropriate governance and delineating authority among network administrators and staff;
vii) periodically testing backup hardware and recovery plans;
viii) ensuring the physical security of the facility, systems, and data; and
ix) instituting security policies and procedures for handling data-security breaches.[41]

---

[39] *See* Marek Dubovec, *supra* note 30, at 132. The integrity is presumed, but may be questioned if there is some impropriety, especially the ability of the Registrar to alter registrations.
[40] *Id.*
[41] *Credit Reporting Knowledge Guide 2018*, supra note 36, at 74.

The International Registry has implemented custom software to alert the Registrar to any unauthorized interference with the database.[42] Timestamp assurance and tamper checking systems assure the integrity of database records.

Where a registry does not operate under governmental authority that would shield it against legal threats to its assets, the collateral registry's legal framework should bolster registry integrity by protecting its assets and databases from seizure or other legal or administrative process. Currently, the International Registry is unique in this regard. CTC Article 27(4), addresses this issue by providing that, "(t)he assets, documents, data bases and archives of the International Registry shall be inviolable and immune from seizure or other legal or administrative process."

7. Interoperability

Definition: Ability to communicate with, or transfer data among other systems (e.g. on-line payment systems) in an automated manner that does not require the user to be extensively familiar with the operation of the other systems.[43]

The definition of Interoperability previously articulated by the Project has been refined to clarify that Interoperability refers to the collateral registry's ability to interface with other systems in a manner that is transparent to the collateral registry user.

To a certain extent all electronic registries are interoperable with other systems if they are remotely accessible (e.g. over the Internet). For each collateral registry, the extent to which Interoperability is required or contemplated as an optional feature will vary according to the applicable statutory and regulatory framework.

Depending on the relevant legal framework, collateral registries might need to be interoperable with a national ID database. In addition, other interconnections may be contemplated with a business registry, an intellectual property registry[44], and a motor vehicle registry.[45] Such interconnections may be established directly or indirectly through a portal. In countries where notices of tax liens are registered, collateral registries may be interoperable with the tax authority database. Moreover, international

[42] Cowan & Gallagher *supra* note 3, at 231.
[43] *See* ISO/IEC 2382:2015 Information technology — Vocabulary at 2121317, defining interoperability as the "capability to communicate, execute programs, or transfer data among various functional units in a manner that requires the user to have little or no knowledge of the unique characteristics of those units."
[44] For the legal challenges presented by the coordination between collateral registries and IP registries see Andrea Tosato, Secured Transactions and IP Licenses: Comparative Observations and Reform Suggestions, 81 Law and Contemporary Problems 155-180 (2018), at 175-176.
[45] *See* Marek Dubovec, *supra* note 30, at 127, 139-40.

registries can be designed for interoperability with state registries where a registration entered into a state registry can then be immediately forwarded to the international registry.[46] The adoption of open technology standards and protocols, such as those developed by the Universal Trade Network Organization (UTNO), facilitates seamless interoperability between digital trade systems, applications, and networks.[47] Finally, almost all collateral registries will have to be interoperable with payment systems that allow users to pay the required fees securely on-line, though this is a different mode of interoperability than the ones described previously.

In practice, when a registrant would enter a debtor's (also known as the "grantor") national ID number into a collateral registry that is interoperable with a national ID database, the registry would perform a search on the national ID database and automatically populate the debtor name field in the registry with data from the national ID database.[48] If the name were incorrect, the user would be alerted to a potential error in the ID number entered for the debtor.[49] Ideally, upon registration of a security interest against a motor vehicle in a collateral registry that is interoperable with a motor vehicle registry, the collateral registry would forward a notice of such registration to the motor vehicle registry which would associate it with that vehicle's record of ownership.[50] Users of the motor vehicle registry would then be alerted to the existence of the security interest.[51]

Interoperability facilitates registrations and reduces data entry errors but is not critical to accomplishing the fundamental functions of public notice of collateral registries. As such Interoperability should not be considered as CPF *per se*, but only if the law that the governs the collateral registry in question demands that it is interoperable with other systems.

8. Reliability

Definition: Ability of a system to perform its required functions for a specified period of time.[52]

---

[46] Charles Mooney, *Relationship Between the Prospective UNIDROIT International Registry, Revised Uniform Commercial Code Article 9 and National Civil Aviation Registries*, UNIF. L. REV., 1999-2, 335, 343.

[47] *See* https://www.marcopolo.finance/details-of-major-trade-finance-network-in-development/ (last accessed Feb. 28, 2019).

[48] *See* Marek Dubovec, *supra* note 30, at 127.

[49] *Id.*

[50] *Id.* at 140.

[51] *Id.*

[52] *See* ISO/IEC 27040:2015 Information technology — Security techniques — Storage security; *see also* ISO/IEC 2382:2015 Information technology — Vocabulary, at 2123024, defining reliability as, "ability of a functional unit to perform a required function under given conditions for a given time interval."

The definition previously articulated by the Project has been slightly simplified. A system's level of Reliability reflects its ability to function consistently over time. The Reliability of a collateral registry comprises two primary elements:

a. The reliability of the software and hardware that enables data entry, retention, and retrieval (for example, registration or searching); and
b. The reliability of the data itself (for example, whether the registrations returned by a search contain the relevant information).

Changes to search logic may negatively impact Reliability in terms of consistent software operation over time. For example, by failing to retrieve registrations that previous logic retrieved for identical search criteria. This is a risk associated with registries that utilize a close match search logic that may be regularly refined. The UNCITRAL Model Law contemplates such a search logic in Article 28 (Option B) of the Model Registry Provisions.

9. Retention

Definition: Property of preserving data in a system for a specified period of time.

The Project's previous definition of Retention has been clarified. Retention of registration data for providing notice of the possible existence of security interests is the primary purpose of a collateral registry. The IFC Toolkit for Secured Transaction Systems and Collateral Registries (the IFC Toolkit) emphasizes the importance of an add-only policy for amending and terminating registrations.[53] Under this policy, the registry retains the original record and adds amendment and termination notices without removing registration records before their natural lapse. This allows a searcher to discover a registration even after its effect has been terminated and to retrieve the prior state of a record that has been amended. This is especially important if termination was unauthorized or does not apply to all secured creditors of record. The UNCITRAL Model Law provides another option which is to remove a registered notice upon registration of a cancellation (termination) notice.

If the record is corrected, such as upon discovery of an error made by the registry, a record of the registration prior to its correction may be important to determine liability when a searcher relied on the uncorrected record before the correction was made.[54] Data retention is essential to data integrity – see Integrity *supra* for World Bank recommendations regarding data backup.

10. Validation

[53] *See* IFC, supra note 1, at 71.
[54] *Id.; and see* UNCITRAL Model Law, Model Registry Provisions, art. 31.

Definition: Confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled.

The definition previously provided by the Project is carried over without modification. ISO 9000 and CNSSI provide additional support for this definition, which was originally based on the ISO/IEC 27000:2016 definition.[55] Validation improves the quality of data contained in the registry by rejecting submissions that do not conform to required data specifications. Validation may be as simple as verifying that a required field has not been left blank or that the required number of digits for an ID number have been entered.

II. ADDITIONAL CPFS FOR COLLATERAL REGISTRIES

The CPFs identified by the Project and amended as suggested above identify in a large part the technical features and system attributes that a collateral registry must possess to perform its core functions in a manner that adequately addresses design and operational risks while serving the needs of its users. However, this Working Paper advances the submission that six additional CPFs ought to be considered to cover fully the spectrum of risks faced by these registration systems.

The first (Access Control) complements the CPFs of authentication and accessibility. The second, Timeliness, highlights the importance of making a submitted registration effective almost instantaneously by storing and making it publicly available for searching. The following two (Legal Authority and Compliance, Legal Authority of the Registrar) emphasize the need for the registry to have a solid legal foundation and for the registrar to have legal authority to respond to certain registry errors. Two more CPFs are suggested (Error Correction and Continuity) in relation to the legal duties of the registrar to maintain the integrity of the registry data and to secure its continuous operation.

A. ACCESS CONTROL

Definition: the process of ensuring that access to the registry is authorized and restricted according to registry requirements.[56]

Access Control occurs after the registry has identified and authenticated a user (i.e. after determining that the user is in fact who it purports to be – see § E(2) *supra*). Access Control is the process of determining whether the user is authorized to access specific

[55] *See* ISO 9000:2015 - Quality management systems – Fundamentals and vocabulary, ISO (Sep. 2015); *and see* CNSSI-4009, Committee on National Security Systems (CNSSI) (2015) at 130, https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf (last accessed Feb. 8, 2019); *see also* ISO/IEC 27000:2016 Information technology — Security techniques — Information security management systems — Overview and vocabulary.
[56] *See* ISO/IEC 27000:2018 § 3.1.

registry data and functions (e.g. does the user have the necessary database server permissions to submit a registration?).

This definition encompasses both electronic access (e.g. a user remotely accessing the registry through an internet connection) and physical access to the registry hardware (e.g. a technician replacing hardware). As a practical matter, electronic access control (e.g. server-side database permission verification) occurs whenever the user attempts to access a registry function or process such as viewing or entering data (e.g. whether the user has permission to submit a registration or only to conduct a registry search). For instance, access control mechanisms implement the legal requirement for only authorized entities to submit effective amendments and terminations with respect to a registration, as contemplated in article 5(2) of the Model Registry Provisions of the UNCITRAL Model Law. Various measures can be implemented to counter attempts to gain unauthorized access, these include automatically terminating sessions that are inactive for a certain period of time and using technology such as CAPTCHA to identify automated intrusive attempts.[57] Physical access control is accomplished by door locks and other security measures.

An access control strategy should also address the threat of harm by a "trusted insider" whose authorized access is used either maliciously or negligently. Pre-employment, ongoing screening, and training of trusted-insiders (including employees, contractors, and vendors who have access to the registry) is essential. A study of 7,800 publicly reported breaches of information systems between 2012 and 2017 found that 50% of breaches involved insiders.[58] Negligence, including unintentional exposure of trusted-users' accounts to co-option by unauthorized individuals, accounted for 44% of insider breaches.[59] To minimize such threats, access authorization should not exceed what is necessary for an employee's authorized tasks. Audit logs of all user actions should be maintained for monitoring user activity and diagnosing breaches.

B. TIMELINESS

Definition: the property of making a registration publicly searchable, and therefore effective, almost instantly after its submission.[60]

---

[57] CAPTCHA is the acronym for "Completely Automated Public Turing test to tell Computers and Humans Apart." To continue a session, users must correctly identify numbers or letters contained in randomly generated CAPTCHA images.

[58] *See* https://www.mckinsey.com/business-functions/risk/our-insights/insider-threat-the-human-element-of-cyberrisk (last accessed Mar. 25, 2019).

[59] *Id.*

[60] See *UNCITRAL Guide on the Implementation of a Security Rights Registry*, United Nations (Mar. 2014), § 109, *recommending*, "[i]f the registry is designed to enable users to electronically submit information in an initial or amendment notice to the registry without the intervention of registry staff, the registry software should be designed to ensure that the information becomes publicly searchable immediately or nearly

Generally, a registration does not becomes effective (and thus does not make the security interest effective against third parties) until it is publicly searchable.[61] Therefore, the registry should almost immediately accept or reject a notice upon its submission (note that this requirement precludes any registry staff intervention).[62] Upon accepting a registration, the registry should almost immediately store and index the registration to make it publicly searchable and generate a printable search result confirming effectiveness of the registration.[63] This registration confirmation should include the date and time that the registration became searchable, and thereby effective, as well as the registration number assigned to the notice, and all information entered for the notice.[64]

Timeliness benefits the registrant, the searcher, and the debtor.[65] The debtor benefits by having quicker access to funds because the lender need not wait for registrations to become searchable.[66]

C. LEGAL AUTHORITY, COMPLIANCE, AND GOVERNANCE

Definition: the property of ensuring that the registry is established and operates pursuant to a sound legal framework.

While the focus of the Project has been to develop best practices and associated CPFs related to the technical aspects of design and operation of electronic registries, it is important to highlight the need for a sound legal foundation, which is essential for notices of security interests. Registrations in collateral registries render property rights in the form of encumbrances and transfers of ownership effective against third parties and establish a priority for those rights, which may not be the case for other electronic registries. Statutes and regulations provide collateral registries with authority and credibility that foster their use and reliance on their services; moreover, they establish the governance under which these publicity systems must operate.

---

immediately after it is transmitted." Compare with UCC 9-516(a) under which a filing is effective upon communication of the record to the filing office.

[61] *Id.* § 107, citing, *UNCITRAL Legislative Guide on Secured Transactions*, United Nations (2010), Annex I, rec. 70, *recommending*, "[t]he law should provide that registration of a notice or an amendment becomes effective when the information contained in the notice or the amendment is entered into the registry records so as to be available to searchers of the registry record."

[62] *See* Marek Dubovec, *supra* note 30, at 135; *and see* Charles Mooney, *supra* note 46,at 339.

[63] *Id.*

[64] *See* IFC, *supra* note 1, at 70.

[65] *See* Marek Dubovec, *supra* note 30, at 136.

[66] *Id.*

This legal framework provides the basis for a functional documentation, including the process model narrative (PMN) from which the designer develops and implements the rules and processes of the registry. The IFC Toolkit describes the PMN as "the most essential document" needed by a collateral registry designer or operator.[67] The legal framework should not prevent the Registrar from updating the registry design as necessary to fulfil its objectives in the future.

Collateral registries collect and process vast amounts of data in performance of their core functions (see above I.B.2 Authentication, I.B.4 Confidentiality, I.B.5 Disposition, I.B.6, I.B.9 Retention). Though large part of this information is commercial in nature, a substantial quantity of personal data is also collected in the process. For example, if a notice is registered with respect to a security interest granted by an individual, personal information such as their name and residential address, sometimes even date of birth, may be required to be provided. Equally, a collateral registry may be accessible for registrations only upon establishment of user accounts, requiring the person in question to provide a variety of personal information and possibly even credit card or bank account details. In designing and operating a collateral registry system all necessary steps should be taken to comply with national, regional and international privacy and data protection laws. Depending on the relevant jurisdiction, these laws might establish mandatory rights for users vis-à-vis the registry, such as a right of access or a right to erasure; moreover, they might impose specific duties on the registrar regarding record keeping, data protection procedures, and mandatory disclosure rules.

Thus, taken together, legal authority, compliance and governance constitute an additional CPF:

> Legal Authority of a Collateral Registry
>
> Definition: The registry should be established on the basis of a sound and clearly defined legal and regulatory framework to support the effective implementation of the registry's operations and the achievement of its policy objectives.
>
> 1. The legal and regulatory framework of the registry should have its basis in appropriate legislation.
>
>   a. The core functions of the registry should be regulated by the law to avoid the risk of the administrative agency modifying the regulations to implement inconsistent policies.
>
>   b. The regulations should address only operational aspects.

[67] IFC, *supra* note 1, at 79.

2. The registry must be fully compliant with its legal and regulatory mandate and operate in conformity with their requirements and objectives.

    a. Compliance includes, but is not limited to, applying appropriate technologies that enable the registry to make available and secure data in accordance with the rules and regulations related to data retention, confidentiality, integrity, and availability.

The statutes and regulations that govern registry operation shape the requirements and objectives of each of the CPFs. For example, accessibility: the regulation may provide that the registry is not liable for loss or damage resulting from lack of access precluded by maintenance performed outside peak periods, or technical or security problems (see section 14 of the Regulations and Procedures for the International Registry). For availability, the law may provide that anyone may register a notice or that a notice may be registered only through an authorized user account or under a digital signature (e.g., Article 5 of the Model Registry Provisions of the UNCITRAL Model Law). For confidentiality, the law (e.g., Article 18(1)(c) of the Cape Town Convention) may prescribe confidentiality of information other than that relating to a registration.

The registry's legal obligations related to data retention and disposition derive from specific legislation and regulation as well as from more general data retention and disposition laws. For example, registry regulations may dictate the length of time that registrations are retained and accessible for public searches, while general retention of records law may require confidentiality and disposal of information after the expiration of a prescribed period.

D. LEGAL AUTHORITY OF THE REGISTRAR

Definition: The legal authority of the Registrar to respond to registry errors.

Although in general, only the registrant should submit initial, amendment, and termination notices, there are instances when the integrity of the registry requires the Registrar to intervene to "correct errors", to register notices of non-consensual interests such as judgment liens or court-ordered terminations. The corrective action is not implemented by actually altering any data. As with the legal authority of the registry, the applicable legal framework should set out the Registrar's duties and the bounds of its authority/access. For example, Regulation 5.17 of the International Registry Regulations addresses the Registrar's authority and duties regarding an error in a registration or a discharge of a registration, or the chronological order of registrations, caused by a malfunction in the International Registry.[68] In such an event, Regulation

[68] Regulations and Procedures for the International Registry, Reg. 5.17, ICAO (2016).

5.17 authorizes the Registrar to i) correct such an error or discharge a registration; or alternatively ii) request the named parties to the original registration to amend or discharge that registration, leave it as registered, or seek a court order.[69] Article 31 of the UNCITRAL Model Law similarly provides for the correction of registry errors and their legal effect. The Registrar's authority to amend or terminate an erroneous registration (caused by a malfunction in the registry) comes with specific duties to give notice to affected parties.[70]

Similarly, the Registry regulations govern the scope and limits of registry staff duties. For example, Section 9.5 of the International Registry Procedures restricts the helpdesk to technical support only – they may not answer legal questions.[71] Users of the International Registry frequently ask Registry Officials questions that they are not at liberty to answer including, what data should be entered in a registration, what type of registration should be made, and how to analyze Priority Search Certificates.[72] The failure to abide by this protocol may trigger the first type of liability identified under Article 28 of the CTC.

E. ERROR CORRECTION

Definition: The process of eliminating a detected failure of a registry requirement.[73]

An important additional CPF (Error Correction) is suggested by the Registrar's unique position of authority to take corrective action for errors arising from registry malfunction discussed under the preceding CPF on the Registrar's legal authority.[74] These errors may affect the system itself or the publicly available data. Errors in the system may not affect parties to transactions, or third-party searchers, and the Registrar should have unrestricted authority and ability to correct such errors. Errors in the data that has been made publicly available are more difficult to address since they may have already

[69] *Id.*, the Registrar may do so "provided that such correction or discharge shall be effective only from the time it is made, and shall have no effect on the priority of any other registration."
[70] *Id.*
[71] *Id.* at 9.5, "The help desk is for technical support only and cannot provide support on other matters, including legal questions. The help desk cannot respond to queries concerning an administrator's, a registry user's or a searching person's: (a) computer or network system; (b) system security policies; (c) Internet access, including its connectivity and performance; or (d) browser."
[72] Cowan & Gallagher, *supra* note 3, at 236.
[73] *See* ISO/IEC 27000:2018 §§ 3.16, 3.17, 3.47.
[74] Error correction might also encompass the registry's role in notifying certain affected parties of an error reported to the registry (e.g. when a debtor reports that collateral described in a financing statement exceeds the scope of the security agreement). This situation parallels the need for credit bureaus (and other CRSPs) to resolving a borrower's claim of erroneous information reported by a lender; in such cases the World Bank reports that generally the CRSP has 15 days to address the error or notify consumers that additional time is required. 70% of 103 credit bureaus surveyed reported that they correct errors within two weeks. See *Credit Reporting Knowledge Guide 2018*, supra note 36, at 66-67.

affected third parties who relied on their accuracy. Any corrective action would need to take into account the interests of affected parties (see further D. Legal Authority).

This CPF relates to the responsiveness of the registry to such errors and comprises four parts: i) detection – a process of continuous or regular checks to detect such errors; ii) response – prompt response to correct errors or otherwise respond as authorized by the legal framework; iii) corrective action to eliminate the cause of an error and to prevent recurrence; and iv) notice – issue prompt notice of such response to affected parties, as required by the legal framework.

F. CONTINUITY

Definition: the ability to continue delivery of registry services at acceptable levels following a disruptive incident.[75]

This broad definition encompasses the resilience required to recover from minor disruptions (e.g. system failure or loss of power) as well as the potentially more disruptive event of the loss of a supplier's services (e.g. a software or cloud-services provider terminating its operations). Continuity is differentiated from Availability by its focus on ensuring long-term operation of the registry, whereas Availability relates to the percentage of time that the registry's services are available over a given period (e.g. a registry may have the necessary assets and resources for Continuity of operations for the next five years and expect its services to be available 99% of the time during that period). For more on continuity see Section IV Business Continuity Management, *infra*.

Continued operation of a collateral registry must be ensured. For example, para 4.179 of the Official Commentary on the CTC includes business continuity among the areas in which the registry should adhere to international standards. Para 4.176 of the Official Commentary explains that the responsibilities of the Registrar with respect to any intellectual property rights necessary for International Registry operation, such as software licenses.[76] When application software is procured from a third-party provider, the registry must either acquire all necessary intellectual property rights to use, copy, distribute, and modify these computer programs or at least obtain perpetual licenses with the same scope.

If the registry relies on outsourced services, such as cloud-hosted internet-services, the registry must be able to migrate the system to another service provider upon termination of the outsourcing agreement. This includes having the technical capability and legal

[75] *See* ISO 22301:2012 § 3.3.

[76] *See* Regulations and Procedures for the International Registry ¶ 4.176, ICAO (2016), "It is also the responsibility of the Supervisory Authority to ensure that any rights required for the continued effective operation of the International Registry in the event of a change of Registrar will vest in or be assignable to the new Registrar. These would include any intellectual property rights necessary for the continued operation of the Registry."

rights necessary to retrieve registry data and adapt software as necessary for compatibility with another provider's system.

Comprehensive disaster recovery (DR) processes that allow the registry to immediately failover to a second (or third) data center in the case of a catastrophic event at the primary site are key. DR sites should be geographically diverse such that proper distance and non-technical diversity (e.g. of political systems) is achieved such that it is nearly impossible for a total outage across all DR sites. DR processes would ideally achieve a recovery point objective (RPO) of zero (i.e. no loss of data or Integrity) and a recovery time objective (RTO) of zero (i.e. immediate recovery or no reduction of Availability). For more on RPO and RTO see Section IV Business Continuity Management, *infra*.

III. EVALUATION OF RISKS TO CPFS IN ELECTRONIC COLLATERAL REGISTRIES

A. IDENTIFYING ESSENTIAL ELEMENTS OF A COLLATERAL REGISTRY DATABASE

The CPFs defined above (see II, III) are relevant to two distinct elements of a collateral registry:

1. A database containing transactional data (registrations); and
2. A database containing information about registry users.

The first element does not include a database for information that many collateral registries collect solely for statistical purposes. Since this information is not publicly disclosed, with the exception of aggregated statistics, it must be secured similarly to the information about the users. The collection of information for statistical purposes is not a universal model, and not contemplated in the UNCITRAL Model Law, so the application of the CPFs to that database is not examined. While these two elements may share similar risks and CPFs, the emphasis of risk management is different for each element, as is the corresponding hierarchy of related CPFs. For example, confidentiality is more of a concern for personal information and user passwords than for the information in registrations. Some registered information may however be confidential (e.g., an industry in which the debtor operates), and upon its entry into the Registry be separated from the other information (e.g., collateral description), in which case Confidentiality (I.B.4) would apply to it. Similarly, Retention (I.B.9) and Integrity (I.B.6) are the primary concerns for transactional data. Both elements of the database require a similar emphasis on Authentication (I.B.2) and Access Control (II.A) before permitting data entry. Thus, the importance of each CPF depends to some extent on the context of the specific data and operations they are applied to. For example, registrations

must be publicly available at all times and be generally accessible, but the registration function may only be accessible to authenticated and authorized persons. Therefore, in the context of searching, Availability (I.B.3) and Accessibility (I.B.1) are far more important factors than Authentication (I.B.2) and Validation (I.B.10). In the context of entering registrations, Availability, Authentication and Validation are important factors that contribute to Integrity (I.B.6). Retention (I.B.9) and Integrity are of prime importance to all stakeholders. Nonetheless, as discussed in more detail below, best practices for information systems risk management dictate that, at a holistic level, the system must manage risk commensurate with the highest level of risk in any of three major risk categories: Confidentiality, Integrity, and Availability. Therefore, before the risk management measures required for a collateral registry may be identified, the risk of non-performance of each CPF in the context of Confidentiality, Integrity, and Availability must be categorized.

B. DEFINING RISK IN ELECTRONIC COLLATERAL REGISTRIES

The risk that the registry won't be able to perform in the manner intended by its designers and expected by its users is inherently difficult to quantify because of its contextual and unpredictable nature – a function of registry implementation, required features, and both the physical and on-line environment that the registry is exposed to over time. As a result, it is generally not possible to reduce risk to zero. Instead, risk management techniques must be adopted to contain risk to an acceptable level. Risk management of an information system has been defined as:

> The process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system, and includes: (i) the conduct of a risk assessment; (ii) the implementation of a risk mitigation strategy; and (iii) employment of techniques and procedures for the continuous monitoring of the security state of the information system.[77]

Within information systems literature, security is often described in terms of a triad of three elements: confidentiality, integrity, and availability (CIA).[78] When any element of

---

[77] U.S. Department of Commerce. *Minimum Security Requirements for Federal Information and Information Systems*, Federal Information Processing Standards (FIPS) Publication 200, March 2006, 17pp. https://doi.org/10.6028/NIST.FIPS.200.

[78] *See e.g.*, Michael Nieles et al., *NIST Special Publication 800-12 Rev 1: An Introduction to Information Security*, NIST (2017), § 1.4. *defining* "Security controls" *as* "The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for a system to protect the *confidentiality, availability, and integrity* of the system and its information." (emphasis added) *and explaining that* "In this document, the terms security controls, safeguards, security protections, and security measures have been used interchangeably. ",

the CIA triad is compromised, the system is insecure. Thus, risk management focusses on assessing and reducing the risk to these three CPFs.

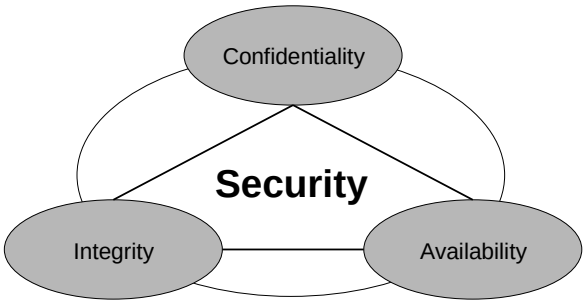

Figure 1: Model of the security triad in information systems.

The three CPFs that form the triad can be considered core CPFs, whose performance is enhanced by, or dependent on the other 12 CPFs:

1. Confidentiality requires: Authentication and Access Control to prevent unauthorized access to confidential information (e.g. a user's personal information should only be accessible by that specific user or as specifically authorized for registry purposes – for example, billing information).
2. Integrity requires: Reliability, Retention, Validation, and in some cases: Authentication, Access Control, and Disposition. Error Correction may be necessary from time to time.
3. Availability requires: Accessibility, Reliability, and Continuity; in certain cases, it may require Interoperability.

Legal Authority provides the rules that define the requirements for the CIA triad. Finally, Legal Authority of the Registrar is necessary to implement some of the duties defined under the registry's legal framework.

Because risk in information systems is difficult to quantify, risk management focuses on the impact that would result if any of the CIA triad elements were compromised. In this context, for example, U.S. federal agencies are required to classify impact as either low,

---

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf (last accessed Feb. 5, 2019); *and see Minimum Security Requirements for Federal Information and Information Systems, Federal Information Processing Standards (FIPS) Publication 200*, NIST (March 2006), at 1, *explaining*, "[t]he generalized format for expressing the security category (SC) of an information system is:
SC information system = {(confidentiality, impact), (integrity, impact), (availability, impact)},
where the acceptable values for potential impact are low, moderate, or high", https://doi.org/10.6028/NIST.FIPS.200 (last accessed Feb. 5, 2019).

moderate, or high for each of the three CIA elements.[79] This categorization must be conducted for each type of information contained in the information system.[80] For example, confidentiality may be categorized as having a high impact on personal user data as mandated by privacy law. By contrast, the impact of confidentiality with regard to notice registrations intended for public searches is low. The required security level for the information system is determined by the highest impact level assigned to any of the three CIA elements for any or the information types contained in the system.[81] For example, if the impact of integrity is considered high for any information type, the system is considered to be a high impact system and must at a minimum employ security controls defined for high impact systems. This is true even if the impact of availability and confidentiality is considered to be low (i.e. the highest impact category of any datatype determines the required security level for the system as a whole). Details of the minimum security requirements that must be implemented for information systems in each of the three impact categories are set out in NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*.[82] For example, all information systems must enforce access control policies that limit access to authorized users.[83] However, testing to identify system vulnerabilities to unauthorized access (penetration testing) is only required for high impact information systems.[84]

C. IDENTIFYING TYPES OF RISKS TO ELECTRONIC REGISTRIES

The NIST FIPS 199 Standards for Security Categorization of Federal Information and Information Systems provides definitions and examples for determining the potential impact and corresponding security category of data contained in an information system based on the expected adverse effects of loss of confidentiality, integrity, or availability.[85] These definitions are adapted for collateral registries in Table 2 below.

Table 2: Classification of Potential Impact

Potential Impact	**Extent of adverse effect on registry**	**Examples of adverse effects that might result**

[79] Standards for Security Categorization of Federal Information and Information Systems - FIPS Pub. 199, at 4 NIST (2004), https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf (last accessed Feb. 8, 2019).
[80] *Id.*
[81] *Id.*
[82] *Recommended Security Controls for Federal Information Systems: Special Publication 800-53*, NIST (2017), App. D., https://csrc.nist.gov/CSRC/media//Publications/sp/800-53/rev-5/draft/documents/sp800-53r5-draft.pdf (last accessed Feb. 8, 2019).
[83] *Id.* at 327.
[84] *Id.* at 328.
[85] FIPS Pub. 199, *supra* note 79.

	operations and assets	
Low	Limited	x) degradation in registry capability to an extent and duration that the registry is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; xi) minor damage to registry assets; or xii) minor financial loss.
Moderate	Serious	i) significant degradation in registry capability to an extent and duration that the registry is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; ii) significant damage to registry assets; or iii) significant financial loss.
High	Severe or catastrophic	i) severe degradation in or loss of registry capability to an extent and duration that the registry is not able to perform one or more of its primary functions; ii) major damage to registry assets; or iii) major financial loss.

Table 3 identifies the result of non-performance for each of the identified CPFs and suggests the level of impact (low, moderate, or high) this may have on an electronic collateral registry. Legal authority (of the Registry and the Registrar) is not included in Table 3 because it is considered foundational and essential to the performance of all other 13 CPFs.

Table 3: Risks and impacts of CPF non-performance

Critical performance factors	Result of non-performance	Impact
1. Access Control	Inability to restrict privileged access and control. This can negatively impact other CPFs including confidentiality, integrity, and reliability (e.g. unauthorized registrations may be submitted).	High
2. Accessibility	Resources within the registry or the entire registry are unavailable.	Moderate to high depending on duration

3. Authentication	Inability to verify users and those with privileged access and control. This can negatively impact other CPFs including confidentiality, integrity, and reliability. (e.g. unauthorized registrations may be submitted).	High
4. Availability	Users are unable to query or submit information to the registry. (In general, electronic collateral registries should be accessible 24 hours a day, every day of the year.[86]).	Moderate to high (occasional brief periods of scheduled unavailability may be acceptable)
5. Confidentiality	Information may be acquired by unintended recipients (e.g. personal user information may be acquired by a third party).[87]	Moderate for user information; low for notices of security interests
6. Continuity	Resources within the registry or the entire registry are unavailable.	Moderate to high depending on duration of unavailability
7. Disposition	Personal user information is retained in the registry beyond time limits mandated by general retention of records law.	Low
8. Error Correction	The quality of the data is corrupted, and a corrective action is not taken promptly.	High
9. Integrity	The quality of the data is corrupted and not accurate.	High
10. Interoperability	The information is unable to be shared with other	Low

[86] For example, *see* Regulations and Procedures for the International Registry § 3.4, ICAO (2016), "The International Registry shall be accessible 24 hours a day, 7 days a week, except if precluded by maintenance performed outside peak periods, or technical or security problems, as set out in the Procedures."

[87] For example, *see* Regulations and Procedures for the International Registry § 4.1, ICAO (2016), "Each registry user entity may elect to exclude from the information generated by a search under Section 7.6 its physical address and administrator's telephone number, and in the case of a natural person, his/her date of birth."

	registries; information from other registries is unable to be accessed.	
11. Reliability	Search results are incomplete.	High
12. Retention	Effective registrations are not returned in a search.	High
13. Timeliness	Registrations are not immediately searchable or effective.	Moderate to High depending on duration
14. Validation	Unable to guarantee that information required to process a registration has been entered.	High

D. CATEGORIZING THE IMPACT RISK OF THREATS TO A REGISTRY

From the above discussion, we can now categorize the CPFs identified for a registry by their role in the CIA triad and the potential impact of their non-performance to the security of the registry. Table 4 groups the CPFs by their relevance to the CIA triad and by impact level.

Table 4: CPFs grouped by relevance to the CIA triad and by impact level

CIA Triad Group	CPF	Impact
Confidentiality	Access Control	High
	Authentication	High
Integrity	Access Control	High
	Authentication	High
	Reliability	High
	Retention	High
	Validation	High
	Error Correction	High
	Disposition	Low
Availability	Reliability	High

	Continuity	High
	Accessibility	Moderate
	Timeliness	Moderate
	Interoperability	Low

Under the NIST framework, a high impact level for any one of the triad groups signals that the registry warrants implementation of high security levels. Therefore, using the impact levels suggested above, the security procedures that a collateral registry should implement under the NIST framework are those listed for high impact information systems in Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*.[88]

E. BROAD CATEGORIZATION OF SOURCES OF THREATS

As earlier identified by the Project, risks may be related to one of three types of events: (i) accidental; (ii) negligent; or (iii) malicious. *Accidental* events in this context relate to those failures that are beyond the control of registry operators. Examples of accidental events may include unforeseeable events caused neither by the Registrar nor its users, such as natural disasters and other types of *force majeure* instances. The next category, *negligent* events, encompass actions (or inaction, as the case may be) of the Registrar to adequately address a foreseeable risk.[89] Finally, *malicious* events are intrusions and attacks on the registry initiated by an internal or external actor. Examples of malicious events include theft of data and denial of service attacks.

The IFC Toolkit emphasizes that data stored in a collateral registry must be secure against all types of threats because it determines priority of competing interests in collateral. Accordingly, the IFC Toolkit emphasizes that registries must adopt a comprehensive security strategy to ensure that registry data is protected, and registry operation is not disrupted. The IFC Toolkit specifically identifies three types of security among those that must be considered when developing a security strategy:[90]

i. security of data against electronic tampering (e.g. firewalls, anti-virus software, user-authentication, control of user and user-group permissions);
ii. security against natural or human-caused disaster (e.g. facility location and physical hardness, fire suppression, continuity of power, regular backup of data to a remote secure facility); and

[88] *Recommended Security Controls for Federal Information Systems*, supra note 82, at App. D.
[89] *See Borg Warner Acceptance Corp. v. Secretary of State*, 240 Kan. 598 (1987).
[90] Secured Transaction Systems and Collateral Registries, *supra* note 1 at 71.

iii. physical security of the registry facility – measures to prevent physical penetration of the registry facility – i.e. controlled access by authorized personnel only (e.g. locks, administrative controls).

For reliability, the IFC Toolkit recommends a configuration with separate web, database, and email servers behind a firewall.[91] Each server should be in a redundant configuration with automatic failover in the event of a server crash.[92]

IV. BUSINESS CONTINUITY MANAGEMENT

A. BCM STANDARDS

Continued operation of a collateral registry must be ensured.[93] The responsibilities of the Registrar include ensuring that any intellectual property rights necessary for Registry operation, such as the patents and copyrights to use and modify the relevant application software or equivalent perpetual licenses, will vest in, or are assignable to a new Registrar. In some cases, this may require the Registrar to acquire rights to modify the software to ensure that the Registry can continue to perform its services and be upgraded as necessary. The World Bank recommends that credit registries develop and routinely test business continuity plans – guidance that is equally cogent for collateral registries.[94]

Business Continuity Management (BCM) involves the processes and procedures for ensuring continued business operations at acceptable predefined levels following a disruptive incident.[95] Some jurisdictions require a plan for handling business-critical operations and regulations and standards often govern the implementation of a BCM plan. [96] BCM standards include: ISO/IEC 27001:2013 Information Security Management Systems; ISO 22301:2012 Societal Security – Business Continuity Management Systems - Requirements; the NFPA 1600: Standard on

[91] *Id.* at 4.1.4.
[92] *Id.*
[93] *See* Regulations and Procedures for the International Registry ¶ 4.176, ICAO (2016), "It is also the responsibility of the Supervisory Authority to ensure that any rights required for the continued effective operation of the International Registry in the event of a change of Registrar will vest in or be assignable to the new Registrar. These would include any intellectual property rights necessary for the continued operation of the Registry."
[94] *Credit Reporting Knowledge Guide 2018*, supra note 36, at 74.
[95] *Data Protection Best Practices*, Storage Networking Industry Association (SNIA) (Oct. 2017), at 28, https://www.snia.org/sites/default/files/DPCO/Data%20Protection%20BP%20White%20Paper%20Final%20v1_0.pdf (last accessed Feb. 8, 2019); and see *ISO 22301:2012, Societal security – Business continuity management systems – Requirements*, ISO (2012) § 3.3.
[96] *Data Protection Best Practices*, supra note 95 at 28.

Disaster/Emergency Management and Business Continuity/Continuity of Operations Programs; and BS 25999, the British Standard for Business Continuity Management.[97]

ISO 22301-2012 defines BCM as a:

> holistic management process that identifies potential threats to an organization and the impacts to business operations those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities.[98]

The scope of ISO 22301:2012 includes "requirements to plan, establish, implement, operate, monitor, review, maintain and continually improve a documented management system to protect against, reduce the likelihood of occurrence, prepare for, respond to, and recover from disruptive incidents when they arise."[99] Integral to a BCM plan are a number of service disruption objectives that are particularly relevant to shaping risk management and BCM plans for collateral registries. Quantifying these objectives will help guide system design that impacts CPFs such as availability, reliability, and retention (e.g. the frequency and extent of data backup operations). The objectives (adapted here for registries) include:

i) MAO: maximum acceptable outage (or MTPD: maximum tolerable period of disruption) – the time it would take for adverse impacts of not providing a registry service to become unacceptable;
ii) MBCO: minimum business continuity objective – the minimum level of registry services that is acceptable during a disruption;
iii) RPO: recovery point objective – the point to which registry data must be restored to enable operation on resumption
iv) RTO: recovery time objective – the period of time following an incident within which a registry service must be resumed (RTO must be less than MAO).[100]

V. OUTSOURCING

A. WHY OUTSOURCE?

In the context of collateral registries, outsourcing is an agreement, between the Registry and a service provider, under which the service provider performs a process, service, or

[97] *Id.*
[98] *ISO 22301:2012*, supra note 95 § 3.5.
[99] *Id.* at 1.
[100] *Id.* §§ 3.25-26, 3.28, 3.44-45*;* see also *Data Protection Best Practices*, supra note 95 at 29.

activity that the Registry would otherwise perform.[101] Outsourcing is a relatively easy way to access new technologies to improve flexibility and efficiency while reducing costs.[102] The economies of scale created by large data centers and cloud services providers may make outsourcing a more cost-effective option than a dedicated secure facility with redundant climate control systems, backup-power generation capabilities and qualified staff. The IFC Toolkit explains that while the government must retain ultimate responsibility for the registry and ownership of registry data, all other aspects of the registry may be outsourced to public or private entities.[103] A number of governments have outsourced the hosting of their collateral registries to the company that developed the collateral registry software. These include the Federated States of Micronesia, Jamaica, the Marshall Islands, Palau, Papua New Guinea, the Solomon Islands, Tonga, and Vanuatu. Under a public-private partnership, a private entity developed, maintains and secures the collateral registries of seven Canadian provinces.[104]

B. OUTSOURCING CONSIDERATIONS

Although outsourcing offers a number of advantages, it also presents data security challenges. This is particularly true of cloud services where the computing and data storage infrastructure may be geographically dispersed.[105] Ultimate responsibility and liability for registry data and operation rests with the Registry. Therefore, oversight of the outsourced services, and verifying that they comply with best practices is paramount. The agreement entered into with the entity providing the outsourced services must establish the required operating standards and procedures to verify compliance.[106] In addition, the obligations and duties of the provider upon contract termination must ensure timely transfer of registry information to the Registry. Additional consideration

---

[101] See *Final Report on EBA Guidelines on Outsourcing Arrangements, European Banking Authority (EBA)*, (2019), at 19, https://eba.europa.eu/documents/10180/2551996/EBA+revised+Guidelines+on+outsourcing+arrangements/38c80601-f5d7-4855-8ba3-702423665479 (last accessed Mar. 6, 2019).

[102] *Id.* at 4.

[103] Secured Transaction Systems and Collateral Registries, *supra* note 1 at 73; similar limits and allowances for outsourcing of IT and fintech services apply to financial institutions, e.g. *see Final Report on EBA Guidelines on Outsourcing Arrangements,* supra note 101 at 6, *explaining*, "The responsibility of the institutions' and payment institutions' management body for the institution or payment institution and all its activities can never be outsourced." *and* "Functions that are considered critical [] may also be outsourced."

[104] New Brunswick, Newfoundland and Labrador, Nova Scotia, and Prince Edward Island formed the initial partnership with UNISYS in 1996, Northwest Territories and Nunavut signed on in 2001, and Yukon joined in 2016, *see* https://www.acol.ca/en/pprs/about/what-is-acol (last accessed Mar. 25, 2019).

[105] *Final Report on EBA Guidelines on Outsourcing Arrangements,* supra note 101 at 14-15.

[106] For example, for many of its cloud services, Amazon Web Services (AWS) has certification for compliance with ISO/IEC 27001:2013, 27017:2015, 27018:2014, and ISO/IEC 9001:2015, *see* https://aws.amazon.com/compliance/iso-certified/ (last accessed Feb. 14, 2019).

must be given at the outset to develop a plan to migrate the system to another service provider upon termination of the outsourcing agreement. For example, will the software developed to be compatible with the initial service provider be compatible with another provider's services?

C. GUIDANCE FROM THE BANKING REGULATOR

The European Banking Authority (EBA) has developed guidelines for outsourcing IT and data services, including cloud services[107] that may be instructive for collateral registries to follow when developing an outsourcing policy. The following subsections highlight some of the EBA guidelines for outsourcing agreements.[108]

1. Governance arrangements

Registries are fully responsible and accountable for complying with all of their regulatory obligations, including outsourced functions.[109] Therefore outsourcing agreements must provide for Registries to make and implement decisions related to outsourced functions as well as to continually monitor service provider performance.[110] Outsourcing agreements must also include appropriate confidentiality provisions regarding registry data and other information.[111]

2. Geographical provisions

Outsourced cloud services may be geographically dispersed and be subject to different laws. Such geographical and jurisdictional dispersal increases the burden and complexity of registry oversight and adding risk.[112] This risk may be mitigated by using a private cloud in a stable jurisdiction. Factors that must be taken into consideration when Registry services (e.g. data storage) are outsourced to service providers in other countries include, i) political stability; ii) data protection laws; iii) insolvency laws applicable in the event of service provider financial failure that might impact urgent recovery of data; and iv) law enforcement provisions and efficacy.[113]

In order to ensure that the Registry can effectively manage outsourced functions, the service agreement should specify where (i.e. regions or countries) the services will be provided and where Registry data will be stored or processed.[114]

---

[107] See generally, *Final Report on EBA Guidelines on Outsourcing Arrangements,* supra note 101.
[108] The selection of guidelines highlighted here is by no means comprehensive.
[109] See *Final Report on EBA Guidelines on Outsourcing Arrangements,* supra note 101, § 35.
[110] *Id.*, § 40.a., 75.h.
[111] *Id.*, § 40.d.
[112] *Id.*, § 67
[113] *Id.*, § 68.
[114] *Id.*, § 75.f.

3. Sub-outsourcing

Sub-outsourcing occurs when the contracted provider of outsourced services further outsources the provision of a service to another service provider.[115] Sub-outsourcing complicates the Registry's task of overseeing outsourced services by increasing the number of service providers that the Registry must evaluate and monitor. Sub-outsourcing also increases the likelihood of geographical and jurisdictional dispersal of outsourced services. This is especially true for chains of sub-outsourcing, where one or more sub-outsourcers further sub-outsource to other service provider(s).[116] If the service agreement does permit sub-outsourcing, the agreement should require the service provider to: i) obtain prior authorization from the Registry before sub-outsourcing data; and ii) oversee any sub-outsourced services to ensure that the primary service provider's contractual obligations to the registry are continuously satisfied.[117] The Registry should only authorize sub-outsourcing to entities that agree to i) comply with all applicable laws, regulations, and contractual obligations; and ii) grant the Registry the same contractual rights of access and audit as those granted by the primary service provider.[118]

4. Evaluating, monitoring, and auditing

Registries must perform due diligence evaluations of service providers before entering into an outsourcing agreement. Service provider criteria that should be evaluated include, business reputation, expertise, resources (including personnel, financial, IT infrastructure, and IP licenses), and regulatory compliance.[119] If the outsourcing includes processing or storing confidential data, the service provider must have appropriate policies and procedures in place.[120]

The service agreement must provide for ongoing monitoring and management of outsourcing arrangements including evaluation of the CPFs identified in sections I and II *supra* (e.g. Confidentiality, Integrity, and Availability).[121] The service agreement should grant the Registry and its agents i) full access to all relevant facilities (e.g. head offices and operation centers), including all relevant devices, systems, networks, information, and data used for providing the outsourced function, including related financial information, personnel, and the service provider's external auditors; and ii) unrestricted rights of inspection and auditing related to the outsourcing arrangement, to

[115] *Id* §§ 12, 42.d(ii).
[116] *Id.*, § 67
[117] *Id.*, § 78.c-d.
[118] *Id.*, § 79.
[119] *Id.*, § 70.
[120] *Id.*, § 72.
[121] *Id.*, § 100.

enable them to monitor the outsourcing arrangement and to ensure compliance with all applicable regulatory and contractual requirements.[122]

The service provider should be required to provide regular reports on service delivery, and of any certifications, reviews, or audits.[123] The agreement should also require the service provider to notify the Registry of any changes in its financial position, ownership, or organizational structure.[124]

5. Termination

As part of business continuity management, Registries must maintain a plan to handle termination of an outsourcing agreement. The plan must ensure that, within an appropriate time after termination, the Registry will be able to perform the outsourced functions itself or transfer them to alternate service providers.[125] Therefore, outsourcing agreement provisions must provide that data owned by the Registry can be accessed in the case of the insolvency, or discontinuation of the service provider's operations.[126]

Registries should take appropriate corrective or remedial action following any indications of inadequate performance or noncompliance with applicable laws and regulations.[127] Such action may include terminating the outsourcing agreement, with immediate effect, if necessary.[128]

VI. TRUSTWORTHINESS AND ASSURANCE

A. TRUSTWORTHINESS

The Project had previously identified trustworthiness as an essential element of a registry, which is of a paramount importance in the context of collateral registries. A collateral registry is trustworthy if it fulfills its required functions, including the CPFs identified above.[129] Trustworthiness includes two primary components: functionality and assurance. Functionality embodies the features, functions, and services provided by the registry.[130]

---

[122] *Id.*, § 87.
[123] *Id.*, § 104.
[124] *Id.*, § 42.d(ii).
[125] *Id.*, §§ 40.f., 42.c.
[126] *Id.*, § 75.m.
[127] *Id.*, § 105.
[128] *Id.*
[129] See *Special Publication 800-53, supra* note 82, § 2.6 discussing assurance and trustworthiness in the context of security and privacy controls for information systems.
[130] *Id.*

B. ASSURANCE

Assurance is the measure of confidence that registry functionality is implemented correctly, operating as intended, and producing the desired result.[131] Trustworthiness of systems, including their components and services, is recognized as an important part of risk management.[132] Assurance assessments generate relevant and credible evidence about the functionality and behavior of the registry and identify the elements of the registry that produced the evidence. This evidence determines the level of confidence in registry functionality.[133] The evidence collected by the assessment also facilitates the important process of continuous improvement by identifying which elements of the registry require improvement.[134] Regular assessments are essential to achieving the goal of continuous improvement and staying abreast of developing technology and evolving threats.

C. INDEPENDENT AUDITS

It is not enough for the registry simply to declare itself trustworthy – an objective process of certification is required.[135] Providing users with the results of objective audits and certification that the registry meets international best practice standards not only provides assurance, it creates transparency and engenders trust among registry users.[136] ISO/DIS 16363:2012 - *Space Data and Information Transfer Systems - Audit and Certification of Trustworthy Digital Repositories* defines procedures suitable for objectively auditing and certifying the trustworthiness of registries.[137] A regular cycle of audits and certification is required to maintain trustworthy status.[138] Where the registry can demonstrate that it has implemented practices required by related standards, this may serve to satisfy similar requirements of the audit (e.g. employing the codes of practice found in the ISO 27000 series of standards).[139]

The scope of ISO 16363 is broad, it encompasses the IT system, including hardware, software, communications equipment and firewalls as well as supporting physical infrastructure, personnel, management and administrative procedures.[140] This includes, among others, fire protection and flood detection systems, as well as management procedures to assess staff skill levels relative to evolving relevant technology, and the

---

[131] *Id.*
[132] *Id.*
[133] *Id.*
[134] *Space Data and Information Transfer Systems - Audit and Certification of Trustworthy Digital Repositories (BS ISO 16363:2012)*, ISO (2012) at § 1.6.
[135] *Id*. at § 1.3.
[136] *Id.* at § 2.1.
[137] *Id.* at § 1.1, stating that the scope of the document is "the entire range of digital repositories."
[138] *Id.* at § 2.1.
[139] *Id.* at § 5.2.
[140] *Id.*

registry's intellectual property rights practices.[141] Disaster preparedness and recovery plans are also assessed.[142]

[141] *Id.*
[142] *Id.* § 5.2.4.

ANNEX I - CPF RISK MITIGATION STANDARDS

A. MITIGATIONS OF RISKS

It is insufficient to merely implement a number of safeguards with the expectation that this will manage all risks. Linkov et al identify four management stages within resilience in information systems:[1]

1. *Plan*: Have a strategy by which to keep services during failure of one or more components.
2. *Absorb*: Maintain a minimally functional service while isolating disruption.
3. *Recover*: Have an ability to restore each component to its original state.
4. *Adapt*: Use the knowledge learned from the event to address the risk.

The NIST identifies 17 security-related areas for which policies and procedures must be developed to protect information systems.[2] Each of these policies and procedures relate to one or more of the above four management stages and are adapted here for collateral registries:[3]

(i) **access control**: limiting access, for submitting data to the Registry, to authorized users;
(ii) **awareness and training**: to ensure that registry personnel are a) aware of the security risks and applicable laws associated with their activities; and b) adequately trained to carry out their duties and responsibilities;
(iii) **audit and accountability**: a) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and b) ensure that the actions of information system users can be uniquely traced to those users so they can be held accountable for their actions;
(iv) **certification, accreditation, and security assessments**: a) periodically assess the security controls to determine if the controls are effective; b) develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities; and c) monitor security controls on an ongoing basis to ensure their continued effectiveness;
(v) **configuration management**: a) establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation); and b) establish and enforce security configuration settings;
(vi) **contingency planning**: establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery to ensure availability and continuity of operations in emergency situations;
(vii) **identification and authentication**: identify registry users and authenticate the identities of those users as a prerequisite to allowing access to the registry;

[1] Linkov, I., Eisenberg, D. A., Plourde, K., Seager, T. P., Allen, J., and Kott, A. Resilience metrics for cyber systems. Environment Systems and Decisions 33, 4 (2013), 471–476.
[2] U.S. Department of Commerce. *Minimum Security Requirements for Federal Information and Information Systems*, Federal Information Processing Standards (FIPS) Publication 200, March 2006, 17pp. https://doi.org/10.6028/NIST.FIPS.200.
[3] *Id.*

(viii) **incident response**: a) establish an operational incident handling capability that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and b) track, document, and report incidents to appropriate registry officials and/or authorities;

(ix) **maintenance**: a) perform periodic and timely registry maintenance; and b) provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct registry maintenance;

(x) **media protection**: a) protect information system media; and b) sanitize or destroy information system media before disposal or release for reuse;

(xi) **physical and environmental protection**: a) limit physical access to information systems, equipment, and the respective operating environments to authorized individuals; b) protect the physical facility and support infrastructure for the registry; c) provide supporting utilities for the registry; d) protect information systems against environmental hazards; and e) provide appropriate environmental controls in facilities containing information systems;

(xii) **planning**: develop, document, periodically update, and implement security plans that describe the security controls in place, and the rules of behavior for individuals with access to the registry;

(xiii) **personnel security**: a) ensure that individuals occupying positions of responsibility within registry organizations (including third-party service providers) are trustworthy and meet established security criteria for those positions; b) ensure that organizational information and information systems are protected during and after personnel actions such as terminations and transfers; and c) employ formal sanctions for personnel failing to comply with organizational security policies and procedures;

(xiv) **risk assessment**: periodically assess the risk to registry operations (including mission, functions, or reputation), registry assets (including, among others, facilities, auxiliary power systems, heating, ventilating and air-conditioning (HVAC) equipment, hardware software, data, IP rights), and individuals, resulting from the operation of the registry and the associated processing, storage, or transmission of registry information;

(xv) **systems and services acquisition**: a) allocate sufficient resources required to operate, maintain, and secure the registry; b) employ system development life cycle processes that incorporate information security considerations; c) employ software usage and installation restrictions; and d) ensure that third-party providers employ adequate security measures to protect information, applications, and/or services outsourced from the registry;

(xvi) **system and communications protection**: a) monitor, control, and protect registry communications (i.e., information transmitted or received by the registry) at its authorization boundaries (e.g. by using routers and firewalls to protect connections to the Internet); and b) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within the registry; and

(xvii) **system and information integrity**: a) identify, report, and correct information and registry flaws in a timely manner; b) provide protection from malicious code at appropriate locations within the registry; and c) monitor information system security alerts and advisories and take appropriate actions in response.

Procedures and policies addressing each of these topics are detailed in NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*.[4]

B. IDENTIFICATION OF RELEVANT STANDARDS

Standards for technical implementation are divided by subject matter and functionality. Modern collateral registries comprise record management, networking, and cloud computing services in order to make the electronic registry usable for remote users. Standards related to any of these areas are therefore relevant to collateral registries. The International Standards Organization (ISO) develops widely adopted standards through consultation of a broad range of experts. The process is guided by technical committees that oversee the review and update of these standards. Of particular note for information systems are the ISO27001 series of standards.

The National Institute of Standards and Technology (NIST) in the United States has developed a series of standards and publications addressing information systems security. The NIST is responsible for developing information security standards and guidelines for federal information systems.[5] Within NIST, the Information Technology Laboratory (ITL) is responsible for the development of management, administrative, technical, and physical standards and guidelines for cost-effective security of information and protection of individuals' privacy in federal information systems (other than national security-related systems).[6] The 800-series Special Publications (SP) include ITL's guidelines for information systems security.[7] Topics on information systems security covered by IS/IEC 27001 can generally be found in SP 800-53.[8]

The NIST handbook on information security (SP 800-100) details issues related to staff responsibilities, staff training, service agreements with vendors, risk assessment, incident response and is presented in a less technically formal style, as compared to ISO27001.[9] This may help registry operators and designers in addition to the adoption of a recognized standard.

Cybersecurity addresses similar threats to information security, but focusses on external threats.[10] NIST's Cybersecurity Framework (CSF) is especially helpful as a guide to establishing, or strengthening, cybersecurity procedures around a core framework of five concurrent and continuous functions: "Identify, Protect, Detect, Respond, Recover."[11] The CSF is technology neutral and relies on existing global standards, guidelines, and practices that evolve

---

[4] *Recommended Security Controls for Federal Information Systems: Special Publication 800-53*, NIST (2017), App. D., https://csrc.nist.gov/CSRC/media//Publications/sp/800-53/rev-5/draft/documents/sp800-53r5-draft.pdf (last accessed Feb. 8, 2019).
[5] *Id.* at i.
[6] *Id.* at ii.
[7] *Id.*
[8] *See Framework for Improving Critical Infrastructure Cybersecurity: Version 1.1*, NIST (2018), at Table 2: Framework Core, *citing* ISO/IEC 27001:2013 and NIST SP 800-53 Rev. 4, https://doi.org/10.6028/NIST.CSWP.04162018 (last visited Mar. 4, 2019).
[9] Information Security Handbook: A Guide for Managers - NIST Special Publication 800-100, NIST, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-100.pdf (last accessed Feb. 13, 2019).
[10] *See ISO/IEC TR 27103:2018(en)* at Intro.
[11] *Framework for Improving Critical Infrastructure Cybersecurity*, supra note 8, at 3.

with technology and business requirements.[12] The five core functions are intended to be carried out concurrently and continuously to adaptively respond to the dynamics of cybersecurity risk.[13] The five functions develop attributes necessary for an organization to address cybersecurity risk:

i) *Identify* develops the necessary understanding to manage cybersecurity risk;
ii) *Protect* develops and implements appropriate safeguards to ensure service delivery;
iii) *Detect* develops and implements processes to identify the occurrence of a cybersecurity event;
iv) *Respond* develops and implements responses to detected events; and
v) *Recover* develops and implements plans to maintain resiliency and restore services impaired by cybersecurity incidents.[14]

Each function is divided into categories and subcategories. The CSF provides references to the relevant sections of multiple international and NIST standards for each subcategory.[15] For example *Protect* is divided into six categories which are further divided into subcategories (e.g. "Remote access" is one of seven subcategories under the *Protect* category named "Identity management, authentication and access control").[16] For each subcategory, the CSF provides citations to specific sections of relevant standards which generally include, among others, ISO/IEC 27001:2013 and NIST SP 800-53 Rev. 4.[17] The CSF is available as a free download from the NIST website in English, Spanish, and Arabic.[18]

The ISO standard, ISO/IEC TR 27103:2018 is similar to the CSF – it "provides guidance on how to leverage existing standards in a cybersecurity framework."[19] ISO/IEC TR 27103:2018 incorporates a framework of the same five core functions as the CSF: *Identify*, *Protect*, *Detect*, *Respond*, and *Recover*.[20] The ISO standard's core functions include many of the same categories as the CSF.[21]

Table 5: List of standards used in assessment of CPFs.

Category	**Standard**	**Scope**
Record management	ISO 15489-1:2001 [2]	Records management
	ISO/IEC 9798 [11]	Entity authentication
	ISO/TR 13028:2010 [12]	Digitization of records

[12] *Id.* at 2.
[13] *Id.* at 7.
[14] *Id.* at 7-8.
[15] *See Id.* at Table 2: Framework Core.
[16] *Id.* at 29.
[17] *Id.*
[18] *See* https://www.nist.gov/cyberframework/framework (last accessed Mar. 4, 2019).
[19] *See https://www.iso.org/standard/72437.html* (last accessed Mar. 4, 2019).
[20] *ISO/IEC TR 27103:2018(en),* supra note, 10, at § 6.2.
[21] *Id.* at Annex A.

	ISO/TR 17068:2012 [13]	Trusted third party repository for digital records
	ISO 13008:2012 [1]	Migration of records
Information security	ISO/IEC 27001 [7]	Information security management
	ISO/IEC 38500:2015 [10]	IT governance
	NIST Cybersecurity Framework (CSF)	Critical infrastructure cybersecurity
	NIST SP 800-53	Security and Privacy Controls
	NIST SP 800-100 [15]	Information security and response
	NIST SP 800-160	Systems Security Engineering
	NIST FIPS PUB 199	Standards for Security Categorization
	NIST FIPS PUB 200	Security Requirements
Networking	RFC 2196 [14]	Secure development of information systems connected to the internet
	ISO/IEC 27033-3:2010 [8]	Network security

C. Limitations of Technical Standards

As previously noted by the Project, there is a tremendous amount of value in utilizing standards, but they are not without their limitations. For example, a caveat of the ISO 27000 family of standards is that the determination of which controls a user should implement is based on the user's own assessment of risk and the user's selection of controls to address the risks it identified.[22] Certification of compliance with the standard is achieved through an audit of the implementation and effectiveness of the selected controls rather than an analysis of the risk assessment and choice of controls.[23] Thus, the standard offers the advantages of a flexible approach but relies on the user's expertise in risk assessment and security to develop an appropriate solution.[24] Applying the standard to a less than optimal solution would only result in a false sense of security. As the British Computer Society (BCS) points out, "it is perfectly possible to be fully compliant with the standard, but be insecure."[25] Reliance on standards as a

[22] *ISO 27002: Information Technology, Security Techniques, Code of Practice for Information Security Management*, ISO, 2005.
[23] *Id.*
[24] *Why ISO 27001 Is Not Enough* (BCS, 2009), https://www.bcs.org/content/ConWebDoc/2659 (last accessed Feb. 27, 2019).
[25] *Id.*

single, exhaustive measure by which to achieve a state of best practice overlooks the need to follow up their deployment by monitoring and evaluating their effectiveness in order to refine, adapt, and develop the optimal strategy for each registry.

Insight offered by senior officials at the International Registry (IR) after its first seven years of operation is instructive on this point: "the three main risks to the IR are complacency, human error and unknown technology assumptions. The nature of the data stored in the IR database means that unrecognised errors are of most concern, the 'unknown unknowns.'"[26] Steps taken by the IR to address these risks, include, among others, employing independent expert information and communications technology (ICT) security consultants to validate the adequacy of security measures through an annual security audit followed, six months later, by a progress review of issues raised by the audit.[27]

D. INFORMATION SECURITY CONTINUOUS MONITORING (ISCM)

Ongoing monitoring of information security is a critical component of risk management.[28] Information security does not end with the installation of hardware or software, or by announcing a security policy.[29] Instead, continuous monitoring and management is required to protect the confidentiality, integrity, and availability of information.[30] With evolving technology come new threats and vulnerabilities that must be identified and addressed.[31] Information Security Continuous Monitoring (ISCM) is defined as "maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions."[32] NIST Special Publication 800-137 offers guidelines to assist organizations develop an ISCM strategy and implement an ISCM program to monitor threats and vulnerabilities, and the effectiveness of deployed security controls.[33] A registry's ISCM strategy must be based on a clear understanding of security risks that the registry faces and provide meaningful metrics of security effectiveness and compliance with the registry's requirements, including regulations, policies, goals, and standards.[34] By providing actionable information on security status, an effective ISCM program advances the registry from compliance-driven risk management to data-driven risk management.[35]

---

[26] Rob Cowan & Donal Gallagher, The International Registry For Aircraft Equipment—The First Seven Years, What We Have Learned, 45 UCC L. J. 225, 249 (2014), https://www.aviareto.aero/wp-content/uploads/2015/03/UCCLJ-Volume-45-No3-Cowan-Gallagher.pdf (last accessed Feb. 8, 2019).
[27] *Id.* at 249, 253.
[28] Kelley Dempsey et al., *NIST Special Publication 800-137: Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, NIST (2011), at vi, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-137.pdf (last accessed Mar. 1, 2019.
[29] Michael Nieles et al., *NIST Special Publication 800-12 Rev 1: An Introduction to Information Security*, NIST (2017), § 2.7, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf (last accessed Feb. 5, 2019).
[30] *Id.*
[31] *Id.*
[32] Dempsey et al, *supra* note 28.
[33] *Id.* at 3.
[34] *Id.* at vi.
[35] *Id.* at vii.

E. BEST PRACTICES RECOMMENDED BY INDUSTRY

A recent survey of 453 database professionals in 40 countries found that 42% followed published best practices but also developed their own.[36] Another 33% partially followed best practice guidelines.[37] Most of the respondents had worked for more than ten years in the database field; 40% were based in the U.S. and 33% in the U.K.; more than half worked for organizations with over 500 employees.[38] The survey found that two common sources of best practices were software vendors' websites and industry whitepapers.[39] For sources of best practices, 27% always used software vendors' websites while 68% sometimes used them; 21% of respondents always used industry whitepapers and 73% sometimes used them.

Industry organizations often develop and publish best practices for their industry or segment of interest. Examples include the Storage Networking Industry Association (SNIA) and the Data Management Association (DAMA). Some vendors and manufacturers also publish best practices that may be specific to their products or more general, but targeting markets that their products serve. Examples include Microsoft and Amazon Web Services (AWS). Some of the best practices recommended by these industry publications reference international standards such as those promulgated by ISO and IEC. Other best practices published by manufacturers are specific to configuration and installation of specific products. The value of these publications being that following the manufacturer's recommendations is generally a best practice – keeping in mind that selection of the appropriate product remains the registry designer's responsibility. Examples of industry publications of best practices are listed below in Table 6.

Table 6: Examples of industry publications

Publisher	**Title**
Amazon Web Services	AWS Security Best Practices (2016)[40]
	Architecting for the Cloud: Best Practices (2018)[41]
Data Management Association (DAMA)	DAMA Guide to the Data Management Body of Knowledge (DAMA-DMBOK Guide) (2017)[42]
Storage Networking Industry Association (SNIA)	Data Protection Best Practices (2017)[43]

[36] Victoria Holt et al, *The Usage of Best Practices and Procedures in the Database Community*, *Information Systems*, 49 (2015) 163–181, http://dx.doi.org/10.1016/j.is.2014.12.004 (last accessed Jan. 31, 2019).
[37] *Id.*
[38] *Id.*
[39] *Id.*
[40] AWS Security Best Practices, AWS (2016), https://d1.awsstatic.com/whitepapers/Security/AWS_Security_Best_Practices.pdf (last accessed Feb. 14, 2019).
[41] *Architecting for the Cloud: Best Practices*, AWS (2018), https://d1.awsstatic.com/whitepapers/AWS_Cloud_Best_Practices.pdf (last accessed Feb. 14, 2019).
[42] *See* https://dama.org/content/body-knowledge (last accessed Feb. 14, 2019).
[43] *Data Protection Best Practices*, Storage Networking Industry Association (SNIA) (Oct. 2017) https://www.snia.org/sites/default/files/DPCO/Data%20Protection%20BP%20White%20Paper%20Final%20v1_0.pdf (last accessed Feb. 8, 2019).

F. SOAP – An Example of a Widely Adopted Implementation Standard

SOAP (Simple Object Access Protocol) is a communication protocol that allows disparate systems to communicate securely using XML (Extensible Markup Language) for SOAP based web-services.[44] SOAP is widely used for secure communications by internet accessible information systems, including collateral registries.[45] The Web services Security (WS-Security) standard specification defines how SOAP based web-services should be implemented to protect against external attacks and ensure communication confidentiality, integrity, and authentication[46] The WS-Security standard uses signatures (defined in the XML Signature standard) to secure certain parts of SOAP messages.[47] The signatures provide assurance that the message has not been manipulated during transmission (integrity) and authenticate the sender (authentication).[48] The WS-Security standard also provides communication confidentiality using encryption; only the intended recipient of the message is able to read it.[49] Finally, the WS-Security standard uses timestamps to limit message validity for a short period of time so that they cannot be resent as part of an attack on the system.[50]

ANNEX 2 – LIABILITY OF REGISTRARS/FILING OFFICERS

U.S. UCC 9 PROVISIONS

California:

§ 9-524: Delay by the filing office beyond a time limit prescribed by this chapter is excused if both of the following conditions are satisfied:

> (1) The delay is caused by interruption of communication or computer facilities, war, emergency conditions, failure of equipment, or other circumstances beyond control of the filing office.
>
> (2) The filing office exercises reasonable diligence under the circumstances.

Kansas:

---

[44] *See* https://docs.oracle.com/cd/A97335_02/integrate.102/a90297/overview.htm#1007693 (last accessed Mar. 1, 2019).
[45] Communication by the author with Bsystems (Ghana), Feb. 27, 2019.
[46] *See generally* https://www.oasis-open.org/committees/download.php/16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf (last accessed Mar. 1, 2019).
[47] *Id.* at 35.
[48] *Id.*
[49] *Id.* at 51.
[50] *Id.*

§ 9-523(f): Immunity for filing officers. Except with respect to willful misconduct, the state, counties and filing officers are immune from liability for damages resulting from errors or omissions in information supplied pursuant to this act.

Nebraska:

§ 9-528(b): Officials, employees, and agents of the filing office are exempted from all personal liability as a result of any error or omission in providing information as required by this part except in cases of willful misconduct or gross negligence.

Wisconsin:

§ 9-523(7) Liability of filing officer. No filing officer nor any of the filing officer's employees or agents shall be subject to personal liability by reason of any error or omission in the performance of any duty under this chapter except in case of misconduct as defined in s. 946.12.

AUSTRALIA PERSONAL PROPERTY SECURITY ACT (PPSA):

§ 272 Liability for damages

Despite section 271, none of the following persons is liable to an action, suit or proceeding for damages for, or in respect of, anything done honestly, or honestly omitted to be done, in the exercise, or purported exercise, of any power conferred by this Act or the regulations:

(a) the Commonwealth;

(b) the Registrar, or a delegate of the Registrar;

(c) a Deputy Registrar;

(d) the Minister;

(e) a Minister of a State or Territory, or another authority of a State or Territory, in relation to the exercise or performance of a power, duty or function pursuant to an agreement made for the purposes of section 118 (proceeding as if personal property were land);

(f) a member of the Registrar's staff;

(g) a person who is acting as a member of the Registrar's staff;

(h) a person who is authorised to perform or exercise a function or power of, or on behalf of, the Registrar.

SASKATCHEWAN PPSA:

§ 52(1) A person may bring an action against the Crown to recover loss or damage suffered by that person because of an error or omission in the operation of the registry if the loss or damage resulted:

(a) from reliance on a printed search result issued by the registry; or

(b) except as provided in subsections 42.4(2) [lawful suspension of registry functions], 43(3) [not filing a financing statement if fees not paid] and 43(10) [rejection of noncompliant financing statement] and section 43.1, from the failure of the registrar to register a printed financing statement submitted for registration pursuant to section 43.

(2) The Crown or any person acting on behalf of the Crown is not liable, directly or vicariously, for loss or damage suffered by a person because of:

(a) oral advice given by an agent or employee of the Crown with respect to this Act, the regulations or the operation of the registry, unless the person who brings the actions proves that the agent or employee was not acting in good faith; or

(b) a failure to register, or to register correctly, a financing statement in the form of electronic data that is transmitted to the registry for the purpose of effecting a registration.

(4) Except as otherwise provided in this Act, no action or proceeding lies or shall be commenced against the Crown, the minister, the registrar, any deputy registrar, any other person authorized to act on behalf of the registrar pursuant to subsection 42.2(6) or any employee of the Crown if that person is acting pursuant to the authority of this Act, the regulations or any other Act, for anything in good faith done, caused or permitted or authorized to be done, attempted to be done or omitted to be done by that person or by any of those persons pursuant to or in the exercise or supposed exercise of any power conferred by this Act, the regulations or any other Act or in the carrying out or supposed carrying out of any responsibility imposed by this Act, the regulations or any other Act.

§ 54 Payment of claim for loss

54(1) The total amount recoverable in a single action pursuant to section 52, and the total amount recoverable for all claims in a single action pursuant to section 53, shall not exceed a prescribed amount.

(2) Where damages are paid to a claimant pursuant to section 52 or 53, the Crown is subrogated to the rights of the claimant against any person indebted to the claimant whose debt to the claimant was the basis of the loss or damage with respect to which the claim was paid.

(3) Where a claimant recovers pursuant to section 52 or 53 an amount that is less than the value of the interest the claimant would have had if the error or omission had not occurred, the right of subrogation pursuant to subsection (2) does not prejudice the right of the claimant to recover in priority to the Crown an amount equal to the difference between the amount paid to the claimant and the value of the interest the claimant would have had if the error or omission had not occurred.

(4) The Crown may, without action being brought, pay the amount of a claim against the Crown when authorized to do so by the minister on the report of the registrar setting out the facts and the opinion of the registrar that the claim is just and reasonable.

(5) Subject to subsection (1), where an award of damages has been made in favour of a claimant and the time for appeal has expired, or where an appeal is taken and it is disposed of in whole or in part in favour of the claimant, the Crown shall pay the amount specified in the judgment in a manner specified in the judgment, including the costs of the claimant if the judgment so provides.

ONTARIO PPSA:

Protection from personal liability

§ 42(5) No action or other proceeding for damages shall be instituted against the registrar or any person employed in the Ministry of Consumer and Business Services for any act done in good faith in the execution or intended execution of the person's duty under this Act or the Repair and Storage Liens Act or for any alleged neglect or default in the execution in good faith of the person's duty thereunder.