



**United Nations Commission
on International Trade Law**
Working Group VI (Security Interests)
Twenty-third session
New York, 8-12 April 2013

Draft Technical Legislative Guide on the Implementation of a Security Rights Registry

Note by the Secretariat

Addendum

Contents

	<i>Paragraphs</i>	<i>Page</i>
Introduction (<i>continued</i>)		3
D. Overview of secured transactions law and the role of registration (<i>continued</i>)	1-23	3
6. Extended transactional scope of the registry	1-5	3
7. Registration and enforcement of security rights	6	4
8. Conflict-of-laws considerations	7-8	5
9. Notice registration	9-17	5
10. Coordination with specialized movable property registries	18-20	7
11. Coordination with immovable property registries	21-23	8
E. Transitional considerations	24-33	9
I. Establishment and functions of the security rights registry	34-49	10
A. General remarks	34-49	10
1. Establishment of the registry	34	10
2. Appointment of the registrar	35	10



3.	Functions of the registry	36	11
4.	Additional implementation considerations	37-39	11
5.	Registry terms and conditions of use	40-41	12
6.	Electronic or paper-based registry	42-49	12
B.	Recommendations 1-3		14
II.	Access to registry services	50-65	14
A.	General remarks	50-65	14
1.	Public access	50-51	14
2.	Operating days and hours of the registry	52-54	14
3.	Access to registration services	55-58	15
4.	Verification of identity, evidence of authorization or scrutiny of the content of the notice not required	59-61	16
5.	Access to search services	62-65	17
B.	Recommendations 4-10		18

Introduction (*continued*)

D. Overview of secured transactions law and the role of registration (*continued*)

6. Extended transactional scope of the registry

(a) Outright assignments

1. As already explained (see A/CN.9/WG.VI/WP.54, paras. 18-20), the secured transactions law contemplated by the *Secured Transactions Guide* is comprehensive in scope, covering all consensual transactions that in substance function to secure an obligation regardless of the formal character of the secured creditor's property right, the type of encumbered asset, the nature of the secured obligation or the status of the parties (see *Secured Transactions Guide*, chap. I, paras. 101-112, and recs. 2 and 10).

2. The *Secured Transactions Guide* recommends that the secured transactions law (with the exception of the rules governing enforcement on default) should also apply to outright assignments of receivables. Bringing such outright assignments within the scope of the secured transactions law does not mean that outright assignments are re-characterized as secured transactions. Rather, it is intended to ensure that an outright assignee of receivables is subject to the same rules relating to creation, third-party effectiveness and priority as the holder of a security right in receivables. It also ensures that the outright assignee has the same rights and obligations vis-à-vis the debtor of the receivable as a secured creditor (see *Secured Transactions Guide*, chap. I, paras. 25-31, and recs. 3 and 167).

3. Under this approach, an assignee generally will have to register a notice of its right in the security rights registry for the assignment to be effective against third parties that have claims against the assignor; and priority among the rights of successive competing assignees or secured creditors that have acquired rights in the same receivables from the same assignor/grantor will generally be determined by the order of registration (see *Secured Transactions Guide*, chap. III, para. 43). This approach recognizes that outright assignments of receivables not only perform a financing function but also create the same problem of information inadequacy for third parties as security rights in receivables. Unless a notice is registered in the security rights registry as a condition of third-party effectiveness, a potential secured creditor or assignee, or other third party would have no efficient means of verifying whether the receivables owed to a business have already been made subject to a security right or an assignment. While inquiries could be made of the debtors of the receivables, this is not practically feasible if they have not been notified of the assignment or if the transaction covers not only present but also future receivables generally.

(b) Other non-security transactions

4. True long-term leases and consignment sales of movable assets do not operate to secure the acquisition price of assets and consequently do not qualify as security rights so as to fall within the secured transactions law contemplated by the *Secured Transactions Guide*. However, they create the same information inadequacy concerns for third parties as non-possessory security rights, since they necessarily

involve a separation of a property right (the ownership of the lessor or consignor) from actual possession (which is with the lessee or consignee). To address this concern, some States expand the scope of their secured transactions regime (other than the enforcement rules) as it applies to acquisition security rights to these types of transaction. In addition to providing adequate information to third parties, this approach also diminishes the risk of litigation concerning whether a transaction in the form of a lease or a consignment is functionally a secured transaction. As such, a lease or a consignment would be: (a) ineffective against third parties if a notice with respect to it was not registered; or (b) subordinate in priority if the lessor or consignor did not comply with the requirements for obtaining the special priority given to acquisition security rights. The *Secured Transactions Guide* discusses but makes no recommendation on this matter (see *Secured Transactions Guide*, chap. III, para. 44). It may be noted, however, that, a lessor or a consignor can always register a precautionary notice, if it is concerned that its right might be characterized as a security right under the functional concept of security recommended in the *Secured Transactions Guide*, and thus lose its third-party effectiveness or priority status.

5. Some legal systems go even further and require registration of a notice with respect to preferential claims (for a discussion of the related topic of the priority status of preferential claims, see A/CN.9/WG.VI/WP.54, para. 52). The rationale underlying this approach is that, in the absence of registration, it will typically be difficult or impossible for prospective creditors to know whether preferential claims exist, a circumstance that is likely to increase uncertainty and thereby discourage secured credit. The *Secured Transactions Guide* does not recommend this approach. Even registered preferential claims can adversely affect the availability and the cost of secured credit when they are given priority over pre-registered security rights, as preferential claims diminish the economic value of an asset to a secured creditor, who will often shift the economic burden of such claims to the grantor by increasing the interest rate or by withholding the estimated amount of such claims from the available credit (see *Secured Transactions Guide*, chap. V, paras. 90-93).

7. Registration and enforcement of security rights

6. Some legal systems require secured creditors to register in the general security rights registry a notice that they have initiated or propose to initiate an enforcement action. The goal of this approach is to enable the security rights registry to notify third parties that have registered a notice with respect to a competing right in the same encumbered assets of the details of the pending enforcement. The *Secured Transactions Guide* does not recommend this approach. Instead, the *Secured Transactions Guide* recommends that the enforcing secured creditor should be required to search the registry and send out the required notices to interested third parties (including competing claimants) of the particular enforcement remedy that the enforcing secured creditor seeks to exercise (see *Secured Transactions Guide*, rec. 151). Such notification is intended to provide interested third parties (such as a secured creditor with a lower priority ranking than that of the enforcing secured creditor, a guarantor or a co-owner of the encumbered assets) with an opportunity to monitor the enforcement proceedings, bid at any sale, or remedy the default that has given rise to the enforcement proceeding.

8. Conflict-of-laws considerations

7. Where a secured transaction is connected to more than one State, secured creditors and third parties need clear guidance as to which State's law applies. Under the conflict-of-laws recommendations of the *Secured Transactions Guide*, the law applicable to the creation, third-party effectiveness and priority of a security right in tangible assets is the law of the State in which the encumbered asset is located (see *Secured Transactions Guide*, rec. 203). This means that, where a secured creditor wishes to make its security right in a tangible asset effective against third parties by registration, it must register in the registry of the State where the encumbered asset is located. It follows that, where encumbered tangible assets are located in multiple States, registrations in the registries of all those States will be necessary. With respect to the creation, third-party effectiveness and priority of security rights in intangible assets and mobile assets that are ordinarily used in multiple jurisdictions, the applicable law, as a general rule, is the law of the State in which the grantor is located (see *Secured Transactions Guide*, rec. 208). As a result, the secured creditor must register in the registry of the State where the grantor is located.

8. The rules outlined above are the general baseline rules. The *Secured Transactions Guide* recommends different specialized conflict-of-laws rules for security rights in certain types of asset, including: (a) assets that are subject to a specialized registration regime; (b) receivables arising from a transaction relating to immovable property; (c) rights to the payment of funds credited to bank accounts; (d) rights to receive the proceeds under an independent undertaking; and (e) intellectual property rights (see *Secured Transactions Guide*, recs. 204-207, 209-215 and 248). For example, where the encumbered asset is an intellectual property right, the applicable law is primarily the law of the State under which the intellectual property is protected, although a security right that is created and made effective against third parties only under the law of the State in which the grantor is located may still be effective against the grantor's insolvency representative and judgement creditors (see *Supplement*, rec. 248).

9. Notice registration

9. Most States have established registries for recording title and encumbrances on title on immovable property. Many States have also established similar registries for a limited number of high-value movable assets, such as ships and aircraft. It is essential to the successful implementation of the kind of general security rights registry contemplated by the *Secured Transactions Guide* that its very different characteristics be well understood.

10. First, unlike the typical land, ship or aircraft registry, the general security rights registry contemplated by the *Secured Transactions Guide* does not purport to record the existence or transfer of title to the encumbered asset described in the notice or to guarantee that the person named as grantor in the notice is the true owner. It only provides a record of potentially existing security rights on whatever property right the grantor has or may acquire in the assets described in the notice as a result of off-record transactions or events (see *Secured Transactions Guide*, chap. IV, paras. 10-14).

11. Second, title registries typically require registrants to file or tender for scrutiny the underlying documentation. This is because registration generally is considered to constitute at least presumptive evidence of title and any property rights affecting title. While, the security rights registries in some States also require submission of the underlying security documentation, the *Secured Transactions Guide* recommends that States adopt a notice registration rather than a document registration system (see *Secured Transactions Guide*, recs. 54, subpara. (b), and 57). A notice registration system does not require the actual security documentation to be registered or even tendered for scrutiny by registry staff. All that need be registered is a notice that provides the basic information necessary to alert a searcher that a security right may exist in the assets described in the notice. It follows that registration does not mean that the security right to which the notice refers necessarily exists; only that one may exist at the time of registration or may come into existence later.

12. Third, in States that adopt document registration, registration is sometimes treated as a pre-condition to the creation of a security right. As already explained (see A/CN.9/WG.VI/WP.54, paras. 21, 22, 26 and 27), registration of a notice is irrelevant to the creation of a security right; registration makes any security right created by an off-record security agreement between the parties effective against third parties (see *Secured Transactions Guide*, recs. 32, 33 and 67).

13. The *Secured Transactions Guide* recommends notice registration rather than document registration because notice registration:

(a) Reduces transaction costs for registrants (as they do not need to register or provide evidence of the security documentation in order to register) and third-party searchers (as they do not need to peruse what may be voluminous security documentation to determine if a security right may exist in the relevant assets);

(b) Reduces the administrative and archival burden on registry system operators;

(c) Reduces the risk of registration error (since the less information that must be submitted, the lower the risk of error); and

(d) Enhances privacy and confidentiality for secured creditors and grantors (since the only information about a secured transaction that is publicly available is that which is necessary to alert a searcher that a security right may exist in the assets described in the registered notice).

14. As registration in a notice registration system does not necessarily mean that a security right actually exists, third parties with a competing property right in the encumbered assets will normally wish to obtain proof of the existence of an effective security agreement between the parties and the scope of the assets covered by it. The same is true even where the alleged security right has been made effective against third parties by some other method, such as a transfer of possession, since possession by the putative secured creditor may be for a purpose other than security.

15. Some States provide a procedure whereby a third party with a property right in the encumbered asset may demand this information directly from the person named as a secured creditor in a registration or who is otherwise claiming this status. The same right is extended to unsecured creditors of the grantor so as to enable them to

assess whether they should extend unsecured credit and whether it is worthwhile to undertake the expense of obtaining a judgement and pursuing enforcement against the debtor's assets. While the *Secured Transactions Guide* does not make a recommendation on this matter, it is always open to the debtor to request the secured creditor to send the relevant information directly to a third party. However, the debtor or the secured creditor may not be cooperative in which event the third party will need to seek a judicial order under other law.

16. Even in States that allow third parties to demand verification of the existence of a security right and its scope directly from the secured creditor, this right may not apply to potential buyers or potential secured creditors. They can protect themselves simply by refusing to buy or extend secured credit unless the registration relating to the security right is cancelled or the putative secured creditor is willing to undertake to them that it is not asserting and will not assert in the future a security right in the asset in which they are interested.

17. The grantor may also need to obtain up-to-date information about the scope and value of the security right claimed by its secured creditor and a copy of any written security agreement under which the security right is claimed. In some States, the grantor is entitled to demand this information free of charge although limits are usually placed on the frequency with which requests may be made so as to discourage demands that are unjustified or intended to harass.

10. Coordination with specialized movable property registries

18. Where specialized registries exist and permit the registration of security rights in movable assets with third-party effects (as is the case with the international registry under the Convention on International Interests in Mobile Equipment and its Aircraft Protocol), modern secured transactions regimes must deal with matters related to the coordination of registrations in the two types of registry. The *Secured Transactions Guide* and the *Supplement* discuss coordination of registries in detail (see the *Secured Transactions Guide*, chap. III, paras. 75-82, chap. IV, para. 117; and the *Supplement*, paras. 135-140).

19. One way of coordinating registries is through appropriate third-party effectiveness and priority rules. As already mentioned, the *Secured Transactions Guide* recommends that, while a security right in an asset subject to a specialized registry may be made effective against third parties by registration in the general security rights registry, it is subordinate in priority to a security right or other right, a notice of which was registered in the relevant specialized registry, irrespective of the temporal order of registration (see A/CN.9/WG.VI/WP.54, paras. 30 and 37, and *Secured Transactions Guide*, recs. 43 and 77, subpara. (a)).

20. The *Secured Transactions Guide* also discusses other ways of coordinating registries, including the automatic forwarding of information registered in one registry to another registry and the implementation of common gateways to the various relevant registries. This approach raises complexities with respect to the design of the general security rights registry where the specialized registry organizes registrations by reference to the asset as opposed to the grantor-based indexing system used in the general security rights registry (see *Secured Transactions Guide*, chap. III, paras. 77-81; see also A/CN.9/WG.VI/WP.54/Add.2, paras. 24-27). The *Secured Transactions Guide* envisages that States may wish to

modernize their various specialized registries. However, it does not make a formal recommendation as to how States should ensure the most efficient coordination of registries. This approach takes into account the fact that specialized registries are typically subject to law other than secured transactions law, and their purposes, organization and administration vary from State to State and often from registry to registry. Still, the *Secured Transactions Guide* suggests that a secured transactions law reform and the establishment of a general security rights registry may be used as an opportunity to reform specialized registry regimes to ensure an equivalent level of modern and efficient operation, by introducing, for example, notice registration, debtor-based indices, and for third-party effectiveness and priority purposes (see *Secured Transactions Guide*, chap. IV, para. 117).

11. Coordination with immovable property registries

21. Immovable property registries exist in most, if not in all, States. Typically, the general security rights registry is separate from the immovable property registry owing to differences as to: (a) what is registered (that is, document or notice); (b) the requirements for the description of the encumbered asset (that is, specific or generic); (c) indexing structures (that is, asset-based or debtor-based indices; see also A/CN.9/WG.VI/WP.54/Add.2, paras. 21-27) and legal consequences of registration (that is, creation or third-party effectiveness).

22. However, a State implementing a general security rights registry will need to provide potential secured creditors and third-party financiers with guidance as to the rules governing the third-party effectiveness and priority of security rights in movable assets that are at the time when the security right is created or subsequently become attachments to immovable property. As already discussed, the *Secured Transactions Guide* recommends that a notice of a security right in an attachment to immovable property may be registered either in the general security rights registry or in the immovable property registry and that the security right will be subordinate in priority to a security right or other right with respect to which a notice was registered in the immovable registry, irrespective of the temporal order of registration (see A/CN.9/WG.VI/WP.54, paras. 30 and 37, and *Secured Transactions Guide*, recs. 43, 87 and 88).

23. The asset description requirements for the registration of a notice relating to a security right in an attachment to immovable property may differ depending on whether the registration is made in the security rights registry or in the immovable property registry. The *Secured Transactions Guide* recommends that, for the purposes of registration in the security rights registry, an attachment to immovable property, just like any other encumbered asset, should be described in a manner that reasonably allows its identification (see *Secured Transactions Guide*, rec. 57, subpara. (b)). Thus, a description of the movable asset that is or will be attached may be sufficient without a description of the immovable property. In contrast, the immovable property registry regime will generally require that the immovable property to which the tangible asset is or will be attached be described sufficiently to allow the indexing of the notice in the immovable property registry.

E. Transitional considerations

24. The *Secured Transactions Guide* contains a detailed discussion of the various issues that States implementing a secured transactions law based on its recommendations will need to consider (see *Secured Transactions Guide*, Introduction, sect. E). These issues include the transitional treatment of security rights created under prior law, legislative drafting considerations and post-enactment acculturation.

25. The transitional treatment of existing security rights created under prior law is by far the most important of these considerations, since a law based on the recommendations of the *Secured Transactions Guide* will often constitute a significant departure from the enacting State's prior law.

26. The *Secured Transactions Guide* recommends that an enacting State apply its secured transactions law to all security rights including those already in existence on the date that the new law takes effect (the "effective date"). However, it recognizes four important qualifications.

27. First, prior law applies to enforcement matters that were already the subject of litigation or alternative binding dispute resolution proceedings that commenced before the effective date (see *Secured Transactions Guide*, rec. 229). However, this principle does not apply when the parties have recourse to a non-binding process, such as conciliation. In addition, continuing litigation under prior law should not preclude the secured creditor from commencing enforcement action under the new law after the effective date (see *Secured Transactions Guide*, chap. XI, paras. 15 and 16).

28. Second, prior law determines whether a security right allegedly created before the effective date was effectively created (see *Secured Transactions Guide*, rec. 230).

29. Third, a security right that was effective against third parties under prior law remains effective until the earlier of: (a) the time it would cease to be effective against third parties under prior law; and (b) the expiration of a period of time specified in the law after the effective date (the "transition period") (see *Secured Transactions Guide*, rec. 231). Under this approach, the holder of a security right that was created under prior law is given a transition period to comply with the third-party effectiveness requirements of the new secured transactions law.

30. Fourth, the priority of a security right is determined by prior law if: (a) the security right and all competing rights arose before the effective date; and (b) the priority of none of these rights changed after the effective date (see *Secured Transactions Guide*, rec. 233).

31. If the enacting State already has in place a registry for security rights in movable assets, additional transitional considerations will need to be addressed. If the new secured transactions law covers security rights previously within the scope of an existing registry, the enacting State may decide to assume responsibility for migrating the information in the existing record into the new registry record. In contrast to this approach, the *Secured Transactions Guide* recommends that the burden of migration be placed on secured creditors by giving them a transition period (for example, one year) to register or otherwise make their security right

effective against third parties. This approach has been used with considerable success in a number of States (especially, when such “re-registration” is free of charge). If this approach is chosen, a space or field on the registration form should be provided for indicating that the registration is a migration of a registration made prior to the effective date of the new secured transactions law (for a more detailed discussion of these types of transition issue, see chap. XI of the *Secured Transactions Guide*).

32. States implementing the recommendations of the draft Registry Guide will also need to consider issues of legislative method and drafting. Certain recommendations of the draft Registry Guide reiterate recommendations of the *Secured Transactions Guide* relating to the administration of the registry or its technical design. Such recommendations include the following: 7 (see recs. 55, subpara. (b), and 54, subpara. (d)); 11, subparagraph (a) (see rec. 70); 13 (see rec. 69); 12 (see rec. 67); 15 (see rec. 68); 18 (see rec. 55, subparas. (c) and (d)); 23 (see rec. 57); 28, subparagraph (a) (see rec. 63); 29, subparagraph (a) (see rec. 58); 29, subparagraph (b) (see rec. 64); 29, subparagraph (d) (see rec. 65); and 33 (see rec. 72). The rest of the recommendations address purely technical registration matters. Enacting States will need to consider whether to deal with all these issues in the secured transactions law, in the registry regulation, in the terms of use of the registry, or in all or more than one of these texts.

33. Enacting States will also need to consider issues of post-enactment acculturation and, in particular, will need to design a programme aimed at familiarizing potential registry users with the operation of the registry. More specifically, to ensure the smooth implementation of the registry and its active take up by potential users, enacting States will need to consider entrusting an implementation team with the task of developing education and awareness programmes, disseminating promotional and explanatory material and conducting training sessions. The implementation team should also develop instructions on entering information into paper registration forms and electronic screens.

I. Establishment and functions of the security rights registry

A. General remarks

1. Establishment of the registry

34. Typically, the opening provisions of the regulation provide for the establishment of the registry and reiterate briefly that, in line with its purpose as set out in the secured transactions law, the purpose of the registry is to receive, store and make available to the public, information relating to security rights in movable assets (see draft Registry Guide, rec. 1).

2. Appointment of the registrar

35. The regulation typically identifies, either directly or by reference to the relevant law, the authority that is empowered to appoint the registrar, determine his or her duties and generally supervise the registrar in the performance of those duties. To ensure flexibility in the administration of the registry, the term registrar should be understood as referring either to a single person or to a group of persons

appointed and supervised by the registrar to perform his or her duties (see draft Registry Guide, rec. 2).

3. Functions of the registry

36. The opening provisions of the regulation might also include a provision that lists the various functions of the registry that are dealt with in detail in the later provisions of the regulation with cross-references to the relevant provisions of the regulation in which these functions are addressed. This is the approach recommended in the draft Registry Guide (see draft Registry Guide, rec. 3). The advantage of this approach is clarity and transparency as to the nature and scope of the issues that are dealt with in detail later in the regulation. The possible disadvantage is that the list may not be comprehensive or may be read as implying unintended limitations on the detailed provisions of the regulation to which cross-reference is made. Accordingly, implementation of this approach requires special care to avoid any omissions or inconsistencies.

4. Additional implementation considerations

37. It is critical that the technical staff responsible for the design and implementation of the registry are familiar with the legal and practical objectives that it is designed to fulfil, as well as of the practical needs of the registry personnel and of potential registry users. Consequently, it is necessary at the very outset of the design and implementation process to constitute a team that reflects technological, legal and administrative expertise, as well as user perspectives.

38. It will also be necessary at an early stage to determine whether the registry is to be operated in-house by a governmental agency or in partnership with a private sector firm with demonstrated technical experience and financial accountability. While the day-to-day operation of the registry may be delegated to a private entity, the enacting State should always retain the responsibility to ensure that the registry is operated in accordance with the applicable legal framework (see *Secured Transactions Guide*, chap. IV, para. 47, and rec. 55, subpara. (a)). In addition, for the purposes of establishing public trust in the registry and preventing commercialization and fraudulent use of information in the registry record, the enacting State should retain ownership of the registry record and, when necessary, the registry infrastructure.

39. The design team will need to plan the storage capacity of the registry record. This assessment will depend in part on whether the registry is intended to cover consumer as well as business secured transactions and whether it will cover other transactions, such as true leases. If so, a much greater volume of registrations can be anticipated and thus the storage capacity should be increased. Capacity planning will also need to take into account the potential for additional applications and features to be added to the system. For example, designers may wish to provide sufficient capacity to permit expansion of the registry database at a later point to accommodate the registration of judgements or non-consensual security rights or the addition of linkages to other governmental records such as the State's corporate registry or its other movable or immovable registries. Capacity planning will depend as well on whether registered information is stored in a computer database or a paper record. Ensuring sufficient storage capacity is less of an issue if the record is in electronic form since recent technological developments have greatly decreased

storage costs (the *Secured Transactions Guide* recommends that the registry be electronic “if possible”; see rec. 54, subpara. (j), and paras. 42-49 below).

5. Registry terms and conditions of use

40. As already mentioned, registry-related matters are typically dealt with in the secured transactions law and the registry regulation. They may also be addressed in the registry “terms and conditions of use”. The registry terms and conditions of use are the terms and conditions of the agreement that is entered into by people who submit notices to, or search the public record of, the registry. For example, the registry terms and conditions of use may offer the opportunity to a regular user of the registry to open an account. Such an account could offer practical benefits such as quick access and a simplified mechanism for the payment of any fees. In addition, the registry terms and conditions of use should address the issues of the security and confidentiality of information and user data (such as, for example, user name and password, or other modern security technique).

41. Based on their terms and conditions of use, some registries make available to users upon request additional services. These services include, for example, the following: (a) transaction inquiries that allow users to track by their names or account information their transactions over a specified period of time; (b) verification statement reprints that provide reprints of a verification relating to a specific registration; and (c) statistical reports that provide registry designers, policymakers and academics with useful data (for example, as to the number of registrations and searches, the operating costs, and the registration and search fees collected).

6. Electronic or paper-based registry

42. The *Secured Transactions Guide* recommends that, if possible, the registry record, that is, the information in all registered notices, should be electronic in the sense that information in notices is stored in electronic form in a computer database, that is, the container of the information (see *Secured Transactions Guide*, chap. IV, paras. 38-41 and 43, and rec. 54, subpara. (j)(i)). An electronic registry record is the most efficient and practical means of enabling enacting States to implement the recommendation of the *Secured Transactions Guide* that the registry record must be centralized and consolidated (see *Secured Transactions Guide*, chap. IV, paras. 21-24, and rec. 54, subpara. (e)).

43. The *Secured Transactions Guide* further recommends that, if possible, the registry should be electronic in the sense of permitting the direct electronic submission of notices and search requests by users over the Internet or via direct networking systems as an alternative to the submission of paper registration notices and search requests (see *Secured Transactions Guide*, chap. IV, paras. 23-26 and 43 and rec. 54, subpara. (j)(ii)). This approach is the most effective means of implementing the recommendation of the *Secured Transactions Guide* that the system should be designed to minimize the risk of human error (see *Secured Transactions Guide*, chap. IV, rec. 54, subpara. (j)(iii)-(iv)) since it eliminates the need for registry staff to enter the information contained in a paper notice into the registry record and the risk of error associated with the transcription task.

44. Direct electronic registration and searching also contributes to a speedier registration and search process. When information is submitted to the registry in paper form, registrants must wait until the registry staff has entered the information into the registry record and the information is searchable by third parties before the registration becomes legally effective. Search requests transmitted by paper, fax or telephone also give rise to delays since searchers must wait until the registry staff member carries out the search on their behalf and transmits the results.

45. In addition to eliminating these delays and reducing the risk of human error, a registry system in which registrants and searchers have the option to electronically enter the information directly into the registry record offers the following other advantages:

(a) A very significant reduction in the staffing and other day-to-day costs of operating the registry;

(b) Reduced opportunity for fraudulent or corrupt conduct on the part of registry personnel;

(c) A corresponding reduction in the potential liability of the registry to users who otherwise might suffer loss as a result of the failure of registry staff to enter registration information or search criteria at all, or to enter it accurately; and

(d) User access to registration and searching services outside of normal business hours.

46. If this approach is implemented, the registry should be designed to permit registry users to submit a registration and conduct searches from any private computer facility, as well as from computer facilities made available to the public at branch offices of the registry or other locations. In addition, owing to the reduced costs of direct electronic access, the conditions governing access to the services of the registry should permit third-party private sector service providers to carry out registrations and searches on behalf of their clientele.

47. If the registry record is computerized, the hardware and software specifications should be robust and employ features that minimize the risk of data corruption, technical error and security breach. Even in a paper-based registry, measures should be taken to ensure the security and integrity of the registry record but this is more efficiently and easily accomplished if the registry record is in electronic form. In addition to database control programmes, software will also need to be developed to manage user communications, user accounts, payment of fees and financial accounting, computer-to-computer communication and the gathering of statistical data.

48. The necessary hardware and software needs will need to be evaluated and a decision made as to whether it is appropriate to develop the software in-house by the registry implementation team or purchase it from private suppliers. In making that determination, the team will need to investigate whether an off-the-shelf product is available that can easily be adapted to the needs of the implementing State. It is important that the developer/provider of the software is aware of the specifications for the hardware to be supplied by a third-party vendor, and vice versa.

49. Consideration should also be given to whether the registry should be designed to provide an electronic interface with other governmental databases. For example, in some States, registrants can search the company or commercial registry in the course of effecting a registration to verify and automatically input grantor or secured creditor identifier information (for a discussion of electronic matching of names, see A/CN.9/WG.VI/WP.54/Add.2, para. 58).

B. Recommendations 1-3

[*Note to the Working Group: The Working Group may wish to consider recommendations 1-3, as reproduced in document A/CN.9/WG.VI/WP.54/Add.5. The Working Group may also wish to note that, for reasons of economy, the recommendations are not inserted here at this stage but will be inserted in the final text.*]

II. Access to registry services

A. General remarks

1. Public access

50. The *Secured Transactions Guide* recommends that any person may register a notice of an existing or potential security right or search the public record (not the archives; see *Secured Transactions Guide*, chap. IV, paras. 25-30 and rec. 54, subparas. (f) and (g)). This approach is in line with one of the key objectives of the *Secured Transactions Guide* which is to enhance certainty and transparency (see *Secured Transactions Guide*, chap. IV, para. 25, and rec. 1, subpara. (f)). Because of the importance of ensuring public access to registry services, this principle should be stated in the regulation (see draft Registry Guide, rec. 5).

51. Public access is facilitated if the registry is designed to enable users to submit notices and conduct searches electronically without the need for the assistance or intervention of registry personnel. As already discussed (see paras. 42-49 above), registration using paper forms is associated with cost, delay and the potential for error and liability for the registry.

2. Operating days and hours of the registry

52. The approach to the operating days and hours of the registry recommended in the *Secured Transactions Guide* depends on the extent to which the registry is designed to permit direct electronic registration and searching by users or requires their in-person attendance at a physical office of the registry. In the former case, the registry should be accessible continuously except for brief periods to undertake scheduled maintenance; in the latter case, it should operate during reliable and consistent hours compatible with the needs of potential registry users (see *Secured Transactions Guide*, chap. IV, para. 42, and rec. 54, subpara. (l)). In view of the importance of this issue to users, it should be addressed in the regulation or in administrative guidelines published by the registry (see draft Registry Guide, rec. 5).

53. Where the registry provides services through a physical office, the minimum operating days and hours should be the usual business days and hours in the enacting State. To the extent that the registry requires or permits the registration of paper notices, the registry should aim at ensuring that the information is entered into the registry record and made available to searchers on the same business day that the paper notice is received by the registry. Search requests submitted in paper form should likewise be processed on the same day they are received. To achieve this goal, the deadline for submitting paper notices or search requests may be set independently from the business hours. For example, the regulation or administrative guidelines of the registry could stipulate that, while the registry office is open between 09:00 and 17:00, all forms must be received by an earlier time (e.g. 16:00) so as to ensure that the registry staff has sufficient time to enter the information on notices into the registry record or conduct the search. Alternatively, the registry office could continue to receive paper notices throughout its business hours, but set a “cut off” time, after which information in notices received may not be entered into the registry record, or searches performed, until the next business day. A third approach would be for the registry to undertake that information will be entered into the registry record and a search will be performed within a stated number of business hours after receipt of the notice or search request.

54. The registry regulation or administrative guidelines could also enumerate either in an exhaustive way or an indicative way the circumstances in which access to the registry services may temporarily be suspended. An exhaustive list would provide more certainty but there is a risk that it may not cover all possible circumstances. An indicative list would provide more flexibility but less certainty. Circumstances justifying a suspension of the registry services might include any event that makes it impossible or impractical to provide users with access to the registry services (such as force majeure, due, for example, to fire, flood, earthquake, or war, or where the registry provides users with direct electronic access, a breakdown in Internet or network connection).

3. Access to registration services

55. The *Secured Transactions Guide* recommends that the registry must accept an initial notice of a security right submitted to it for registration (as opposed to an amendment or cancellation notice, acceptance of which is subject to different requirements), if it: (a) is presented in the authorized medium of communication (that is, in the prescribed paper or electronic form); (b) is accompanied by the authorized fee, if any; and (c) provides the grantor identifier and the other information required to be included in the notice (see *Secured Transactions Guide*, rec. 54, subpara. (c), and A/CN.9/WG.VI/WP.54/Add. 2, paras. 53 and 54).

56. In addition, the *Secured Transactions Guide* recommends that the registry must request and maintain a record of the identity of the registrant (see *Secured Transactions Guide*, rec. 55, subpara. (b) and paras. 57-59 below). This additional requirement is included as a measure of protection against the risk that a registration was not authorized by the person identified as the grantor in a registered notice. Requiring the registry to request and maintain the identity of the registrant enables the named grantor to determine to whom a demand to amend or cancel the unauthorized registration should be made. In order to facilitate the registration process, the evidence of identity required of a registrant should be that generally

accepted as sufficient in day-to-day commercial transactions in the enacting State (for example, a driver's licence or other state-issued official document); and the registry should have no right or duty to confirm the evidence of identity submitted by a registrant. Registrants should also be given the option of setting up a user account that provides them with special secure access codes for transmitting notices to the registry. This would facilitate access by frequent users (such as financial institutions, automobile dealers, lawyers and other intermediaries), since they would need to provide the required evidence of their identity only once when initially setting up the account.

57. To implement these recommendations, the regulation should provide that a person is entitled to have access to the registration services of the registry, if that person: (a) uses the prescribed form of notice; (b) provides its identity in the manner prescribed by the registry; and (c) has paid, or made arrangements to pay, any fees (see draft Registry Guide, rec. 6). The regulation should further provide that the registry may reject registration of a notice if it does not contain the required information in the designated field for that type of information or if the information entered is illegible (for the information required in an initial notice and an amendment or cancellation notice, see A/CN.9/WG.VI/WP.54/Add.2, para. 50, A/CN.9/WG.VI/WP.54/Add.4, para. 4, and draft Registry Guide, recs. 23, 30 and 32).

58. Where incomplete or illegible notices are submitted in paper form, there will necessarily be some delay between the receipt of the form by the registry and the communication of its rejection and the reasons for the rejection to the registrant. However, in a registry system that allows registrants and searchers to electronically submit registration information directly to the registry, the system should be designed so as to automatically reject the submission of incomplete or illegible notices and display the reasons on the electronic screen.

4. Verification of identity, evidence of authorization or scrutiny of the content of the notice not required

59. As already mentioned (see para. 56 above), the *Secured Transactions Guide* recommends that the registry must request and maintain a record of the identity of the registrant (see *Secured Transactions Guide*, chap. IV, para. 48, and rec. 55, subpara. (b)). To facilitate the registration process, the *Secured Transactions Guide* further recommends that the registry may not verify the evidence of identity offered by the registrant (see *Secured Transactions Guide*, rec. 54, subpara. (d)). This recommendation should be incorporated into the regulation (see draft Registry Guide, rec. 7, subpara. (a)).

60. In addition, the *Secured Transactions Guide* recommends that registration of a notice should be ineffective unless authorized by the grantor in writing. However, to avoid delay and costs for registrants, evidence of the grantor's authorization is not a pre-condition to access to registry services. Rather, the grantor's authorization may be given before or after registration, and a written security agreement is sufficient to constitute authorization (see *Secured Transactions Guide*, chap. IV, para. 106, and rec. 71). This recommendation should be incorporated into the regulation (see draft Registry Guide, rec. 7, subpara. (b)).

61. Once a registrant satisfies the requirements outlined above for obtaining access to the registry services, the registry has no right to reject the notice. Accordingly, the regulation should confirm that the registry may not conduct other scrutiny of the content of the notice (see draft Registry Guide, rec. 7, subpara. (c)). This does not mean that the registered notice will necessarily be legally effective. The registrant is responsible for any errors or omissions in the registration information submitted by the registrant to the registry (on the types of errors or omissions that may render a registered notice ineffective, see A/CN.9/WG.VI/WP.54/Add.3, paras. 17-29). If the registry had to scrutinize the notice and confirm its effectiveness, the result would be delay, cost and potential for error, a result that would run counter to the kind of efficient registry envisaged in the *Secured Transactions Guide*. Accordingly, the regulation should also confirm that it is not the responsibility of the registry to ensure that the information in a notice is entered in the designated field and is complete, accurate and legally sufficient (see draft Registry Guide, rec. 7, subpara. (c)).

5. Access to search services

62. Citing privacy concerns, some States require searchers to provide justifiable reasons for conducting a search. To facilitate public access to the registry's search services, the *Secured Transactions Guide* recommends that a searcher should not be required to give reasons for the search (see *Secured Transactions Guide*, rec. 54, subpara. (g)). To require searchers to justify a search would undermine the efficiency of the search process, since the registry would have to train its employees to perform this function and would have to scrutinize the reasons given and determine whether they are sufficient to justify a search. Depending on the exact reasons required, equal public access to information in the registry may be impeded, since some potential searchers may not have information available to others. Privacy concerns relating to the grantor are more effectively dealt with by requiring grantor authorization for a registration (see para. 60 above) and by establishing a summary judicial or administrative procedure to enable grantors to cancel or amend unauthorized or erroneous notices quickly and inexpensively (see A/CN.9/WG.VI/WP.54/Add.4, paras. 38-41). Privacy concerns relating to the identity of the secured creditor can be addressed by enabling registrations to be effected by and in the name of the secured creditor's representative. In any event, privacy is less of a concern under the notice registration approach recommended by the *Secured Transaction Guide*, since registered notices provide only the minimal information needed to alert a searcher that a security right may exist in the asset described in a registered notice (see paras. 9-11 above).

63. Accordingly, the regulation should provide that any person is entitled to search the publicly accessible registry record provided that person submits the search request in the prescribed form and has paid, or made arrangements to pay any prescribed fee (see draft Registry Guide, rec. 9). The recommended provision refers to the "public" registry record because expired and cancelled registrations must be removed from the public record and archived (see A/CN.9/WG.VI/WP.54/Add.2, paras. 44 and 45, and draft Registry Guide, rec. 20).

64. As with incomplete or illegible registrations, the regulation should provide that the registry may reject a search request if the searcher does not enter a search criterion in a legible manner in the designated field and must provide the

grounds for a rejection immediately or as soon as practicable (see draft Registry Guide, rec. 10). In registry systems that permit registrants to electronically submit search requests to the registry, the software should be designed so as to automatically prevent the submission of search requests that do not include a legible search criterion in the designated field and display the reasons on the electronic screen.

65. Unlike the approach adopted for registrants (see paras. 55-57 above), the *Secured Transactions Guide* does not require the registry to request and maintain evidence of the identity of a searcher as a pre-condition to submitting a search request (see *Secured Transactions Guide*, rec. 55, subpara. (b)). Since a searcher is merely retrieving information contained in registered notices from the registry record, there is no equivalent concern with protecting the grantor from unauthorized registrations. Accordingly, identification evidence should be requested of searchers only if this is necessary for the purposes of collecting search fees, if any.

B. Recommendations 4-10

[Note to the Working Group: The Working Group may wish to consider recommendations 4-10, as reproduced in document A/CN.9/WG.VI/WP.54/Add.5. The Working Group may also wish to note that, for reasons of economy, the recommendations are not inserted here at this stage but will be inserted in the final text.]