AG/RES. 2607 (XL-O/10)

MODEL INTER-AMERICAN LAW ON ACCESS TO PUBLIC INFORMATION

(Adopted at the fourth plenary session, held on June 8, 2010)
(Provisional version pending revision by the Style Committee)

THE GENERAL ASSEMBLY,

RECALLING resolution AG/RES. 2514 (XXXIX-O/09), "Access to Public Information: Strengthening Democracy," which called for the drafting of a model law on access to public information and a guide for its implementation, in keeping with international standards in this field;

RECALLING ALSO that the Plan of Action of the Third Summit of the Americas, held in Quebec City in 2001, indicates that governments will ensure that national legislation is applied equitably to all, respecting freedom of expression and access to public information by all citizens;

RECALLING FURTHER that, in the Declaration of Nuevo León of the Special Summit of the Americas, held in Monterrey in 2004, the Heads of State and Government expressed their commitment to providing the legal and regulatory framework and the structures and conditions required to guarantee the right to access to public information;

TAKING INTO ACCOUNT that, in order to carry out the mandate contained in resolution AG/RES. 2514 (XXXIX-O/09), the General Secretariat established a group of experts, in which representatives of the Inter-American Juridical Committee, the Office of the Special Rapporteur for Freedom of Expression, the Department for State Modernization and Governance [now: Department for Effective Public Management], and the Department of International Law participated**,** along with experts in access to information from a number of countries and civil society; and

WELCOMING the presentation made to the Committee on Juridical and Political Affairs of the Permanent Council on April 29, 2010, on the Model Inter-American Law on Access to Public Information and its Implementation Guide,

RESOLVES:

1. To take note of the Model Inter-American Law on Access to Information (document CP/CAJP-2840/10), which is part of this resolution; as well as its Implementation Guide, contained in document CP/CAJP-2841/10.
2. To reaffirm, as applicable, the mandates contained in resolution AG/RES. 2514 (XXXIX-O/09) "Access to Public Information: Strengthening Democracy." In this regard, to establish that the special meeting scheduled for the second half of 2010 take into account the Model Inter-American Law on Access to Public Information and any observations on it that member states may present.

3. To instruct the General Secretariat to provide support to the member states that so request in the design, execution, and evaluation of their regulations and policies on access to public information by citizens.

4. To thank the General Secretariat and the experts for preparing the Model Inter-American Law on Access to Public Information and its Implementation Guide.

5. Execution of the activities envisaged in this resolution shall be subject to the financial resources available in the program-budget of the Organization and other resources.

APPENDIX

MODEL INTER-AMERICAN LAW ON ACCESS TO INFORMATION

RECALLING:

That the Heads of States and Governments of the Americas, in the Declaration of Nuevo Leon, made a commitment to provide the legal and regulatory frameworks necessary to guarantee the right of access to information;

That the OAS General Assembly instructed the Department of International Law, in resolution AG/RES. 2514 (XXXIX-O/09), to draft a Model Law on Access to Information and Guide for its Implementation, in cooperation with the Inter-American Juridical Committee, the Special Rapporteurship for Freedom of Expression, and the Department of State Modernization and Good Governance, with the cooperation of the member states, civil society and other experts, to serve as a model for reform in the hemisphere, and

REAFFIRMING:

The American Convention on Human Rights, in particular Article 13 on Freedom of Thought and Expression;

The Inter-American Commission on Human Rights' Inter-American Declaration of Principles on Freedom of Expression;

The Inter-American Court of Human Rights' decision in *Claude Reyes v. Chile*, which formally recognized the right of access to information as part of the fundamental right to freedom of expression;

The Inter-American Juridical Committee's Principles on the Right of Access to Information;

The "Recommendations on Access to Information" drafted by the OAS Department of International Law, in coordination with the organs, agencies and entities of the Inter-American system, civil society, State experts, and the Permanent Council's Committee on Juridical and Political Affairs;

The Annual Reports of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights;

The Carter Center's Atlanta Declaration and American Regional Findings and Plan of Action for the Advancement of the Right of Access to Information, and

UNDERSCORING:

That access to information is a fundamental human right and an essential condition for all democratic societies;

That right of access to information applies broadly to all information in possession of public authorities, including all information which is held or recorded in any format or medium;

That the right of access to information is based on the principle of maximum disclosure;

That exceptions to the right of access should be clearly and narrowly established by law;

That even in the absence of a specific request, public bodies should disseminate information about their functions on a routine and proactive basis and in a manner that assures that the information is accessible and understandable;

That the process of requesting information should be regulated by clear, fair and non-discriminatory rules which set clear and reasonable timelines, provide for assistance to those requesting information, assure that access is free or limited to the cost of reproduction of records and require specific grounds for the refusal of access;

That individuals should be afforded the right to bring an appeal against any refusal or obstruction to provide access to information before an administrative body, and to bring an appeal against the decisions of such administrative body before the courts;

That sanctions should be imposed against any individual who willfully denies or obstructs access to information in breach of the rules set forth in this law;

That measures should be taken to promote, implement and enforce the right of access to information in the Americas,

[Member State] agrees to the provisions of the following:

LAW ON ACCESS TO INFORMATION

I. DEFINITIONS, SCOPE AND RIGHT OF ACCESS

Definitions

1. In this Law, unless the context otherwise requires:

    a) "Information" refers to any type of data in custody or control of a public authority;

    b) "Information Officer" refers to the individual or individuals appointed by a public authority pursuant to Articles 30 and 31 of this Law;

    c) "Record" refers to any recorded information, regardless of its form, source, date of creation, or official status, whether or not it was created by the public authority that holds it, and whether or not it is classified;

    d) "Publish" refers to the act of making information available in a form generally accessible to members of the public and includes all print, broadcast and electronic forms of dissemination;

    e) "Public Authority" refers to any governmental authority or private organization falling under Article 3 of this Law;

    f) "Interested Third Parties" refers to persons who may have a direct interest in non-disclosure of information they provided voluntarily to a public authority, because it will affect their privacy or their commercial interests;

    g) "Personal Information" means information which relates to a living individual who can be identified from that information; and

    h) "Senior Official" means any public official whose salary whom exceeds [USD$100,000].

Scope and Purpose

2. This Law establishes a broad right of access to information, in possession, custody or control of any public authority, based on the principle of maximum disclosure, so that all information held by public bodies is complete, timely and accessible, subject to a clear and narrow regime of exceptions set out in law that are legitimate and strictly necessary in a democratic society based on the standards and jurisprudence of the Inter-American system.

3. This Law applies to all public authorities, including the executive, legislative and judicial branches at all levels of government, constitutional and statutory authorities, non-state bodies which are owned or controlled by government, and private organizations which operate with substantial public funds or benefits (directly or indirectly) or which perform public functions and services insofar as it applies to those funds or to the public services or functions they

undertake. All of these bodies are required to make information available pursuant to the provisions of this Law.

Comment: The term benefits should not be construed broadly so as to include any financial benefit received from the government.

4. To the extent of any inconsistency, this Law shall prevail over any other statute.

Comment: While the model law does not contain a provision whereby private information that is required for the exercise or protection of international recognized human rights would be brought under the scope of the law, some states, including South Africa have adopted this approach.

Right of Access

5. Any person making a request for information to any public authority covered by this Law shall be entitled, subject only to the provisions of Part IV of this Law: –

    a) to be informed whether or not the public authority in question holds a record containing that information or from which that information may be derived;

    b) if the public authority does hold such a record, to have that information communicated to the requester in a timely manner;

    c) to an appeal where access to the information is denied;

    d) to make an anonymous request for information;

    e) to make a request without providing justifications for why the information is requested;

    f) to be free from discrimination based on the nature of the request; and

    g) to be provided with the information free of charge or at a cost limited to the cost of reproduction.

6. The requester shall not be sanctioned, punished or prosecuted in response to the exercise of the right of access to information.

7. (1) The Information Officer must make reasonable efforts to assist the requester in connection with the request, respond to the request accurately and completely, and subject to the regulations, provide timely access to the records in the format requested.

    (2) The Information Commission must make reasonable efforts to assist the requester in connection with the appeal.

Interpretation

8. When interpreting a provision of this Law, everyone tasked with interpreting this Law, or any other legislation or regulatory instrument that may affect the right to information, must adopt any reasonable interpretation of the provision that best gives effect to the right to information.

II. MEASURES TO PROMOTE OPENNESS

Adoption of Publication Schemes

9. (1) Every public authority shall adopt and disseminate widely, including on its website, a publication scheme approved by the Information Commission, within [six] months of: -

a) the coming into force of this Law; or

b) its establishment.

(2) The publication scheme shall set out: -

a) the classes of records that the authority will publish on a proactive basis; and

b) the manner in which it will publish these records.

(3) In adopting a publication scheme, a public authority shall have regard to the public interest:

a) in allowing access to the information it holds; and

b) in making information available proactively so as to minimize the need for individuals to make requests for information.

(4) Every public authority shall publish information in accordance with its approved publication scheme.

Approval of Publication Schemes

10. (1) When approving a publication scheme, the Information Commission may provide that the approval will expire at a certain point.

(2) When refusing to approve a publication scheme, the Information Commission shall give reasons and provide reasonable direction to the public authority as to how it may amend the scheme so as to obtain approval.

(3) The Information Commission may, upon giving [six] months notice with reasons, withdraw its approval of any publication scheme.

(4) The Information Commission shall take into account the need to comply with Article 11 (2) when approving or refusing to approve a publication scheme.

Model Publication Schemes

11. (1) The Information Commission may adopt or approve model publication schemes for different classes of public authorities.

(2) Where a public authority in a certain class adopts a model publication scheme which applies to that class of public authorities, it shall not require further approval from the Information Commission, provided that it shall inform the Information Commission that it is applying that model publication scheme.

(3) The Information Commission may put a time limit on the validity of a model publication scheme or, upon giving [six] months notice to all public authorities using it, terminate the validity of any publication scheme.

Key Classes of Information

12. (1) The following are the key classes of information subject to proactive disclosure by a public authority: -

a) a description of its organizational structure, functions, duties, locations of its departments and agencies, operating hours, and names its officials;

b) the qualifications and salaries of senior officials;

c) the internal and external oversight, reporting and monitoring mechanisms relevant to the public authority including its strategic plans, corporate governance codes and key performance indicators, including any audit reports;

d) its budget and its expenditure plans for the current fiscal year, and past years, and any annual reports on the manner in which the budget is executed;

e) its procurement procedures, guidelines and policies, contracts granted, and contract execution and performance monitoring data;

f) the salary scales, including all components and sub-components of actual salary, relevant to all employee and consultant categories within the public authority (including all data related to current reclassification of posts);

g) relevant details concerning any services it provides directly to members of the public, including customer service standards, charters and protocols;

h) any direct request or complaints mechanisms available to members of the public regarding acts, or a failure to act, by that public authority;

i) a description of the powers and duties of its senior officers, and the procedure they follow to make decisions;

j) any statutes, policies, decisions, rules, guidelines, manuals or other records containing interpretations, practices or precedents regarding the discharge by that public authority of its functions, that affect the general public;

k) any mechanisms or procedures by which members of the public may make representations or otherwise influence the formulation of policy or the exercise of powers by that public authority;

l) a simple guide containing adequate information about its record-keeping systems, the types and forms of information it holds, the categories of information it publishes and the procedure to be followed in making a request for information and an internal appeal;

m) its Disclosure Log, in accordance with Article 18, containing a list of requests received and records released under this Law, which shall be automatically available, and its Information Asset Register, in accordance with Article 17;

n) a complete list of subsidies provided by the public authority;

o) frequently requested information; and

p) any additional information deemed appropriate by the public authority

(2) The publication schemes adopted by every public authority shall, within [seven] years of the adoption of the first publication scheme by that public authority in accordance with Article 8 (1), cover all of the key classes of information set out in paragraph 11 (1).

(3) The public authority must create and archive a digital image of its website, complete with information required by its approved publication scheme, on a yearly basis.

Comment: The list of elements subject to proactive disclosure is, of course, subject to the exceptions in Section IV of the Law. However, it is the sole power of the Information Commission (not the public authority) to determine the application of Section IV in the formulation and approval of the publication scheme.

Policy Documents and Specific Populations

13. (1) Public authorities must make copies of each of its policy documents available for inspection. In order for policy documents to be publicly available:

(2) No one shall be subject to any prejudice because of the application of a policy that is not disclosed pursuant to paragraph (1).

14. Public authorities shall release public information which affects a specific population in a manner and form that is accessible to that population, unless there is a good legal, policy, administrative or public interest reason not to.

Other Laws & Mechanisms Providing for Disclosure of Information

15. This Law does not limit the operation of another Law or administrative scheme that: -

a) requires information concerning records in the possession, custody or control, of government to be made available to members of the public;

b) enables a member of the public to access records in the possession, custody or control of government; or

c) requires the publication of information concerning government operations.

16. Whenever an individual makes a request for information, it should be treated at least as favorably as a request under this Law.

Information Asset Registers

17. (1) Every public authority shall create and maintain an updated Information Asset Register listing:

a) every category of information published by the public agency;

b) every published record; and

c) every record available for purchase by members of the public.

(2) The Information Commission may set standards regarding information asset registers.

(3) Every public authority shall ensure that its Information Asset Register complies with any standard set by the Information Commission.

Request and Disclosure Logs

18. (1) Public authorities shall create, maintain and publish a Request and Disclosure Log of all information released in response to a request made under this Law on its website and in the reception area of all its offices accessible by members of the public, subject to protection of privacy of the original requesting party.

(2) The Information Commission may set standards regarding information Request and Disclosure Logs.

(3) Every public authority shall ensure that its Request and Disclosure Logs comply with any standard set by the Information Commission.

Previously Released Information

19. (1) Public authorities must ensure and facilitate access to all records previously released, in the most convenient way possible, to persons requesting such information.

(2) Requests for records contained in Request and Disclosure Logs shall be made available as soon as practicable if they are in electronic form and no later than [three] working days after the records are sought if they are not in electronic form.

(3) Where a response to a request for information has been provided in electronic form, it shall proactively be made available on the public authority's website.

(4) If a second request is made for the same information, it shall proactively be made available on the public authority's website.

III. ACCESSING INFORMATION HELD BY PUBLIC AUTHORITIES

Request for Information

20. The request for information may be filed in writing, by electronic means, orally in person, by phone, or by any alternative means, with the relevant Information Officer. In all cases, the request shall be properly logged pursuant to Article 21 of this Law.

21. Unless the information can be provided immediately, all requests shall be registered and assigned a tracking number, which shall be provided to the requester along with contact information for the Information Officer assigned to the request.

22. No fee shall be charged for making a request.

23. Requests for information shall be registered in the order in which they are received and handled in a fair and non-discriminatory manner.

24. (1) A request for information shall contain the following information: -

a) contact information for the receipt of notices and delivery of the information requested;

b) a sufficiently precise description of the information requested, in order to allow the information to be found; and

c) the preferred form in which the information should be provided.

(2) If the form in which the information should be provided is not indicated, the information requested shall be provided in the most efficient and cost-effective manner for the public authority.

Comment: The requester need not provide their name on the request for information. However, insofar as the request concerns personal information, the requester's name may be required.

25. (1) The public authority in receipt of a request must reasonably interpret the scope and nature of the request.

(2) In the event the receiving authority is uncertain as to the scope and nature of a request, it must contact the requester to clarify what is being requested. The receiving authority must make reasonable efforts to assist the requester in connection to the request, and respond accurately and completely.

26. (1) If the receiving authority reasonably determines that it is not the proper authority to handle the request, it must, as soon as possible and in any case within [five] working days, forward the request to the proper authority for processing.

(2) The receiving authority must also notify the requester that his/her request has been routed to another public authority for processing.

(3) The forwarding authority must provide the requester with contact information for the Information Officer at the public authority where the request has been routed.[1/]

Third Party Response to Notification

27. Interested third parties shall be informed within [5] days of a request being received, and given [10] days to make written representations to the relevant authority either: -

a) consenting to disclosure of the information; or

b) stating reasons why the information should not be disclosed.

---

1. ALTERNATIVE: If the receiving public authority reasonably determines that it is not the proper authority to handle the request, it must, within [five] working days indicate the proper authority to the requester to the requester.

Cost of Reproduction

28. (1) The requester shall only pay for the cost of reproduction of the information requested and, if applicable, the cost of the delivery, if requested. Information provided electronically shall be free of charge.

(2) The costs of reproduction shall not exceed the actual cost of the material in which it is reproduced; delivery shall not exceed the actual cost of the same service in the market. The costs, for this purpose, shall be set periodically by the Information Commission.

(3) The public authorities shall provide information free of all charges, including reproduction and delivery, for any citizen below an income set by the Information Commission.

(4) The Information Commission will set additional rules regarding fees, which may include the possibility that information will be provided for free if in the public interest and that no charge may be levied for a minimum number of pages.

Form of Access

29. Public authorities shall facilitate access to inspection by making available facilities for such purpose.

Information Officer

30. The head of the public authority responsible for responding to requests must designate an Information Officer who shall be the focal point for implementing this law in that public authority. The contact information for each such Information Officer must be posted on the website of the public authority and made readily available to the public.

31. The Information Officer shall, in addition to any obligations specifically provided for in other sections of this Law, have the following responsibilities:

a) to promote within the public authority the best possible practices in relation to record maintenance, archiving and disposal; and

b) to serve as a central contact within the public authority for receiving requests for information, for assisting individuals seeking to obtain information and for receiving individual complaints regarding the performance of the public authority to inform disclosure.

Searching for Records

32. Upon receipt of a request for information, the public authority in receipt of the request must undertake a reasonable search for records which respond to the request.

Records Management

33. The [body responsible for archives] must develop, in coordination with the Information Commission, a records management system which will be binding on all public authorities.

Missing Information

34. When a public authority is unable to locate information responsive to a request, and records containing that information should have been maintained, it is required to make reasonable efforts to gather the missing information and provide it to the requester.

Time to Respond

35. (1) Each public authority must respond to a request as soon as possible and in any event, within [twenty] working days of its receipt.

(2) In the event the request was routed to the public authority from another authority, the date of receipt shall be the date the proper authority received the request, but in no event shall that date exceed [ten] working days from the date the request was first received by a public authority designated to receive requests.

Extension

36. (1) Where necessary because of a need to search for or review of voluminous records, or the need to search offices physically separated from the receiving office, or the need to consult with other public authorities prior to reaching a disclosure determination, the public authority processing the request may extend the time period to respond to the request by up to [twenty] working days.

(2) In any event, the failure of the public authority to complete the processing of the request within [twenty] working days, or, if the conditions specified in paragraph 1 are met, the failure to respond to the request within [forty] working days, shall be deemed a denial of the request.

(3) In highly exceptional cases, involving large amounts of information, the public authority may appeal to the Information Commission for an extension beyond [forty] working days.

(4) Where a public authority fails to meet the standards of this article, no charge should be imposed for providing the information, and any denial or redaction must be specifically approved by the Information Commission.

37. Under no circumstances may, a third party notification excuse the public authority from complying with the time periods established in this law.

Notice to the Requester

38. As soon as the public authority has reasonable grounds to believe that satisfaction of a request will either incur reproduction charges above a level set by the Information Commission or take longer than [twenty] working days, it shall inform the requester and giver him/her the opportunity to narrow or modify the scope of the request.

39. (1) Public authorities shall provide access in the form requested, unless this would: -

a) harm the record;

b) breach copyright not held by public authority; or

c) be impractical because of the need to redact some information contained in the record, pursuant to Section IV of this Law.

(2) Where information requested in electronic format is already available on the internet, the public authority may simply indicate to the requester the exact URL where the requester may access the information.

(3) In cases where the requester requested the information in a non-electronic format, the public authority may not answer the request by making reference to a URL.

40. (1) Where information is provided to the requester, he/she shall be notified and informed of any relevant applicable fees and/or arrangements for access.

(2) In the event that any information or part of the information is withheld from a requester because it falls under the exceptions to disclosure under Section IV of this Law, the requester must be given:

a) a reasonable estimate of the volume of material that is being withheld;

b) a description of the precise provisions of this Law used for the withholding; and

c) notification of the right to appeal.

IV. EXCEPTIONS

Exceptions to Disclosure

41. Public authorities may deny access to information only in the following circumstances, when it is legitimate and strictly necessary in a democratic society, based on the standards and jurisprudence of the Inter-American system: -

a) Allowing access would harm the following private interests: -

1) right to privacy, including life, health, or safety;

2) legitimate commercial and economic interests; or,

3) patents, copyrights and trade secrets.

Exceptions in this sub-paragraph do not apply when the individual has consented to its disclosure or where it was clear when the information was provided that it was part of a class of information that was subject to disclosure.

The exception under sub-paragraph (a) 1 does not apply to matters related to the functions of public officials or in cases where the individual in question has been deceased in excess of [20] years.

Commentary: In cases where information on legitimate commercial and economic interests was provided to the public authority in confidence, such information shall be exempt from disclosure.

b) Allowing access would create a clear, probable and specific risk of substantial harm, [which should be further defined by law] to the following public interests: -

1) public safety;

2) national security;

3) the future provision of free and open advice within and among public authorities;

4) effective formulation or development of policy;

5) international or intergovernmental relations;

6) law enforcement, prevention, investigation and prosecution of crime;

7) ability of the State to manage the economy;

8) legitimate financial interest of a public authority; and

9) tests and audits, and testing and auditing procedures.

The exceptions under sub-paragraphs (b) 3, 4 and 9, do not apply to facts, analysis of facts, technical data or statistical information.

The exception under sub-paragraph (b) 4 does not apply once the policy has been enacted.

The exception under sub-paragraph (b) 9 does not apply to the results of a particular test or audit once it is concluded.

c) Allowing access would constitute an actionable breach of confidence in communication, including legally privileged information.

Comment: Although the Inter-American system provides for a potential exemption for the protection of "public order" it is explicitly rejected as a grounds for refusing access in the present Model Law as it is overly vague and provides for an overbroad application as an exemption.

Comment: In order to meet the standards of the Inter-American system for clear and specific exceptions, the bracketed language in paragraph (b) "further defined by law" should be understood to include both legislation and/or jurisprudence, from which the definition of the exceptions shall emanate. Moreover, although this bracketed language allows further definition by law, these additional definitions are limited in operation by the principles and provisions of this Law. To this effect, the Law establishes a broad right of access to information based on the principle of maximum disclosure (Article 2); establishes that this law prevails over any other law, in cases of inconsistency (Article 4); and requires that anyone interpreting this law, or any other law or instrument that may affect the right to information, must adopt any reasonable interpretation in favor of disclosure (Article 8).

Partial Disclosure

42. For circumstances in which the totality of the information contained in a record is not exempted from disclosure by an exception in Article 41, protected information may be redacted. Information not exempted from disclosure in a same record, however, must be delivered to the requesting party and made available to the public.

Historical Disclosure

43. The exceptions under Article 41 (b) do not apply to a record that is more than [12] years old. Where a public authority wishes to reserve the information from disclosure, this period can be extended for another [12] years only by approval by the Information Commission.

Public Interest Override

44. Public Authorities may not refuse to indicate whether or not it holds a record, or refuse to disclose that record, pursuant to the exceptions contained in Article 41, unless the harm to the interest protected by the relevant exception outweighs the general public interest in disclosure.

45. The exceptions in Article 41 do not apply in cases of serious violations of human rights or crimes against humanity.

V. APPEALS

Internal Appeal

46. (1) A requester may, within [60] working days of a refusal to respond, or of any other breach of rules in this Law for responding to a request, lodge an internal appeal with the head of the public authority.

(2) The head of the public authority must issue a written decision stating adequate reasons, within [10] working days from receipt of the notice of appeal, and deliver a copy of that decision to the requester.

(3) If the requester decides to present an internal appeal, he/she must wait the full term of the timelines in this provision prior to lodging an external appeal.

Comment: An internal appeal should not be mandatory, but instead optional for the requester before proceeding to the external appeals process.

External Appeal

47. (1) Any requester who believes that his or her request for information has not been processed in accordance with the provisions of this Law, whether of not he or she has lodged an internal appeal, has the right to file an appeal with the Information Commission.

(2) Such an appeal shall be filed within [60] working days of a decision being appealed against, or the expiration of the timelines for responding to the request or an internal appeal established by this Law.

(3) Such an appeal shall contain: -

a) the public authority with which the request was filed;

b) the contact information of the requester;

c) the grounds upon which the appeal is based; and

d) any other information that the requester considers relevant.

48. Upon receiving an appeal, the Information Commission may attempt to mediate between the parties with a view toward disclosure of the information without going through a formal appeal process.

49. (1) The Information Commission shall log the appeal in a centralized tracking system and inform all interested parties, including interested third parties, about the appeal and their rights to make representations.

(2) The Information Commission shall set fair and nondiscriminatory rules regarding the processing of appeals which ensure that all parties have an appropriate opportunity to make representations.

(3) In the event the Information Commission is uncertain as to the scope and/or nature of a request and/or appeal, it must contact the appellant to clarify what is being requested and/or appealed.

50. (1) The Information Commission shall decide appeals, including attempts to mediate, within [60] working days and may, in exceptional circumstances, extend this timeline by another [60] working days.

51. (2) The Information Commission, in deciding the case, may:

a) reject the appeal;

b) require the public authority to take such steps as may be necessary to comply with its obligations under this Law, such as, but not limited to, providing the information and/or reducing the fee;

(3) The Information Commission shall serve notice of its decision to the requester, the public authority and any interested party. Where the decision is unfavorable to the requester, he or she shall be informed of his or her right to appeal.

(4) If a public authority does not comply with the Information Commission's decision within the time limits established in that decision, the Information Commission or the requester may file a petition with the [proper] court in order to compel compliance.

Comment: The manner of enforcing the Information Commission's decisions in accordance with paragraph 4 will vary from country to country.

Court Review

52. A requester may file a case with the court only to challenge a decision of the Information Commission, within [60] days of an adverse decision or the expiration of the term provided in the law.

53. The court shall come to a final decision on all procedural and substantive aspects of the case as early as possible.

Comment: These rules are based on the assumption that in many countries courts have all of the inherent powers needed to process these types of cases, including for example imposing sanctions on public authorities. Where this is not the case, these powers may need to be explicitly given to them through the access to information law.

Burden of Proof

54. (1) The burden of proof shall lie with the public authority to establish that the information requested is subject to one of the exceptions contained in Article 41. In particular, the public authority must establish: -

a) that the exception is legitimate and strictly necessary in a democratic society based on the standards and jurisprudence of the Inter-American system;

b) that disclosure will cause substantial harm to an interest protected by this Law; and

c) that the likelihood and gravity of that harm outweighs the public interest in disclosure of the information.

(2) The burden of proof shall also lie with the public authority to defend any other decision that has been challenged as a failure to comply with the Law.

VI. INFORMATION COMMISSION

Establishment of the Information Commission

55. (1) An Information Commission is hereby established, which shall be in charge of promoting the effective implementation of this Law;

(2) The Information Commission shall have full legal personality, including the power to acquire, hold and dispose of property, and the power to sue and be sued;

(3) The Information Commission shall have operative, budgetary and decision-making autonomy and shall report to the legislature;

(4) The legislature shall approve the budget of the Information Commission, which shall be sufficient to enable the Commission to perform its duties adequately.

56. (1) The Information Commission shall be comprised of [three or more] commissioners, reflecting a diversity of skills and backgrounds.

(2) The Commissioners shall appoint a Chair from among themselves.

Commentary: It is preferable for the Commission to be comprised of five Commissioners. In contrast to a collegiate body of five members, a body of three can more easily isolate and render inoperable the advice and participation of one of the Commissioners in cases where the other two are closely associated philosophically, personally or politically – a dynamic that proves more difficult in a body of five.

57. No one shall be appointed Commissioner unless he/she: -

a) is a citizen;

b) is a person of high moral character;

c) has not held a [high-ranking] position in government or with a political party within the past [2] years; and,

d) has not been convicted of a violent crime or a crime of dishonesty, within the last [five] years, for which he or she has not been pardoned.

58. The Commissioners will be appointed by the [Executive Official] after nomination by a two-thirds majority vote of the [legislative body] and in a process in accordance with the following principles: -

a) participation by the public in the nomination process;

b) transparency and openness; and

c) publication of a short list of candidates.

Comment: In order to increase confidence in the institution, it is desirable that both the executive and legislature be involved in the selection process; that any decision by the legislature be by a supermajority (e.g. 60 percent or two thirds) sufficient to ensure bi- or multi-partisan support; that the public has an opportunity to participate in the nomination process; and that the process be transparent. There are two main approaches: executive appointment, with nomination or approval by the legislature; and legislative appointment, with nomination or approval by the executive.

59. (1) The Commissioners shall serve full-time and be paid the same salary as a [high court judge].

(2) The Commissioners shall not hold another job, position or commission, except in educational, scientific or charitable institutions.

Comment: It is strongly recommended that the Information Commissioners should serve full-time, and that their salaries should be linked to an externally established rate to enhance Commissioner's independence.

60. The Commissioners hold office for period of [5] years, which may be renewed once.

Commentary: In order to ensure continuity of service, it is necessary to stagger the terms of the Commissioners, when the Commission is first created, so that no more than two thirds of the Commissioners' terms expire in any given year.

61. (1) The Commissioners may not be removed or suspended from office, except in accordance with the procedure by which he or she was appointed and only for reasons of incapacity or behavior that renders him/her unfit to discharge his/her duties. Such behavior includes:

a) conviction of a criminal offense;

b) infirmity that affects the individual's capacity to discharge his duties;

c) severe breach of the provisions of the Constitution or this Law;

d) refusal to comply with any objective disclosure requirements, such as regarding salary or benefits.

(2) Any Commissioner that has been removed or suspended has the right to appeal that removal or suspension to a court of law.

Duties and Powers of the Information Commission

62. The Information Commission shall, in addition to any other specific powers established by this Law, have all the necessary powers to discharge its duties, including: -

a) to review any information held by a public authority, including through on-site inspection;

b) *sua sponte* authorization to monitor, investigate and enforce compliance with the law;

c) to compel witnesses and evidence in the context of an appeal;

d) to adopt such internal rules as may be necessary to conduct its business;

e) to issue recommendations to public authorities; and,

f) to mediate disputes between parties in an appeal.

63. The Commissioners shall, in addition to other duties specifically established by this Law, have the following duties: -

a) to interpret this Law;

b) to provide support and guidance, upon request, to public authorities concerning the implementation of this Law;

c) to promote awareness and understanding of the Law and its provisions among the public, including through publishing and disseminating a guide on the right of access to information;

d) to make recommendations on existing and proposed legislation;

e) to refer cases of suspected administrative and criminal wrongdoing; and,

f) to cooperate with civil society.

Reporting

64. (1) Public authorities shall report annually to the Information Commission on the activities of the public authority pursuant to, or to promote compliance with this Law. This report shall include, at least information about: -

a) the number of requests for information received, granted in full or in part, and refused;

b) how often and which sections of the Law were relied upon to refuse, in part or in full, requests for information;

c) appeals from refusals to communicate information;

d) fees charged for requests for information;

e) its activities pursuant to Article 11 (duty to publish);

f) its activities pursuant to Article 32 (maintenance of records);

g) its activities pursuant to Article 66 (training of officials);

h) information on the number of requests responded to within the timeframe provided by this Law;

i) information on the number of requests responded to outside the timeframes provided by this Law, including statistics on any time delays in responding; and,

j) any other information useful to assess compliance of public authorities with the obligations under the Law.

(2) The Information Commission shall report annually on the Commission's operation and the functions of the Law. This report shall include, at a minimum, all information it receives from public authorities in compliance with the right of access, the number of appeals filed with the commission, including a break-down of the number of appeals from various public authorities, and results and status of these appeals.

Criminal and Civil Responsibility

65. No one shall be subjected to civil or criminal action, or any employment detriment, for anything done in good faith in the exercise, performance or purported performance of any power or duty in terms of this Law, as long as they acted reasonably and in good faith.

66. It is a criminal offense to willfully destroy or alter records after they have been the subject of a request for information.

67. (1) It is an administrative offense willfully to:

a) obstruct access to any record contrary to Parts II and III of this Law;

b) obstruct the performance by a public authority of a duty under Parts II and III of this Law;

c) interfere with the work of the Commission;

d) fail to comply with provisions of this Law;

e) fail to create a record either in breach of applicable regulations and policies or with the intent to impede access to information; and

f) destroy records without authorization.

(2) Anyone may make a complaint about an administrative offense as defined above.

(3) Administrative sanctions shall follow the administrative law of the state and may include a fine [of up to x minimum salaries], a suspension of a period for [x] months/years, termination, or a restriction of service for [x] months/years].

(4) Any sanctions ordered shall be posted on the website of the Commission and the respective public authority within five days of their having been ordered.

VII. PROMOTIONAL AND COMPLIANCE MEASURES

Monitoring and Compliance

68. The [relevant legislative body] should regularly monitor the operation of this Law, in order to determine whether changes and improvements are necessary to ensure all public authorities comply with the text and spirit of the Law, and to ensure that the government is transparent, remains open and accessible to its citizens, and complies with the fundamental right of access to information.

Training

69. The Information Officer shall ensure the provision of appropriate training for the officials of the public authority on the application of this Law.

70. The Information Commission shall assist public authorities in providing training to officials on the application of this law.

Formal Education

71. The [Ministry of Education] shall ensure that core education modules on the right to information are provided to students in each year of primary and secondary education.

VIII. TRANSITORY MEASURES

Short Title and Commencement

72. This Law may be cited as the Access to Information Law [insert relevant year].

73. This Law shall come into effect on a date proclaimed by [insert relevant individual, such as president, prime minister or minister] provided that it shall automatically come into effect [six] months after its passage into law if no proclamation is forthcoming.

Regulation

74. This Law shall be followed by the adoption of an administrative regulation within [1] year after the adoption of the Law, which shall be drafted with the active participation of the Information Commission.

PERMANENT COUNCIL OF THE
ORGANIZATION OF AMERICAN STATES

COMMITTEE ON JURIDICAL AND POLITICAL AFFAIRS

OEA/Ser.G
CP/CAJP-2841/10
23 April 2010
Original: English/Spanish

COMMENTARY AND GUIDE FOR IMPLEMENTATION FOR THE MODEL INTER-AMERICAN LAW ON ACCESS TO INFORMATION

(Document presented by the Group of Experts on Access to Information pursuant to General Assembly Resolution AG/RES. 2514 (XXXIX-O/09)

EXPLANATORY NOTE

This model law on Access to Information and accompanying commentary and guide for implementation is presented pursuant to the operative paragraphs 9 of resolution AG/RES. 2514, which instructed the Department of International Law, in cooperation with the Inter-American Juridical Committee, the Special Rapporteurship for Freedom of Expression of the Inter-American Commission on Human Rights, and the Department of State Modernization and Good Governance, and with the cooperation of the member states and civil society, to develop a Model Law on Access to Public Information and a guide for its implementation, in keeping with international standards in this field. In developing this model law and guide, the Department of International Law convened a group of experts drawn from the Organization of American States, civil society, and member states who contributed in debating, writing and editing the Model Law pursuant to the highest international standards and best practices on access to information.

The Model Law and Implementation Guide are drafted to work in both Common Law and Civil Law systems. When necessary, the commentaries and instructions provide specific guidance on the application and/or interpretation of specific provisions of the Model Law.

The group of experts that drafted the Model Law and Implementation Guide was made up by the following individuals, from OAS organs, member States, civil society and other organizations, who participated exclusively in their individual capacities: Karina Banfi, Executive Director of the Regional Alliance on Access to Information; Leslie Bar-Ness, Manager, State Government Relations, Symantec Corporation; Eduardo Bertoni, Director, Center for Studies on Freedom of Expression and Access to Information, School of Law, Universidad de Palermo; Catalina Botero, Inter-American Commission on Human Rights, Rapporteur on Freedom of Expression; Sandra Coliver, Senior Legal Officer for Freedom of Information and Expression, Open Society Justice Initiative; Damian Cox, Director, Access to Information Unit, Office of the Prime Minister, Jamaica; Annie Goranson, Discovery Attorney, Symantec Corporation; Patricia Milagros Guillén Nolasco, Counselor for the Secretariat of Public Management, Peru; Edison Lanza, Regional Alliance on Access to Information; María Marván Laborde, Information Commissioner, Federal Institute for Access to Public Information (IFAI), Mexico; Toby Mendel, Senior Legal Counsel, Article XIX; Laura Neuman, Associate Director for the Americas Program and Access to Information Project Manager, the Carter Center; Juan Pablo Olmedo, President, Consejo para la Transparencia, Chile; Maria del Carmen Palau, Specialist, Department of State Modernization and Governability, Secretariat of Political Affairs, OAS; Darian Pavli, Legal Officer for Freedom of Expression and Information, Open Society Justice Initiative; Issa Luna Pla,, Instituto de Investigaciones Juridicas, UNAM, Mexico/American Bar Association Rule of Law Initiative; Melanie Ann Pustay, Director of the Office of Information Policy, United States Department of Justice, USA; Andrea Paola Ruiz Rosas, Chief of the Nromative and Regulatory Unit of the Consejo para la Transparencia, Chile; Pablo Saavedra, Secretary, Inter-American Court of Human Rights; David Stewart, Member, Inter-American Juridical Committee, OAS; Natalia Torres, Researcher, Center for Studies on Freedom of Expression and Access to Information, School of Law, Universidad de Palermo; and Josée Villeneuve, Director of Systemic Issues, Policy and Parliamentary Relations, Office of the Information Commissioner of Canada. The work was coordinated by John Wilson, Senior Legal Officer, and Sarah Rivard, Consultant, Department of International Law, Secretariat for Legal Affairs, OAS.

COMMENTARY AND GUIDE FOR IMPLEMENTATION FOR THE MODEL INTER-AMERICAN LAW ON ACCESS TO INFORMATION

-- Table of Contents --

COMMENTARY AND GUIDE FOR IMPLEMENTATION FOR THE MODEL INTERAMERICAN LAW ON ACCESS TO INFORMATION [AG/RES. 2514 (XXXIX-O/09]

CHAPTER 1: ADOPTION OF COMPREHENSIVE FRAMEWORK

It is widely acknowledged that access to information laws don't stand on themselves in a good-governance, transparent and democratic realm. In fact, an access to information law is only one of many steps. This section describes how to build a comprehensive legal and policy framework considering the elements that an access to information regime will require in order to function efficiently.

A. Study of Existing Laws and Policies

The enactment of the Model Law requires scanning and analyzing the existing legislation and policies related to the matter of the prospective law. For the sake of an effective implementation, the new law should ideally be incorporated into the existing scenario and rules, rather than through the creation of new ways to proceed and manage administrative procedures.

Scanning refers to the review of the norms to be enforced in the legal system of a country in order to find norms that could impact in any way the coming into force of the new law. The scan is necessary in order to *localize* the law by applying the right terminology and to make sure that the existing public institutional structure, procedures and coercive mechanisms of the national legal system are taken into consideration. Some of the norms that would impact the new law are the following: -

1. *Legislative decrees that define the nature and operation of the State powers and autonomous bodies that would be under the scope of the law*. In order to fully cover the powers of the State and also the non-state bodies that operate with substantial public funds, the State's organization of certain powers and responsibilities will have to be studied. Additionally, the public interest institutional terminology used in the legal system should be studied.

2. *Norms that establish administrative procedures or legislation that standardizes procedures in each of the powers and organisms*. The new law must be explicit so that the *expedito* principle of the right to information is protected.

3. *Royalties*. Laws that establish the cost of the government royalties for photocopies or reproduction of documents in various formats, also known as *Leyes de Derechos,* as well as those that establish the commercial price for governmental information.

4. *Administrative silence*. In most countries the legal concept, procedure and sanctions already exists, so the new law would have to incorporate those for the actions where government does not respond to information requests.

5. *Norms that establish administrative responsibility*. The existing system of sanctions, penalties and fines corresponding to administrative misconduct must be observed and

entrenched in the new law. For example, norms that sanction the conduct of leaking or sharing documents without official consent are often spread over several laws.

6. *Norms that include any provision to classify or disclose government documents under a request bases (usually known as petition laws)*. In many countries, the right to petition poses certain obligations and procedures to public servants in answering the publics' petitions. The new access to information law's procedures must not be mixed up with those; rather, public servants should be clear about the new process and be able to handle and treat petitions and information requests differently. In this category, national security legislation should also be taken into account.

7. *Norms that create special secrets, such as fiscal, bank, fiduciary, commercial, and industrial secrets*. The new access to information law should, in any case, define more accurately these preexisting secrets in relation to the categories it presents (exempt or public information).

8. *Norms that establish judicial or quasi-judicial procedures*. Norms that establish judicial or quasi-judicial procedures. The appeals mechanism provided for in the law should have legitimate procedures in the line of equivalent institutions within government, such as an existing Ombudsman. Disregarding this element could diminish legitimacy of the oversight body's actions.

9. *Rights balancing tests / constitutional control*. When existing, this mechanism is found in the country's higher-level legislation. In constitutional legal systems, the new access to information law must not install such tests if there is no public interest or rights balance control provided by the constitution.

10. *Constitutional and legal provisions on data protection or Habeas Data.* Since access laws create a different administrative procedure to handle requests and also, distinct protection of the documents and data, a close look must be given to preexisting provisions on this subject.

11. *Regulation on records management.* Implementing an access to information law without a records management regulation in place creates endemic problems that reverberate in legal efficacy. This legislation must be differentiated from that of historic records. As in-depth discussion of records management policies is provided in *Chapter 5: Adoption of Effective Information Management Policies and Systems to Properly Create, Maintain, and Provide Access to Public Information.*

B. Adoption of Model Law and Amendments to Existing Law

The Model Law responds to a need to set standards for access to information protection in the region, therefore, existing access to information legislation that contradicts the principles set forward by this Model Law should be amended. Reformation of existing access to information laws in the line of the Model Law must be seen as a sensitive democratic step to meliorate and dignify people's lives and the bureaucratic relationship with citizens. Regardless of its moral justification, states party to the American Convention on Human Rights are legally obliged to comply with the holding of the *Claude Reyes vs. Chile* case, where the Inter-American Court of Human Rights mandates to amend existing legislation contrary to the principles of the right of access to information. In this line, the Recommendations on Access to Information of the OAS,

CP/CAJP-2599/08 states that states must "ensure that any exception is previously established by law and responds to an objective permitted under international law." The Declaration of Principles of the Inter-American Commission on Human Rights recalls article 13 of the American Convention of Human Rights where (principle 4) "Access to information held by the state is a fundamental right of every individual. States have the obligation to guarantee the full exercise of this right. This principle allows only exceptional limitations that must be previously established by law in case of a real and imminent danger that threatens national security in democratic societies."

Regarding the adoption processes of access to information laws, experience has shown that it is best when governments, civil society and media work together with congressional leaders. This type of alliance often leads to access to information laws that are more protective of the interests of citizens, and also to a law that is publicly debated and shared with the rest of society thanks to the dissemination role of the media. Indeed, a law enactment process that has been publicized enshrines a merit of transparency in itself since citizens learn about the right to seek information and the obligation of the governmental organizations to share it. The process brings about a more legitimate and democratic final outcome. Nevertheless, it should be acknowledge that there are different paths to achieve the adoption of the laws and, in any case, political scenarios should be analyzed before defining a legal adoption strategy.

Once passed, it is important to maintain the credibility of the law among citizens and stakeholders, even when the implementation is problematic. It is especially important that public servants remain confident in the law and its future benefits, despite the work that they confront in its implementation. This can be achieved through trainings and capacity building. For more information on capacity building for information users and providers, see *Chapter 6: Capacity Building for Information Users and Providers*.

In order to have as efficient an implementation possible, governments must consider that a process of "cleaning the house before opening the door" should take place. Administrative rules that allow state secrets, secret budget items and the no conflict of interest prohibiting laws, are the types of measures to be removed before adopting the access to information law, since they entrench principles contrary to good governance and respect for rights.

C. Rescinding of Laws and Policies Contrary to Access to Information Regime

Inconsistent legislation causes confusion between the past confidential information legislation and the new grounds of refusal that the access to information law provides. Public servants, who are the day-to-day applicants, need to implement this law under a safe ground of predictability and certainty, therefore, rescinding and amending an information regime contrary to the limited exemptions in the access to information law is essential.

In countries such as Colombia, Ecuador and Mexico, the supremacy of the right of access to information is ensured by a constitutional provision, which is the highest-level norm of the civil legal systems. In such cases, the constitutions establish that any law that contradicts a constitutional fundamental right is unconstitutional and shall be derogated. Constitutions, such as the Mexican Constitution, reinforce the respect of fundamental rights by stipulating that international treaties, along with the Constitution and national laws are the *supreme norms*. Hence, in those countries, Article 13 of the Inter-American Convention on Human Rights has the same legal power as any domestic law.

To proceed ensuring the supremacy of the access to information model law among contrary provisions, it is recommended that the new access to information law overrides all other secret or classification of information laws, by rescinding or amending those norms contrary to access to information. For instance, the access to information law of Nicaragua and Panama explicitly mandates that this law will prevail above any other law in case of consistency or contradiction. In no case should the access to information law recognize other classification of information regimes and remit to it.

In some countries, such as Canada, there has been a proposal made such that where legislation could conflict with the right of access to information it should be brought to the attention of the Ombudsman or a legislative Committee that could issue an opinion before the legislation is passed. In any case, a permanent parliamentary review process of new draft legislation that may contradict the right is also highly recommended.

Legislation that conflicts with this Model Law is mostly the following: -

1. State secrecy laws have a long history in the penal codes of the region. They sanctioned the revelation of "state secrets," meaning any information that could harm the economic or military activities of a State, would be considered a "national offence" (*delito contra la patria*). The laws are characterized by using the grounds of "national security" as a broad shield to hide information from public knowledge. State secret provisions were derogated from penal codes of Mexico and Peru during the twentieth century, where they were mainly used to cover discretionary actions and maladministration taken by the government.

2. Ministerial certificates laws are laws that permit a minister to issue a conclusive certificate, that cannot be questioned by an appellate body, ordering that a document is secret. Lower level legislation must not undermine or contradict the access to information law. When this is done, it subtracts credibility from the government's implementation of the law. Best practice in Chile and Peru show that a constitutional prescription ensures an absolute majority of the Congress to introduce new secrets or reserved information legislation.

3. Privacy and data protection, or *Habeas Data* laws can run contrary to the access to information regime. The rights to privacy and to access information should exist in harmony. Many countries in the region have *habeas data* provisions adopted prior to the adoption of access to information laws, so classification procedures and protection is already a familiar concept for the government. Caution must be kept when denying information under the grounds of the different laws. For instance, the access to information law of Mexico defines confidentiality with very narrow language, so that this category only protects the private lives of individuals.

4. Secondary laws or regulations that create other categories of classification of documents than the ones listed in the law can also conflict with the access to information law. Agencies and organisms under the access to information law, because of reasons of autonomy, can develop secondary legislation or regulations to incorporate the law's principles into their own system. Secondary legislation and regulations must not be contrary or exceed the access to information law's mandate, where new classification categories or different procedures for requesting and classifying information appear.

5. Public records legislation and policies should be reconciled with the access to information laws. Archives management policies set a special protection regime, classification periods, and accessibility to historic records. It is important to seek interplay and a close coordination between the records keeping and the right to access to information authorities to clearly define competence among the government information and records.

D. Enacting Supporting Laws Which Promote Openness

The enactment of supporting legislation is not only recommended to promote openness in the various areas of government' actions, but most importantly, to grant the effectiveness of a transparent and rights protection regime. Supporting legislation that will further promote openness while promoting the principles in the access to information law, include: -

1. Whistleblower protection encourages public officials to denounce wrongdoing of other officials. At the same time, whistleblower protection provides effective punishment to offenders and protection to the individual reporting the wrongdoing, in order that they may remain in their position without the risk of being judged or isolated internally.

2. Open meetings laws need not require that all meetings must be open, but strict policies should be established to withhold "executive meetings." In any case, a minute of the latter should be released.

3. Public records laws should standardize records management.

4. Data protection regimes should live harmoniously with the access to information legislation.

5. Civil service laws must be enforced to incorporate professional practices and knowledge of the access to information policies and procedures.

6. Constitutional control or rights balancing tests must exist because access to information is a right that must live harmoniously with other rights, like privacy and security rights. The harm tests and public interests tests must develop special criteria to be applied by courts and administrative tribunals. This should be established by the constitution or the higher-level legislation. These are substantial tools for the oversight bodies to balance conflicting rights on a case-by-case practice. The burden of these tests should not fall on the petitioner.

7. Laws that recognize the judicial value of documents obtained in discovery.

E. Timeline for Implementation

Once the law is enacted, governments need to develop a plan of action that must list key activities, indicate the responsible parties for each activity, and establish a timeline for completion of the implementation of the law. Consequences for not having an implementation plan are major. Without a plan, responsibility for implementation blurs and each agency will try to implement the law at its own convenience. It is likely that if no high-level political will behind the initiative, despite the law having come into force, actions for implementation will certainly

not be taken. Overall, an implementation plan keeps implementation homogeneous among the offices and ensures that the same service is provided to requesters within the government, at the same time, reassuring that the government is ready to comply with the legal mandate.

There are various ways to design a phased in approach plan. In some countries, the implementation occurred simultaneously among all offices under the law, after a *vacatious legis* period of at least a year. But others have adopted a staggered plan allowing the most ready offices to comply with the legislation rapidly, while allowing those mainly concerning security and vast administrative records storage to comply later. In any case, this basic plan should be clearly established in the access to information law.

From experiences such as those in the United States, Chile and Mexico, it is recommended that the full implementation process takes place in no more than two years. During this period of time, the first six month stage could be, for example, to comply with the proactive publication of information on official websites. This could be followed by the installation of information officers, training for public officials and the establishment of a public records management strategy. Taking into account the poverty levels in many countries in the region, implementation at the municipal levels of government will usually takes the longest amount of time when budgetary and infrastructure resources are scare. Therefore, efforts at the very local level must be taken from the first day of the implementation timetable.

It is recommended that a staggered implementation plan be adopted for the purpose of: a) giving the municipal and local level governments longer deadlines to systematize records and organize the administration; b) giving governments sufficient time to review and amend legislation contrary to the right to information; c) giving governments the time to enforce administrative and institutional provisions to avoid conflict of interest relations, secret budget items or any maladministration practice.

Experience also has shown that a period longer than two years for implementation is detrimental for the effective process because of the great personnel rotation within the governmental agencies, that by the time the law comes into force, new imperative training needs arise. Indeed, to stagger implementation agency by agency is not recommended when the law provides for the possibility of transfer of information requests as this is only feasible when all agencies are covered.

KEY POINTS
ADOPTION OF COMPREHENSIVE FRAMEWORK

- The new access to information regime should be integrated and reconciled with other existing legislation, such as laws on state secrecy, data protection, habeas data and public records.

- Inconsistent existing legislation that runs contrary to access to information should be rescinded or amended.

- Supporting legislation must be considered in order to enhance the right to access to information.

- Once the law is enacted, governments need to develop a plan of action that must list key activities, indicate the responsible parties for each activity, and establish a timeline for completion of the implementation of the law.

CHAPTER 2: EXCEPTIONS FROM DISCLOSURE

Implementation of the system of exceptions to the right of access to information is a core issue for the effectiveness and observance of this fundamental right. It is a process of legal interpretation based on the presumption of publicity over other interests. This chapter examines that presumption in relation to the interests protected by the exceptions from disclosure provided in the Model Inter-American Law on Access to Information.

The first thing that needs to be considered is the creation of interpretation guidelines for the exceptions that elaborate how the section on exceptions to access to information in the Law should be applied. Next, it is important that those guidelines make it clear that the legal causes for denial of access may only be interpreted by those government officials empowered to do so. In countries such as Mexico and Peru the power of denial of access is delegated to high-ranking officials who belong to committees or areas charged with reviewing information inside government entities.

In addition, Section V of the Model Law includes an internal appeals process, whereby the requester, having been informed that the information they seek is exempt from disclosure, may lodge an appeal with the head of that public authority. In processing such appeals, the interpretation guidelines and procedural standards addressed in this section must be observed with particular care.

A. Principles of Interpretation of the Exceptions

The principles that guarantee the right of access to information that the Model Law provides, and which is consistent with the standards of the Inter-American system, must be included in every procedure where the exceptions from disclosure are applied.

Legal Recognition of Exceptions
The Office of the Special Rapporteur for Freedom of Expression, Inter-American Juridical Committee, Inter-American Commission, and Inter-American Court of Human Rights have all found that any exceptions to the right of access to information should be set down in a law. Therefore, in exempting information from disclosure it is obligatory to do so in accordance with the law, based on limits on the right of access to information that meet the conditions of proportionality, legitimacy and need.

Restrictive Interpretation
Exceptions to the dissemination of information should not become the rule – the right of access to information should be interpreted in the light of the principle of maximum disclosure. The exceptions contained in Article 41 of the Model Law should be interpreted in keeping with the literal wording of the legal mandate and if there is any doubt over whether or not information should be reserved, the legal presumption requires disclosure.

Principle of Good Faith
As with any application of the Law, one should expect obligated persons to act in good faith even in exempting information from disclosure. In its 2008 Report, the Office of the Special Rapporteur for Freedom of Expression considered that this principle requires all public servants

to interpret the law in such a way as to contribute to the fulfillment of the purposes of the right of access to information.[2]

Reasoned Decision and Grounds
The regional standard on this principle provides that in interpreting exceptions to the right of access to information the official must ground their denial of disclosure on a legal precept and offer reasoned legal arguments as to why the information cannot be divulged.

Preeminence of the Law Over Other Laws that Create Exceptions
In most countries the existence of laws that contradict or run contrary to the right of access to information pose an obstacle and significant complications for government officials responsible for reserving information. The predominant principle on the standard of interpretation of the right of access to information is that the rules on access to information prevail over other laws contrary to the system of disclosure. In their Joint Declaration of 2004, the Rapporteurs for Freedom of Expression stated unequivocally that "urgent steps should be taken to review and, as necessary, repeal or amend, legislation restricting access to information to bring it into line with international standards in this area, including as reflected in this Joint Declaration."[3]

B. Private Interest

The right of access to information is not an absolute right; it is limited by legitimate personal and public interests. Article 41 (a) of the Model Law establishes exceptions to disclosure based on the following private interests: -

a. *The right to privacy of individuals, including life, health or safety.* These rights are in most countries protected by constitutional provisions. Therefore, the express consent of the individual concerned is required for the disclosure of that information. Accessing it without said consent is an infringement of their legal interests.

b. *Legitimate commercial and economic interests* where the information was provided in confidence are protected by provisions of private law that safeguard a person's property, commercial, economic, and financial rights. It should be noted that it is not the fact that the information was relayed in confidence that automatically protects it under the exceptions to disclosure. Instead, the interest must also be a legitimate commercial and economic interest.

c. *Patents, copyright and trade secrets*, where an individuals' interest is at stake and intellectual property legislation protects this type of commercial property.

---

[2] Catalina Botero, *Report of the Office of the Special Rapporteur for Freedom of Information*, OEA/Ser.L/V/II.134 Doc. 5, approved by the Inter-American Commission on Human Rights on Feb. 25, 2009.
[3] *International Mechanisms for Promoting Freedom of Expression - JOINT DECLARATION* by the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression, 2004, available at http://www.cidh.org/Relatoria/showarticle.asp?artID=319&lID=1.

With respect to the invocation of private interests as grounds for denial of the right of access to information before a jurisdictional body or an information review committee, the organs of the Inter-American system have determined in their interpretation of Article 13 of the American Convention on Human Rights that the burden is on the state to justify a denial of access to information, not on the requester or the party to whom the information pertains.

This provision of the Model Law also follows the right to self-determination with regard to a private individual's information; that is, the recognition that a person has the right privacy and, consequently, must consent to disclosure before such information is made public.

C. Public Interests

Article 41 (b) of the Model Law establishes exceptions to disclosure based on the following public interests: -

1. *Public safety*. Legislation and/or jurisprudence must ensure that a definition must be clearly laid out and it must be possible to determine what harm disclosure of the information would entail.

2. *National security*. Where the definition of national security should be clearly set down in a law or case law that provides concrete elements for the determination of potential harm.

3. *The future provision of free and frank advice within and among public authorities*. This exception protect deliberate process of public authorities in order to ensure effectiveness of public administration and the State mandate.

4. *Effective formulation or development of policy*. Both universal and Inter-American system standards promote openness, transparency and civil society or affected groups participation in the formulation of development policies, grounds for refusal could be argued, once the later has been granted, and deliberation process to the final formulation is pending.

5. *International or intergovernmental relations*. This legally prescribed limit is applied when it is possible to determine that disclosure would harm the public interests of a State where its international relations are concerned.

6. *Law enforcement, prevention, investigation and prosecution of crime*. This exception protects the judicial proceeding and strategy in criminal cases where disclosure of the information before a final decision is returned could affect the course of the investigation and procedure for dispensation of justice.

7. *Ability of the State to manage the economy*. This exception protects state activities necessary for ensuring the economic and financial stability of the country.

8. *Legitimate financial interest of a public authority*. This exception protects public finances and the best expenditure of them.

9. *Tests and audits, and testing and auditing procedures*. This exception prohibits disclosure where it might undermine a public examination process and its final outcome.

It should be noted that, independently of all the exceptions provided in Article 41 of the Model Law, Article 45, provides that none apply in cases of violation of human rights or crimes against humanity, the latter as defined in the Rome Statute of the International Criminal Court.

D. Partial Disclosure of Information

Article 42 of the Model Law recognizes that a single record may contain both, information subject to exemption, and, information subject to disclosure. This latter information, where no real threat to a private or public interest is posed, should be disclosed. In any case, a detailed explanation of the information withheld and its grounds should be provided to the requester.

E. Length of Restrictions on Access to Information

The Model Law provides that exceptions for public interests do not apply to records older than 12 years. However, that restriction is lifted when the reasons that led the information to be reserved cease to have effect. By the same token, this restriction may be extended on the basis of reasoned arguments and grounds to show that the reasons that originated the exemption persist and that to lift it would be contrary to public interest.

F. Public Interest Override

The public interest and harm tests are standards against which the justification for an exemption to disclosure must be weighed, to determine if it meets requirements of proportionality and necessity. In applying these tests it is necessary to adopt a restrictive interpretation of the exemption, as is mentioned in this chapter. The presumption of publicity thus requires an exemption be the least restrictive as possible; that is: non-disclosure must have a direct effect on the exercise of a particular exception, be proportionate to the public or private interest protected, and interfere to the least extent possible with the effective exercise of the right of access.

In the words of the Special Rapporteur for Freedom of Expression, an exception must pass a three-part test: a) it must be related to a legitimate aims that justify it; b) it must be demonstrated that the disclosure of the information effectively threatens to cause substantial harm to this legitimate aim; and, c) it must be demonstrated that the harm to the objective is greater than the public's interest in having the information.[4]

[4] Catalina Botero, *Report of the Office of the Special Rapporteur for Freedom of Information*, OEA/Ser.L/V/II.134 Doc. 5, approved by the Inter-American Commission on Human Rights on Feb. 25, 2009.

KEY POINTS
EXCEPTIONS FROM DISCLOSURE

- In the interpretation of the exceptions, public officials should: -
    - Issue exemptions in accordance with the law, based on limits on the right of access to information that meet the conditions of proportionality, legitimacy and need;
    - Ensure that exceptions to the dissemination of information should not become the rule – the right of access to information should be interpreted in the light of the principle of maximum disclosure;
    - Act in good faith even in exempting information from disclosure; and
    - Ground the denial of disclosure on a legal precept and offer reasoned legal arguments as to why the information cannot be divulged.

- In applying the public interest harm test, it is necessary to adopt a restrictive interpretation of the exemption. That is, the exemption option that least restricts the right of access to public information should be adopted. The exemption should: i) be conducive to the attainment of the objective; ii) be proportionate to the interest that justifies it; and, iii) interfere to the least extent possible with the effective exercise of the right.

CHAPTER 3: MONITORING, ENFORCEMENT, AND EFFECTIVENESS OF THE LAW

In instituting a functioning access to information regime, it is critical to pay great attention to the oversight and enforcement mechanisms and to the establishment of tools for determining effectiveness of the system. A national oversight agency monitors and supports implementation of the access to information legislation; may set policy and offer recommendations; assures consistency among agencies; promotes the right of access to information; and can provide requisite training and capacity building for key civil servants as well as lead campaigns to promote public awareness and understanding of the right of access to information law.

Assuring a procedure that allows persons to enforce their right to information when a request is ignored or denied, or when their rights are otherwise impeded, is arguably the most important set of provisions within an access to information law.[5] Without an independent review procedure of decisions, the right to information will quickly become discretional and based on the whims and desires of the persons receiving the request. If the enforcement mechanisms are weak or ineffectual it can lead to arbitrary denials, or foment the "ostrich effect", whereby there is no explicit denial but rather the government agencies put their heads in the sand and pretend that the law does not exist. Thus, some independent external review mechanism is critical to the law's overall effectiveness.

The institutional framework and apparatus developed for oversight and enforcement of the right to information vary. This section will discuss models for monitoring and enforcement, which range from more limited oversight and intermediary enforcement mechanisms to those whereby the bodies are mandated and vested with wide-ranging powers and responsibilities. While the Model Law advances an exemplary system, whereby the oversight and enforcement duties are vested in an Information Commission with more expansive powers, ultimately, the decision regarding which model will function best depends greatly on the specific political, economic and social context and needs of the jurisdiction. Nevertheless, what is increasingly clear is that in order to ensure full and continuing compliance with the law, there is a need for statutorily mandated instruments dedicated to the promotion, monitoring and enforcement of the access to information regime.

Finally, access to information statutes should incorporate a mandate and the means for determining the overall effectiveness of the regime. Quantitative and qualitative data related to the use of the law, most frequently asked for documents and information, effectiveness of automatic disclosure, agency responses, costs, and impact will allow governments to identify and resolve challenges and recognize successes and best practices.

A. Oversight

An oversight body with the responsibility for coordinating implementation efforts across government agencies, promoting training of functionaries and public education, responding to agencies questions, and ensuring consistency and sustainability is critical to the success of any access to information law. Experience indicates that without a dedicated and specialized oversight

---

[5] *See* Neuman, Laura, "Access to Information Laws: Pieces of the Puzzle," in The Promotion of Democracy through Access to Information: Bolivia, Carter Center, 2004.

body the compliance rate is lower, the number of requests more limited, and the right to information eroded.[6] Moreover, without a continuous oversight body, government efforts are dispersed and diluted with no clarity in responsibilities, lack of clear guidelines, and reduced ability to conduct long-term planning and to promote best practices, thus costing governments more in terms of human and financial resources. For those jurisdictions without an oversight body, there is no one for the agencies to contact for support or with questions and concerns, and the weight of implementation and public education falls squarely on their already overburdened shoulders. In these cases, users are forced to navigate the systems on their own and public servants are burdened with additional responsibilities, but often less training and resources.

There are a number of models for establishing an oversight body, but perhaps the most effective – as highlighted in the Model Law – is a system with a dedicated Information Commission responsible for overseeing the functioning of the access to information regime as well as its enforcement. Not only is there a cost benefit in combining the functions of oversight and enforcement in one Commission, but also the benefits of a specialized unit that can ensure consistency across the related matters. For instance, if a number of appeals are being brought against the same agency or for similar reasons, the Commission can both rule on the issue as well as insure additional training in order to stem the need for future litigation. In some jurisdictions, the duties are vested in an existing body, such as the Ombudsman or is placed in a body that is separate from an Information Commission, with obligations for both oversight and enforcement., In all cases, the oversight bodies have served to enhance the government's implementation efforts and ensure that the objectives of the law are more fully met.

Regardless of which system is selected, it is vital that the oversight body or unit enjoy a statutory mandate. Where oversight is voluntary, over time the initial units have seen staff reduction, insufficient funding or complete disbandment. Voluntary oversight mechanisms have emerged when the legislature failed to mandate a national coordinating body as part of the law or regulations, but practice dictated the need. In these situations, the lack of a specifically legislated oversight body has resulted in a corresponding low awareness of the law, no tracking or monitoring of implementation, and a dismally low request rate. As experience builds in the field, it points to the need for an oversight body that is specialized, dedicated to the issue, well-staffed and properly resourced. In many cases, this suggests that adding the access to information oversight function to an already stretched Human Rights Ombudsman or like institution with disparate mandates may not serve the overall goal.

Therefore, as the Model Law provides, in developing statutory language and implementation of a proper oversight mechanism, the legislation should make specific provision for the Commission to be in charge of monitoring implementation efforts; receiving monthly reports and assisting in the annual report to the legislature; and leading efforts for training of public servants, promotion campaigns and necessary material development, such as standard operating procedure manuals. Ideally, the Commission also would be responsible for reviewing the manner in which records are maintained and managed by public authorities and assure the automatic publication of documents by the public authorities, in line with best practice. The agency itself should be designed and staffed to ensure capabilities to collate reports and provide statistical analysis, including number of requests and complaints, and to monitor all systems.

---

[6] Id.

B. Enforcement

Compelling adherence to the tenets and principles of access to information laws through well-designed and implemented enforcement mechanisms is paramount to ensuring the statute's overall effectiveness, particularly in cases with poor implementation or wavering political commitment.[7]

Although jurisdictions around the world have varied in the design of their enforcement mechanisms, there is a growing recognition that the optimal system would be: -

- independent from political influence;
- accessible to requesters without the need for legal representation;
- absent overly formalistic requisites;
- affordable;
- timely; and
- preferably specialist, as an access to information laws is complex, necessitating delicate public interest balancing tests.[8]

More specifically, advocates have called for legal provisions that guarantee "a right to appeal any decision, any failure to provide information, or any other infringement of the right of access to information . . ."[9] The recent Americas Regional Findings and Plan of Action for the Advancement of the Right of Access to Information calls on all states to assure that "enforcement mechanisms are accessible and timely, including establishing intermediate appeals bodies, providing necessary human and financial resources, and capacitating all judges and any others responsible for resolving access to information claims."[10]

It is widely accepted as the norm that in any appeal of an information request, the burden of proof for the negative decision lies with the public authority. This includes decisions related to release as well as costs and transfer of requests, where applicable. Additionally, the burden always falls on the public authority to demonstrate convincingly that the disclosure of requested information will cause harm to the protected interested, and that this harm outweighs the public interest, as delineated in the exceptions section of the Model Law.

In most jurisdictions with an access to information law, a requester that has received a negative decision, whether it is a complete or partial denial of information, lack of response, or other determination ripe for appeal, may seek internal review[11]. This often entails a review of the decision by a more senior administrator or Minister within the same agency that made the initial negative determination. In many jurisdictions, internal appeals are mandatory before the aggrieved requestor is eligible for external review. The Model Law provides the opportunity for internal appeal, but does not require it prior to the issuance of an appeal to the independent

---

[7] *See* L. Neuman 'Enforcement Models: Content and Context", Access to Information Working Paper Series, World Bank Institute, 2009.
[8] Id.
[9] *See* Carter Center "Atlanta Declaration and Plan of Action for the Advancement of the Right of Access to Information," International Conference on Access to Public Information, Atlanta, GA, 2008.
[10] *See* Carter Center "Americas Regional Findings and Plan of Action for the Advancement of the Right of Access to Information," Americas Regional Conference on the Right of Access to Information, Lima, Peru, 2009.
[11] There are a few countries that do not provide internal review of initial decisions, such as France, but these are unique cases.

Commission. However, should a requester choose to lodge an internal appeal, the Model Law suggests that the time for agency response be specified and limited in order to insure that this stage does not incur unnecessary additional delays.

In considering whether to make the internal appeal obligatory, there are arguments that focus on delay as a claimant exhausts administrative appeals and whether it serves as merely an obstacle before one can seek an independent review. However, surprisingly perhaps, anecdotal and statistical evidence indicates a high level of positive resolutions by internal review, without necessitating appeals to the Commission or Courts, which would potentially bear more costs in terms of time and resources. Thus, whether mandatory or optional, it is beneficial for the legislation to provide some system of internal appeals.

C. Models of Enforcement

Following an internal review, if still dissatisfied or if the internal review is bypassed, the information requester is afforded the opportunity for appeal to an external body. While the Model Law calls for a specific enforcement system, as with the oversight mechanisms, there are a number of potential models, including[12]:

1. An Information Commission(er) or Appeals Tribunal with the power to issue binding orders
2. An Information Commission(er) or Ombudsman with the power to make recommendations
3. Judicial Review

Ultimately, the model of enforcement selected for appeals outside of the agency depends highly on the specific context and culture – political, economic and bureaucratic - of the country as well as budgetary considerations, but the first model, which is included in the Model Law, has proven successful in a variety of jurisdictions.

1. Information Commission(er) or Tribunal: Order-Making Powers

As presented in the Model Law, in this system external appeals are made first to an access to information commission(er) or specific appeals tribunal with the power to issue rulings and binding orders. This model often is considered the best of the three models in meeting the basic set of enforcement principles. Appeals to bodies such as an Information Commissioner often are more accessible as there is no need for legal representation, it is affordable as there are no court costs or other fees[13], and, in the best cases, highly independent. This system can allow the

---

[12] This and the following sections draw largely from L. Neuman "Enforcement Models: Content and Context", Access to Information Working Paper Series, World Bank Institute, 2009.

[13] In some jurisdictions, such as Ireland, there are application fees for submitting certain types of cases to the Information Commissioner for review. For example, if the request is for personal information or the agency has failed to respond then the application fee if waived. In other cases the application fee may be £50 or £150, depending on the nature of the appeal. For comparison, the Circuit Court application fee is £60 or £65, depending on the type of case, £60 for notice of trial plus £11 for every affidavit filed, £50 for official stamp of an unstamped document given as evidence, and £5 for every copy and the Supreme Court application fee is £125 plus additional costs for filings and copies. See The Court Services of Ireland,

decision-makers to become specialists in the area of access to information. With the power to order agencies to act or apply sanctions, this model serves as a deterrent to the government and can alleviate the need for further appeals to the Courts. Binding decisions are issued through a written ruling, which in mature jurisdictions creates a body of precedent that can guide future internal agency and commissioner decisions and facilitate settlements.

This model lends itself to the principles of independence, affordability, accessibility, timeliness and specialist, but as with any model, these benefits are not always realized. There are some potential disadvantages, but again in practice these often are mitigated by this model's benefits. Quasi-judicial proceedings, such as those before a Commission with order-making powers, may become overly formalistic and legalistic. Decisions contain jargon, which may be challenging for requesters to understand, and the administration may be slower than the Commissioner model with fewer powers as more exhaustive investigations are undertaken, due process requirements must be fulfilled, and lengthy judgments must be written and issued. These models may be more costly for the state as new institutions are established and staffed, and technical procedures (such as summons and notice, in-camera reviews, and hearings) are met to satisfy legal necessities. Finally, although called "binding," in the face of agency non-compliance there remains the need for judicial involvement and in the most extreme cases police engagement.

As posited in the Model Law, the Commission is directed to establish rules and regulations that ensure its proper functioning, such as a tracking system of appeals and notice to all parties, and ensure that all parties have an opportunity to be heard. To support their order making powers, the Commissioners are vested with the ability to compel witnesses and evidence and make on-site inspections. To strengthen further the authority of the Commission, the law could provide the Commission the right to instigate investigations on its own accord, without a specific appeal lodged.

The Model Law provides an opportunity for mediation. This is an area that could be expanded to allow for a more general mandate in order to clarify and resolve some – or all - of the contested issues more quickly. Notably, the Model Law follows the present Mexican law example of only providing a right of additional appeals to the requester. If the requester remains unsatisfied, she has the legal ability to seek further review before the Courts, through judicial review, while the agency is bound by the Commission's decision. Finally, as discussed above, throughout the appeal proceedings the burden of proof for any negative decision rests on the public authority.

Although the Model Inter-American Law on Access to Information recommends establishing an Information Commission, there are two additional appeals processes applied in jurisdictions around the world.

2. Information Commissioner or Ombudsman: Recommendation Power

The second model utilizes an Information Commissioner or Ombudsman[14] with more limited faculties for enforcement. In this design, the enforcement body is vested solely with the power to issue recommendations to the relevant administrative agency or public functionary. These Commissioners or Ombudsmen often possess weaker powers of investigation and with no order-

---

Circuit Court Fees, Schedule One and Two and Supreme Court and High Court Fees Order Schedule One Part Two.

[14] The term Information Commissioner with recommendation powers and Ombudsman are used interchangeably in this Chapter.

making powers tend to emphasize negotiation and mediation. The benefits of this model include a lack of formalism, encouraging accessibility for complainants, and it can be the speediest, as the investigations are generally limited to unsworn representations.[15] The abridged powers may encourage less adversarial relations between the recommender and the implementer, with the Ombudsmen relying more on resolution through persuasion and dialogue, thus potentially leading to greater compliance. Finally, the independence of an Ombudsman may be augmented by their status as officers of the legislature (Parliament) rather than as a quasi-independent part of the executive, which often is the case for Information Commission(er)s with order-making powers.

But without the "stick" of order-making powers, recommendations may not be followed.[16] Over time, even those bodies vested with the more limited powers of investigation and recommendation may become increasingly formalistic, contentious and slow. Moreover, with this model a body of rulings may not be created that can serve to guide future agency determinations on disclosure[17], and the Ombudsman may be prohibited from instigating inquiries without a formal complaint. Emphasis often is placed on mediation and negotiated resolution, notwithstanding that one of the parties (requester or agency) might clearly be correct in its assertions. With fewer powers of investigation and order, there may be more limited resources, and if the Ombudsman has a shared mandate to receive complaints on a variety of issues he or she may have less dedicated time to freedom of information and potentially less specialization.

3. Judicial Review

The final enforcement model provides for appeals directly to the judiciary. When a request for information is denied, the requester must appeal to the federal or administrative court. The main benefits of such a model are that the courts have the power to order the release of information if inappropriately denied, possess wide-ranging powers of investigation, have clearly established mechanisms for punishing agency non-compliance, and they may determine the procedural and substantive matters *de novo*.

However, in practice there are a number of disadvantages to this model. For most citizens, the courts are neither accessible nor affordable. Often for successful litigation under the judicial model, the information requestor may need to hire an attorney or advocate and pay the many court costs. In most jurisdictions, the court calendars are overwhelmed and it may be months or years before the case is heard and even longer to receive the written decision, perhaps making moot the need for the information.

The cost, the delay, and the difficulty for citizens in accessing the courts serve a chilling effect on the utilization of this enforcement mechanism. With all these obstacles, the deterrent effect that courts often play is minimized and may actually encourage a perverse incentive among some civil servants to ignore the law or arbitrarily deny requests as they recognize that most persons will not be able to effectively question their decisions. Moreover, in many newer democracies often there

---

[15] In Hungary, the annual report from 2001 indicated that the Information and Data Protection Commissioner took an average of only 52.6 days to fully process a case and issue a recommendation. See Neuman, Laura "Mechanisms for Monitoring and Enforcing the Right to Information Around the World" in Access to Information: Building a Culture of Transparency, Carter Center, 2006.

[16] This is not always the case. For example, since 1987, there has been 100% compliance with all New Zealand Ombudsmen recommendations on access to official information. Prior to that, non-compliance only was due to individual Ministers exercising the veto power provided in the legislation.

[17] Some jurisdictions, such as New Zealand, may publish "casenotes," which can be relied upon by government agencies as a decision-making guide.

is a lack of trust in a judiciary that may not yet have matured into a strong, independent branch of the state. Finally, consideration must be given to the litigation costs for the government (and taxpayer) and the burden on the court system.[18]

D. Establishment of Commission

In the case where a Commission has been chosen as the enforcement model, as conceived in the Model Law, consideration must be given to the establishment and implementation of the office.

1. Independence

Paramount to the success of this model is its independence. A series of factors may determine the real (or perceived) independence of this office and its officers, including the manner of selecting the Commissioners, their term limit and procedures for dismissal, from which branch of government they receive their powers and to whom they report, and the autonomy in budgeting.

i) Selection Process

The selection process, and threshold assents for appointment are integral to the perceived legitimacy of the Commission. There are a number of ways in which selection may occur. One common method is through executive appointment, sometimes in partnership with the leader of the opposition, such as in Jamaica where the Appeals Tribunal is appointed after consultation with the Prime Minister and leaders of the opposition. In other cases, appointment is through Congressional or Parliamentary selection. The Commissioners may be elected wholly by Parliament with no Executive branch involvement, or more often, the President presents a closed list of candidates to the Legislature for selection or approval, either through assent or lack of dissent. This is the case in Canada, whereby the Information Commissioner is nominated by the executive and appointed through committee resolution from both Chambers. Moreover, in Mexico, the five commissioners of the Federal Access to Information Institute are nominated by the executive branch, whose nominations may be vetoed by a majority of the Senate or the Permanent Commission. In Honduras, the Commissioners are elected by Congress with a two-thirds vote, after nomination by a committee comprised of the President, Attorney General, Human Rights Commission, National Convergence Forum, and Superior Court of Accounts. The Model Law suggests a number of important mechanisms for increasing confidence in the selection process, including mandating both the executive and legislative branches of government involvement in the selection process as well as engaging public participation. Moreover, it emphasizes transparency in the decision-making.

In addition, the Model Law calls for the selection of an odd number of Commissioners – such as five – in order to facilitate voting and to have a sufficient number of Commissioners to diminish potentials for political capture. In cases where there is a single Information Commissioner, while it may entail less strain on the budget, the potential for politicization of the person or the office is greater. Where there have been three Commissioners, such as in some states in Mexico, there

---

[18] In a 2002 case in South Africa that went to the High Court, the Auditor-General theorized that they had spent over $300,000 Rand (close to $30,000 US) in defending their decision to deny information. See, "The Promotion of Access to Information Act: Commissioner Research on the Feasibility of the Establishment of an Information Commissioner's Office", The Open Democracy Advice Centre, Cape Town 2003.

have been problems of deadlock where two like-minded persons are consistently opposing the one. For that reason, although more expensive, five Commissioners may be preferable.

ii) Length of Service

Once appointed, the term of office becomes a key consideration for continuing independence. Periods of appointment are in many respects a balancing act. If term limits are too short, then the Commissioner may be more concerned with pleasing those responsible for subsequent appointments than in serving the duties of his or her post. On the other hand, if terms are too long then officers may be less responsive to the shifting trends of openness and needs of all constituencies. At a minimum, the term of service should be longer than the term of the President or appointing body, thus reducing potential for politicization. The length of term is relevant not just to ensure sufficient independence, but also the functioning of the Commission. As previously noted, enforcing the right of access to information often necessitates some specialization, which takes time to acquire. Thus, shorter terms could signify less proficiency in the body. Examples of terms include Canada's seven-years, with possibility of one seven-year extension, Chile's seven-years with no potential for additional terms, and Honduras and Jamaica's five-year non-renewable terms.

iii) Dismissal or Termination

Foremost in assuring the ongoing independence of the Commission are the standards for dismissal. Generally, members of the enforcement body should only be suspended or removed "for reasons of incapacity or behavior that renders them unfit to discharge their duties."[19] These behaviors, as illustrated in the Model Law, may include conviction as a criminal offence or infirmity that affects the individual's capacity to fully serve. The statute or implementing regulations should not provide additional reasons for removal that could in time become politicized or manipulated.

iv) Budget Sovereignty

Lastly, budget sovereignty is a significant component to overall independence and autonomy. If the Commission is vested with its own line item in the budget, it is less obliged to a specific ministry or agency for proposing and promoting its financial needs. In cases, for example, where an executive branch ministry must submit the Commission's budget for legislative approval, there is an inherent dependency created with that "host" agency. Fiscal autonomy is afforded in the Model Law by allowing the Commission to present its budget requirements directly to the legislature.

2. Other Considerations

---

[19] Basic Principles on the Independence of the Judiciary, Adopted by the Seventh United Nations Congress on the Prevention of Crime and the Treatment of Offenders held at Milan from 26 August to 6 September 1985 and endorsed by General Assembly resolutions 40/32 of 29 November 1985 and 40/146 of 13 December 1985. See also, Principles relating to the Status and Functioning of National Institutions for Protection and Promotion of Human Rights (Paris Principles), endorsed by the Commission on Human Rights in March 1992 (resolution 1992/54) and by the General Assembly in its resolution A/RES/48/134 of 20 December 1993.

Beyond issues of independence, in implementing the enforcement mechanism, attention should be paid to the seniority and expertise of the Commissioner(s), the amount of time dedicated to serving the role, salary for Commissioner(s), and the staffing of the Commission offices. Increasingly, Access to Information Commissioners, or at a minimum the President of the Commission, is a dedicated full-time position.

In terms of salary, Commissioner(s) often play an adjudicating role. As such, their salary should be commensurate with a similarly placed Judge or Appellate body. In Mexico, the Commissioners hold the rank of Vice-Minister, with an equivalent pay scale. In juxtaposition, the Appeals Tribunal in Jamaica is a part-time, with a small stipend provided only when hearing cases. The effectiveness of the body suffers in comparison. Moreover, the post should be full-time to allow for the necessary dedication to the post, and to diminish potentials for conflicts of interest. As the Model Law states, the Commissioners should serve full-time and "shall not hold another job, position or commission, except in education, scientific or charitable institutions."

To ensure the proper functioning of the Commission, a staff or secretariat may be required. Experience has shown that for intermediary appeal bodies to be successful they must be endowed with appropriate resources, including full-time personnel that can become expert on the intricacies of applying the access to information law and support the Commission in their investigations, mediations, and hearings. Finally, a professional secretariat is helpful in assisting claimants, particularly when the rules for appeal are quite formalistic.

E. Inter-American System

Any person, group of persons or non-governmental organization may present a petition to the Inter-American Commission on Human Rights (IACHR)[20] alleging violations of the rights protected in the Inter-American Convention on Human Rights[21] and/or the American Declaration of the Rights and Duties of Man (American Declaration)[22], including the right of access to information contemplated in Article IV of the American Declaration and Article 13 of the American Convention.

The IACHR may only process individual cases where it is alleged that one of the Member States of the OAS is responsible for the human rights violation at issue. The Commission applies the Convention to process cases brought against those States which are parties to that instrument. For those States which are not parties, the Commission applies the American Declaration.

---

[20] The IACHR meets in ordinary and special sessions several times a year. It has seven members who act independently, without representing any particular country. Its functions include the promotion of human rights in the hemisphere and the processing of individual cases presented by individuals against Member States of the OAS alleging violations of the American Declaration and/or the American Convention.

[21] The Convention entered into force in 1978. As of the end of 2009, it had been ratified by 25 countries: Argentina, Barbados, Brazil, Bolivia, Chile, Colombia, Costa Rica, Dominica, Dominican Republic, Ecuador, El Salvador, Grenada, Guatemala, Haiti, Honduras, Jamaica, Mexico, Nicaragua, Panama, Paraguay, Peru, Suriname, Trinidad and Tobago, Uruguay and Venezuela.

[22] The American Declaration was the first international human rights instrument of a general nature that defines the human rights obligations that all Member States of the OAS assume by virtue of their membership in the organization. *See* I/A Court H.R., *Interpretation of the American Declaration of the Rights and Duties of Man within the Framework of Article 64 of the American Convention on Human Rights.* Advisory Opinion OC-10/89 of July 14,1989. Series A No. 10, paras. 43-45.

Petitions presented to the IACHR must show that the victim has exhausted all means of remedying the situation at the domestic level. If domestic remedies have not been exhausted, it must be shown that the victim tried to exhaust domestic remedies but failed because: 1) those remedies do not provide for adequate due process; 2) effective access to those remedies was denied, or; 3) there has been undue delay in the decision on those remedies. If domestic remedies were exhausted, the petition must be presented within six months after the final decision in the domestic proceedings.

When the IACHR receives a petition that meets, in principle, the requirements established in the American Convention, it proceeds to process the petition in accordance with the Convention and its own Rules of Procedure. Proceedings before the IACHR involve an admissibility phase and a merits phase, during which the IACHR receives information from the petitioner and the Member State in question. If after hearing the case the IACHR concludes that the Member State has violated one or more rights established in the American Declaration or the American Convention, it issues a report in which it sets out its factual and legal conclusions and makes recommendations to the State regarding the reparations owed to the victim.

At the conclusion of proceedings before the IACHR, if the State has accepted the jurisdiction of the Inter-American Court[23], the IACHR or the State may submit the case to the Court. The IACHR generally submits cases to the Inter-American Court when a State has failed to comply, in whole or in part, with the IACHR's recommendations. While the Inter-American Court's decisions are formally binding in nature,[24] States are also required to comply in good faith with decisions of the IACHR.[25]

F. Sanctions

In order to assure full functioning and compliance with the law, the best access to information legislation includes a comprehensive section on sanctions for failure to fulfill the procedural responsibilities or for affirmative actions to subvert the law. Sanctions, which often carry a fine or other administrative remedy such as suspension or termination, should apply when civil servants fail to comply with the provisions set forth in the law, such as time for response or obligation to assist requesters. Additionally, actions to impede the release of information – from obstruction and hiding information to destruction of documents – should also carry a sanction. Generally, administrative sanctions work better, as they are more likely to be applied.

Nevertheless, there should be provision for criminal sanctions when the action rises to the level of intentional obstructionism. When a civil servant has knowingly, i.e. in the face of an information request, willfully destroyed or altered requests, it is important that there be the potential for applying more severe penal sanctions.

---

[23] The Inter-American Court is a judicial body composed of seven judges who act independently, and it meets several times a year to hear and decide cases. The Inter-American Court may hear cases brought by individuals against States that have accepted its jurisdiction, but only after proceedings before the IACHR have concluded and the case is submitted to the Court.

[24] *See* American Convention on Human Rights, arts. 67-68.

[25] I/A Court H.R., *Case of Loayza-Tamayo v. Peru*. Merits. Judgment of September 17, 1997. Series C No. 33, paras. 79-81.

In determining the extent of the penalties – civil or penal – the local laws and regulations should be considered. In some cases, the criminal codes may need to be amended in order to allow for penal sanctions for the willful behavior.

Finally, the law should extend to provide sanctions for failure to follow a Commission order. Without clear sanctions, the civil servant's obligations under the law may be ignored.

G. Effectiveness

The overall effectiveness of an access to information regime – from passage, implementation and enforcement of the law to its ultimate use – will depend on a variety of factors. However, to begin to disaggregate the elements that translate into impact, systems for reporting, analysis and benchmarking must be developed.

As described above, a key role for an oversight body is to receive monthly or annual reports from the public agencies, to systematize the findings and develop recommendations. This, however, only is possible when benchmarks are instituted and sufficient reporting requirements are ensconced in legislation and then enforced.

Moreover, at a minimum, public bodies should be mandated to submit annual reports on the number of requests received, the number of requests fulfilled and denied, the reasons for denial, the time periods for responding, and any obstacles or challenges that the agencies are encountering in meeting the benchmarks. Once the reports are received and analyzed, the oversight body should be mandated to report to the legislature and the public the effectiveness and impact of the right of access to information. The annual reports should be available to the public, and citizens could be encouraged to engage with governments in evaluating the extent of implementation efforts and influence of the law. The Model Law calls on the public authority to submit comprehensive reports, and for the Commission to annually chronicle these submissions as well as inform on its own operations.

Clear targets and best practices guidelines should be established and relayed to implementers and citizens alike. These may serve to guide the civil service in their implementation efforts, as well as assure greater uniformity among the public bodies.

Finally, to further advance the openness regime, the Information Commission could be mandated to undertake periodic reviews of all or a sampling of requests, responses and appeals to identify any trends. If certain agencies are failing to meet their mandate, additional training or corrective actions could be applied. Moreover, if requests for certain information are routinely made, this could be added to the list for proactive disclosure.

KEY POINTS
MONITORING, ENFORCEMENT, AND EFFECTIVENESS OF THE LAW

- Although there are a number of different models for oversight and enforcement depending on the country's specific context and culture, the preferred system as presented in the Model Law is an Information Commission that has the dual responsibility of supervising the implementation and application of the law as well as the quasi-judicial power to hear appeals and issue orders.

- Oversight bodies should: -
    - Be statutorily mandated;
    - Have clearly defined responsibilities for monitoring implementation efforts; receiving reports; training of public servants; developing standard operating procedures; reviewing recordkeeping processes and automatic publication; and leading promotion campaigns; and
    - Be sufficiently staffed and resourced to fulfill their duties.

- Information Commissions should be: -
    - Comprised of one or an odd number of members, preferably five;
    - Selected with involvement from both Executive and Legislative branches, as well as with civil society engagement;
    - Vested with a term limit that extends beyond the Presidency, and is sufficiently long to allow for a specialization. Term limits for the initial Commissioners should be staggered so that they do not all leave at the same time;
    - Dismissed only for reasons of incapacity or behavior that renders them unfit, and should be afforded the right of appeal;
    - Afforded budget sovereignty as a means of insuring greater independence;
    - Full-time and paid a sufficiently high salary, such as an equivalent to a lower court judge; and
    - Sufficiently staffed and resources to fulfill their duties.

- Sanctions should be administrative/civil in nature, except for criminal penalties for willfully destroying or altering records that are the subject of a request for information.

- Benchmarks and indicators for implementation and application of the law should be developed, and made public in an annual report.

CHAPTER 4: ALLOCATION OF RESOURCES NECESSARY TO CREATE AND MAINTAIN AN EFFECTIVE ACCESS TO INFORMATION SYSTEM AND INFRASTRUCTURE

Adequate resourcing of an access to information program constitutes a key feature of its effectiveness and the attainment of the policy goals set out in the legislation. It is therefore crucial to establish a realistic budget and identify a source of funding in the planning phase of the legislative framework, prior to its proclamation. Without these two essential components, public authorities will not be able to deliver on their responsibilities efficiently and will have difficulty to manage increases in volume of requests.

Setting up an access to information program requires the same steps as budgeting for a new program. Based on the new functions, the public authority will have to recruit staff, find a place to house the new staff, set-up the infrastructure including information management, develop capacity in the access to information office as well as other parts of the public authority including a training program, establish service standards and publicize the new services being offered.

The need for adequate and permanent allocation of resources does not disappear after the initial program implementation. Sufficient resources must be allocated to ensure a sustainable level of services. A perennial program stemming from a legislative framework creates rights for applicants and obligations for public authorities. There is no choice for public authorities but to meet their legal obligations. Public authorities will inevitably face unpredictable variations in the volume of requests, which tend to put a significant amount of pressure on their ability to deliver on their responsibilities.

The ultimate risks of under-resourcing the program are a lack of credibility in the program and negative public perception of the transparency and openness of government. Lack of resources will also expose the public authority to complaints.

A. Factors for Consideration to Establish a Realistic Budget

As access to information is multifaceted, the following are considerations in establishing a realistic budget for the creation (start-up) and the implementation (operating budget) of the program:

1. *Scope of law*

   In forecasting the costs associated with the introduction of an access to information program, it is important to look at the scope of the law. The Model Inter-American Law on Access to Information suggests in Article 3, including all public bodies at all levels of the national governmental structure (central, regional and local) including all branches of the government (executive, judicial and legislative). In determining resource options, a jurisdiction may consider an incremental or phased-in approach whereby the access to information regime will be implemented in phases over a period of time.

2. *Access to information is demand-driven*

   Public authorities subject to the legislative framework do not control the volume of requests they receive. Given their legal obligations to respond to access request within a legislated framework, they cannot delay responses or diminish the quality of responses if

they do not have sufficient resources to process requests. In the initial resource allocation exercise, it can be difficult to precisely determine an adequate resources level based on a projected number of requests likely to be received in the first years of operations. It may be prudent to adjust budgets in the initial years of the program to ensure that the allocated resources are sufficient to meet the demand. If they are not, a gap will grow between the volume of demand and the capacity to deliver on access to information obligations. Backlogs of unanswered requests are likely to arise.

3. *Wages and compensation make up most of the cost of an access to information program*

Based on various studies, the primary cost component of an access to information budget consists of salary expenditures. In determining the number of employees required to implement and operationalize the program, it is important to include not only the staff that will be directly responsible for dealing with access requests, but also the staff in other areas of the public authority that are the record holders. The wages of access to information personnel and investigators will also vary in terms of expertise and experience and, consequently, in rates of pay. The wages portion of permanent budgets would be ideally adjusted to the cost-of-living index in each jurisdiction.

4. *Information management, record keeping and the use of technology*

Efficiently managed information is a fundamental requirement to having an efficient access to information program. Poor information management practices will result in an onerous and time consuming process where public bodies have to search for disorganized information and review large volume of pages. For more information on information management, see *Chapter 5: Adoption of Effective Information Management Policies and Systems to Properly Create, Maintain, and Provide Access to Public Information.* Prior to the adoption of an access to information law, an assessment of the current information management systems should be undertaken to ensure that they will be sufficient for the purpose of the access to information law. The adoption of effective information management policies and systems is a key component to support the access to information program and requires sufficient resources - both human and financial. Overtime, this will lead to cost savings.

5. *Measures to promote openness*

Part II of the Model Law suggests to public authorities to disseminate information about their function on a routine and proactive basis, in a manner such that the information is accessible and understandable. Proactive disclosure will mitigate the number of requests a public authority will receive over time, reducing the costs associated with the treatment of requests. These measures are a cost-efficient way to attain the policy goals set out in the legislation. Technologies are widely available to implement these measures.

6. *Capacity building*

The implementation of an access to information law will pose educational challenges from the standpoint of users and public officials. Sufficient resources should be allocated in the start-up budget and subsequent permanent budgets for capacity building and training. For more information on capacity building, see *Chapter 6: Capacity-Building for Information Providers and Users.*

B. Assessment of Resource Levels

All government-wide functions or activities created with the adoption of the access to information law, including the roles and responsibilities of all institutions: public authorities, central agencies (including oversight body and support services), enforcement and the judiciary, should be considered in the allocation of resources. This chapter focuses on the allocation of resources for core access to information functions only.

Credible cost projections are based on qualitative and quantitative information. Public officials from all levels of government that will have responsibilities – direct or indirect - with the administration of the program are the primary source of information. Comparative analysis of similar programs and functions in other jurisdictions is also very useful. The benchmarks for this analysis can be domestic or international. Assessments of numerical and statistical information such as workload trends, performance indicators and risks are also helpful. Documentation such as audits, financial projections and funding submissions for similar programs can also be useful to establish and substantiate averages and ranges.

Start-up and permanent budgets will vary depending on access to information functions (illustrated in Figure 1 below) as elaborated in the law, workload and operating costs. A startup budget encompasses all resource requirements needed for implementing the access to information program in the first year of operations. A permanent budget is composed of budgetary needs required to run the access to information program on a daily basis in subsequent years. The successful implementation of the access to information program requires a stable source of funds.

Figure 1
Mapping of functions associated with access to information

ATI Process	Publication scheme	Support Services	Capacity building	Internal Appeal	Information Commissioner	Judicial Review
Handling requests Search for records Review and approval Preparation (redaction) Release	Disclosure log Information Asset Register Preparation of information for publication Publication of classes of information	Legal advice IM/IT support Staffing actions	Training program for information providers and users	Appeal process Reasons	Compliance activities including investigations Awareness and training Policies and guidance Approval of publication schemes	Review process Reasons

Finding a source of funds

Offices responsible for handling requests for information can be found within each public authority or can be central to the government. Budget design will vary depending on the regime in place. Public authorities may be required to absorb the costs of administering the access to information program into their individual budgets. This means that existing resources must be reallocated to the access to information program from other programs, operations and corporate services of that public authority. This funding method may lead to uneven application of the legislation across the government. A central source of funding would come from the government's treasury and may be a more effective to support a government-wide program especially if the costs of the program are steadily increasing over the years.

For special projects, awareness activities and training events, additional sources of funds may be found in partnership with external stakeholders such as non-governmental organizations, international bodies and universities.

Forecasting the workload

(1) Workload

The primary function associated with an access to information program is responding to requests for information. As illustrated in Figure 1, this involves the handling of the requests, retrieval of records, the preparation of the records, review and approvals, and the release of the records, where appropriate.

As access to information is demand-driven, the starting point to estimate the appropriate level of resources is forecasting the number of requests likely to be received by the public authorities in the first years of operation.

The workload distribution among all the public authorities subject to the law will not be even across the board. Certain public authorities will receive a greater number of requests than others depending on the type of lines of business they are involved in, the issues they deal with, the interests of requesters, and so on. A more precise estimate of the costs associated with the access to information program could be done on an individual basis.

The following are some questions to help determine the workload:

- How many public authorities will be covered by the access to information law?
- What records are subject to the access to information law?
- What is the level of public, civil society and media engagement?
- What is the degree of literacy of the population?
- Is the public authority involved in a line of business of interest to a large segment of the population?
- Will there be measures to promote openness outside of the formal request process e.g. publication schemes, disclosure logs, information asset registers?

(2) Workload per employee

Once the volume of requests is estimated, the time required to treat an information request can provide a measure in determining how many full-time employees are required to process a request. This can vary significantly based on the type of requests received. The complexity of information requests has an impact on completion time. Complex requests may necessitate consultations with several other public authorities, requiring more experienced analysts and legal advisory services. A large part of the access to information process will be spent on the review of records to ensure that all exceptions are properly applied.

A recent study of the Mexican access to information program shows that, on average, 27.2 hours are devoted to responding to an information request and 25.1 hours to handle an appeal.[26] In the same study, the author provided the following formula for calculating the number of full-time public servants required in mandated public bodies: *Number of requests -multiplied by the average completion time - divided by the average annual hours of a full-time public servant – equals the number of full time public servants required*.[27] The same formula can be adapted to determine the number of investigators required at the Information Commission.

This formula, although simple to use, only takes into consideration the work done in processing information requests. As illustrated in Figure 1, time spent on training (access to information analyst and public servants generally), capacity building, the development of policies and guidelines, public awareness, and reporting also needs to be taken into account.

In addition, time spent by other areas of the public authority on searching, retrieving and reviewing records in response to access requests, the internal appeal process and by the support services cannot be undermined. All these functions are critical to the effectiveness of an access to information program and a sustained compliance with the legislative requirements. A single focus on processing information requests can lead to inconsistency in the application of the law, poor decisions, and lack of understanding by staff in other areas of the public authority about their access to information obligations. Lack of adequate resources therefore exposes public authorities to complaints to the Information Commission. Workload per employees will grow as a result of the time associated with resolving complaints.

(3) Costs associated with the workforce

The larger portion of the resource requirements associated with an access to information program is for personnel compensation and benefits. In administering the program, public authorities will have to hire staff at varying levels of experience and expertise. The types of employees typically found in access to information offices are: clerical staff, junior analysts, experienced analysts and managerial staff. At the Information Commission, the types are similar: clerical staff, investigators, lead investigators and managerial staff. They are also often supported by legal advisers.

New additional staff may not be required in all situations where the workload does not justify a full time employee. It may be possible to assign some functions and duties to employees already in place while at the same time keeping in mind training and caseload considerations.

---

[26] Budgeting Implications for ATI legislation *The Mexican Case*, Alfonso Hernandez-Valdez, World Bank Institute, Access to Information Working Paper Series, at page 18.
[27] *Id*.

(4) Other costs associated with the administration of the program

Additional expenditures should be considered when preparing a budget, items related to tools, equipment, training, accommodation, utilities, supplies, etc. Centralizing purchases may result in cost savings. These additional expenditures usually represent 25 to 40% of the overall budget. They tend to be higher in the first few years following the implementation of the law as some items are one-time expenses.

An inventory of existing and usable equipment such as computers, scanners and photocopiers across the various departments and authorities may help to maximize their use and limit the costs associated with the implementation of an access to information program. The cost of equipment can also be shared with other programs.

A checklist of expenditure items can be found in the checklist at the end of this chapter.

C. Assessing and Negotiating the ATI Budget of an Information Commission

As discussed in greater detail in *Chapter 3: Monitoring, Enforcement, and Effectiveness of the Law*, it is important to establish strong oversight and enforcement mechanisms to maintain and protect the right to information. The Model Law vests in the Information Commission all oversight and enforcement duties including vast investigative powers. As the role of the Information Commission is to scrutinize government's compliance with the law, these duties require an appropriate degree of independence and financial autonomy. There is a risk for political influence or interference if the Commission obtains its budget from the government.

The guidance offered in Section B above also applies, with some adjustments, to the Information Commission. In order to forecast the number of complaints, benchmarking with other similar programs will provide very useful information. However, there is a direct correlation between the number of complaints and the way the access to information program is administered upstream. A well functioning access to information process with trained public servants will tend to limit the number of external appeals.

The choice of the oversight and enforcement model will also bear costs. As indicated in Chapter 3, the Model Law advances an Information Commission model with 3 or more commissioners to limit as much as possible political pressures and interference. The costs associated with such a model may be too much for a jurisdiction to bear. However, as indicated in Chapter 3, other models such as judicial review may bear higher costs.

The choice of a funding model is crucial to ensuring that the Commission is adequately resourced and that financial needs are met on a permanent basis and not reduced arbitrarily. The following illustrates various funding models for an information commission and their advantages and disadvantages.

1. Funding From the Executive Branch of Government

One model for the funding of an Information Commission is through an executive branch ministry or agency, or the central ministry responsible for providing oversight of the financial management in government departments and agencies. In essence, this model requires the Information Commission to seek budgetary approval from the executive.

This model raises significant issues with regards to the independence and the financial autonomy of the Information Commission. It is dependant for funding on the very government it is mandated to investigate. As a result of this conflict of interest, the Executive Branch can significantly weaken the Commission's ability to investigate complaints and its credibility.

2. Funding From the Legislative Branch

Another model is to have the Information Commission report directly to the legislative body. Under that model, the commission would regularly submit to the legislative body its requests for funding (ongoing and additional funding). This model emphasizes the independence of the Commission from the executive branch and its financial autonomy.

3.Funding From the Executive Branch on Recommendation/Review by Legislative Branch/Congress

An alternative to the previous models could be the establishment of a mechanism whereby the Commission could get funding from the executive branch on review/recommendation of the legislative branch. This model has the advantage of reducing the perception of, and potential for budgetary obstruction.

Mexico, Jamaica and Canada follow this model. In Mexico, the budget of the Information Commission is set on an annual basis. The funds come from the executive on the approval of Congress. The starting point for the budget is the appropriations from the previous budget. In Jamaica, the executive branch sets the amount required subject to a review by the legislative branch. The budget is negotiated on an annual basis, based on the previous budget. In Canada, the base budget for the Commission is not negotiated on an annual basis. A special parliamentary committee provides an oversight function for independent parliamentary/congressional agents needing additional resources. The special parliamentary committee makes recommendations to the executive branch for approval of the funding.

4. Funding by Statute

Another model is funding by statutory authority. Any change to the budget would be submitted to the legislative branch. Although this model offers autonomy and independence, the challenge with this model is the potential lack of flexibility in adjusting the budget when there are increases in workload.

Checklist of Line Items for the Budget

Start-up budget – Mandated Public Authority	☑
Compensation and benefits (based on an estimate of workload) - Wages for personnel in access to information unit (access to information processing and other functions) - Wages for personnel in other areas of the public authority (related to searching and reviewing documents) - Wages for personnel providing corporate support (administration, finance, human resources, website administration); - Wages for personnel to support the internal appeal process; - Wages for personnel providing advisory and assistance services; - Benefits	
Operating costs - Costs associated with awareness and education function (Printing, publication and communication services) - Training - Website design and hosting: o Domain registration; o Hosting services; o Internet service provider.	
Accommodation - Rental - Furniture	
Equipment - Information technology (hardware and software): o Computers; o Server; o Case management system; o Digital storage capacity; o Redaction software; - Information management (hardware and software) - Scanners - Photocopier - Fax machine	
Utilities, materials and supplies - General (electricity, telephone, water, etc.)	

Permanent budget – Mandated Public Authority	☑
Compensation and benefits (based on verified workload) - Wages for personnel in access to information unit (access to information processing and other functions) - Wages for personnel in other areas of the public authority (related to searching and reviewing documents) - Wages for personnel providing corporate support (administration, finance, human resources, website administration); - Wages for personnel providing advisory and assistance services; - Wages for personnel to support the internal appeal process; - Benefits	
Operating costs - Costs associated with awareness and education function (Printing, publication and communication services) - Training - Website hosting: o Domain registration; o Hosting services; o Internet service provider.	
Accommodation - Rental payments	
Utilities, materials and supplies - General (electricity, telephone, water, etc.)	
Repairs and maintenance of equipment: - Information technology (hardware and software): o Computers; o Server; o Case management system; o Digital storage capacity; o Redaction software; - Information management (hardware and software) - Scanners - Photocopier - Fax	

Start-up budget – Information Commission	☑
Compensation and benefits (based on an estimate of workload) - Wages for investigators and managerial staff - Wages for commissioner(s) - Wages for personnel providing corporate support (administration, finance, human resources, website administration); - Wages for personnel providing advisory and assistance services; - Benefits	
Operating costs - Costs associated with awareness and education function (Printing, publication and communication services) - Training - Website design and hosting: o Domain registration; o Hosting services; o Internet service provider; - Travel and transportation	
Accommodation - Rental payments - Furniture	
Equipment - Information technology (hardware and software): o Computers; o Server; o Case management system; o Digital storage capacity; o Redaction software; - Information management (hardware and software) - Scanners - Photocopier - Fax machine	
Utilities, materials and supplies - General (electricity, telephone, water, etc.)	

Permanent budget – Information Commission	☑
Compensation and benefits (based on verified workload) - Wages for investigators and managerial staff - Wages for commissioner(s) - Wages for personnel providing corporate support (administration, finance, human resources, website administration); - Wages for personnel providing advisory and assistance services; - Benefits	
Operating costs - Costs associated with awareness and education function (Printing, publication and communication services) - Training - Website design and hosting: o Domain registration; o Hosting services; o Internet service provider; - Travel and transportation	
Accommodation - Rental payments	
Utilities, materials and supplies - General (electricity, telephone, water, etc.)	
Repairs and maintenance of equipment: - Information technology (hardware and software): o Computers; o Server; o Case management system; o Digital storage capacity; o Redaction software; - Information management (hardware and software) - Scanners - Photocopier - Fax	

KEY POINTS

ALLOCATION OF RESOURCES NECESSARY TO CREATE AND MAINTAIN AN EFFECTIVE ACCESS TO INFORMATION SYSTEM AND INFRASTRUCTURE

- It is important to establish a realistic start-up budget and permanent budgets, and identify the source of funds in the planning phase of the legislative framework, prior to its proclamation.

- Adequate and permanent resources must be allocated to ensure a sustainable level of services and protect the right to information.

- The effectiveness of the access to information program strongly relies on the resources allocated to implement the law and the set up of the appropriate infrastructure (staff, information management and capacity building).

- Forecasting the resource levels based on projected number of requests may require adjustments in the first years of operations.

- Efficiencies can be found in existing programs where staff and equipment can be shared or reallocated to the access to information program.

- Measures to promote openness will mitigate the costs associated with the treatment of requests over time.

- The duties of the Information Commission require an appropriate degree of independence and financial autonomy. The choice of a funding model is crucial to ensuring that the financial needs of the Commission are met on a permanent basis and not reduced arbitrarily.

CHAPTER 5: ADOPTION OF EFFECTIVE INFORMATION MANAGEMENT POLICIES AND SYSTEMS TO PROPERLY CREATE, MAINTAIN, AND PROVIDE ACCESS TO PUBLIC INFORMATION

Providing appropriate access to information begins with establishing an effective information management policy. A central tenet of this policy should be to protect designated information and make it accessible to the public. While the underlying components of an information management policy may be the same from public authority to public authority, what a particular policy will ultimately look like will depend on the public authority's function, business needs and legal requirements. The policy must be tailored to fit the needs and the objectives of the public authority and should be developed by balancing the competing interests of providing prompt and easy access to information with controlling the increasing amount of information being created within the public authority. Various technology solutions are available that may help address and automate these issues. However, no tool will be able to do all that is required to develop and implement an information management system. To successfully accomplish this task, public authorities will need to utilize internal human resources to define the goals, build the policy and develop consensus. Once this has been accomplished, technology solutions appropriate to the public authority's size and resources can be leveraged to implement and maintain the information management policies.

A. Information Management

Information is being created today at an unprecedented pace. More and more official communication is done via email, and documents are often created electronically and never printed. Much of the information being created may be stored in locations outside of the public authority's network (e.g. a personal file storage device or personal email account), increasing the risk of loss and the complexity in trying to recover this data.

Taking a new approach to the management of information can be time-consuming, costly and require modification of current processes and systems. However, the importance and benefits of establishing an information management foundation cannot be understated. Instituting organized and systematic information management practices ensures that important historical information will be preserved and readily available in the future. In addition, implementing a system by which information is managed and preserved will facilitate ease of access and retrieval, so that this information can ultimately be disseminated for the public good. Although the initial investment to create or further an information management process may seem burdensome, the long-term benefits far outweigh the initial challenges.

One of the foundational elements of an information management policy is the identification, management and retention of records. Generally speaking, a record is a piece of information that has some operational, fiscal, legal or historical value.[28] Certain categories of information may be deemed to be "records" of an organization pursuant to law, regulation or public policy. In contrast, non-record information may be beneficial to retain for a certain period of time, but will

---

[28] Electronic Discovery Reference Model, http://edrm.net/wiki/index.php/Records_Management_-_Record_Definition

likely not have the same specific retention requirements typically given to records based on their intrinsic value.

In order to support a public access to information law, an effective system for creating, managing and archiving information (including records) is imperative. Without such a system, it will be more difficult and time-consuming to locate and identify information and provide it within the timeframes mandated by law. In addition, lack of an effective system can create suspicion as to the transparency and legitimacy of public officials and their actions. "Any Freedom of Information legislation is only as good as the quality of the records to which it provides access. Such rights are of little use if reliable records are not created in the first place, if they cannot be found when needed or if arrangements for their eventual archiving or destruction are inadequate."[29]

Assess the Current Process

In order to implement an effective information management policy that allows for improved access to public information, public authorities must begin by reviewing their current information management and record keeping practices. Information exists in many different forms – paper documents, electronic documents, emails, notes, presentations, audio files, video files, etc. A "record" of the organization is a subset of information that has a distinct value to the organization. This value may be proscribed by law or regulation (e.g. the emails of a public official), or it may be due to the business nature of the communication. In most cases, the media on which the information appears is irrelevant, as it is the content of the information itself that determines whether something is a "record" of the organization. Retention policies will identify the types of information that must be retained, the appropriate length of time, and whether and when the information may be expired or destroyed. The importance of properly identifying and maintaining these records for the public interest is paramount in order to facilitate the purpose and intent of an access to information law.

It should be clearly understood that every public authority is different and each will have its own particular needs and limitations. Individual circumstances, budgets and risks will inform how a public authority assesses its information management strategy and the timeline by which it chooses to implement programs and processes to address its needs. What is reasonable for one public authority may not be reasonable for another, and individual factors must be taken into account when evaluating a process or technology. The suggestions provided in this chapter should not be considered exhaustive. Rather, the information contained herein is intended to help public authorities think through some of the issues to consider when evaluating an information management process designed to promote access to information.

Develop a Plan

In order to effectively establish an information management process, a public authority should first prioritize its needs and establish goals, and then determine what the greatest challenges are to reaching those goals. Often times the challenges identified will be budgetary, but they can also include issues such as developing consensus within a public authority or overcoming political roadblocks. Once these goals and challenges have been identified, the public authority can more efficiently begin to devise a plan to address them. One of the benefits of developing this plan is that it creates a level of accountability. If goals and challenges and the process by which they will be addressed are recorded, the public authority has a baseline from which to measure its progress.

---

[29] *Draft UK Code of Practice on the Management of Records*

A fundamental issue to consider as the plan is being developed is what types of information are most often requested and how this information is currently identified and produced. Beginning with an evaluation of how the system currently works can help inform the process and focus efforts on those parts of the process that need the most support. During this evaluation, care should be taken to think through ways in which information can be organized and archived so that the process of requesting the information is easier for the public and the identification and production of the information is most efficient. It is important to also consider historical information that may be difficult to access or retrieve because it exists on "outdated" media such as floppy disks. If this information needs to be retained and accessed, steps should be taken to evaluate methods to transfer this data into other, more readily accessible formats. As technological solutions are evaluated, these considerations should be continually examined in order to define the requirements of a system. It is imperative that public authorities think through the various issues that may arise in the information retrieval process so that these challenges can be addressed. A failure to do this will reduce overall efficiency and may ultimately result in multiple searches being conducted for the same request.

Once an evaluation of the information commonly requested has been done, the public authority may want to consider how and to what extent this information may be proactively disclosed. While proactive disclosure may seem to some to be an additional burden on an otherwise already time-consuming and complicated process, it will ultimately lower cost and reduce the amount of information requested. In addition, when information is proactively disclosed, citizens are likely to have more confidence in their government and the systems used to maintain and organize information.

As different sources of information are created on a day to day basis, whether by database, file share or email, public authorities should consider how that information may be successfully retrieved in the event it is requested. Often times, employees will create databases or other content sources based on their immediate business needs, overlooking the fact that this information may ultimately need to be accessed. Public authorities can overcome this challenge by reviewing the content of the information and the form in which it is usually created. Next, the public authority can determine the most efficient way this information may be accessed and provide guidance to its employees on how best to create content sources keeping access in mind.

In developing the information management plan, another important topic to consider is how the approach to information management can be standardized across agencies or departments. This is especially important when it comes to implementing technology, as technology provides the ability for disparate agencies or departments to share information across systems, increasing efficiencies and reducing redundant requests and productions. The more that various groups can agree to standardize on one process and system, the greater the benefit they are likely to see. In addition, the Information Commission and those individuals directly involved with the management of an organization's information should coordinate with the National Archives and other similar libraries to ensure conformity of practices in the treatment and preservation of historical information going forward.

While taking all of these issues into consideration at the outset may seem like a significant investment of time and cost, it is far more beneficial to make this investment at the beginning of the process than it is to amend or evolve the process later because issues or challenges were not addressed. For additional discussion on the issues to consider when creating the infrastructure to support an access to information law and the corresponding allocation of resources, see *Chapter*

4: Allocation of Resources Necessary to Create and Maintain an Effective Access to Information System and Infrastructure.

Consider a Data Map
Before a public authority can determine an appropriate information retention policy, it should understand what information is being created every day by its employees and the systems they use to do it. Having this high-level understanding of how information is created and where it is used will help inform decisions around how to organize and maintain this information. The product of this effort is often referred to as a "data map" as it maps the information within a public authority.

The data map typically includes the types of information that exist within a public authority, where this information is located, and who is responsible for maintaining it. The data map can be as detailed or as simple as the public authority desires, can be paper or electronic, and should be updated on a regular basis to reflect any changes. While there is technology available to help create a data map, it can also be created manually by developing a simple index or catalog of information types.

In developing a data map, it is often beneficial to designate one individual who can lead this initiative and coordinate among the many people that may be involved with identifying systems and information within the public authority. Undertaking the process to understand what exists on systems is not easy and may take some time to work through. However, if done correctly, this process will effectuate better decision making and will facilitate the eventual information retrieval process.

Determine Appropriate Retention Policies
Once record information has been identified, clear and established retention rules should be established detailing the various records that need to be preserved and how long these records should be retained. This analysis should include not only electronic information, but any paper records that may exist as well. The determination and application of retention rules will depend on the laws and regulations of the country and the local jurisdiction, and the business needs of the public authority. Various third party standards exist that are focused on the information management process. These standards and guidelines were established to help public authorities approach and organize their approach to information management.[30] For some, it may be beneficial to engage an expert to help develop this plan.

Generally speaking, when dealing with information management, the simplest approach is often the best as it promotes compliance. Fewer retention categories mean fewer decisions that must be made about particular information or a particular record. In addition, grouping categories of information together helps facilitate its retrieval when a request for access is made.

Destruction of Information
An equally important part of the information management lifecycle is the destruction of information that does not need to be kept for legal, regulatory or other business purposes. Without a methodical approach to expiring information, systems can become clogged with data

---

[30] For example, the International Organization for Standardization created ISO 15489, dedicated to helping organizations establish a framework to enable an information management process. *See* http://www.iso.org/iso/pressrelease?refid=Ref814; *see also*, The International Council on Archives at http://www.ica.org.

that no longer has any value to the public authority. This overload makes searching for particular or relevant information difficult and it can delay efforts to respond to a request within required timeframes. As the creation of electronic information continues to accelerate, the lack of routine expiration can overwhelm an information management process and stymie public access to information.

Once determined, retention policies should be memorialized and published, and a schedule should be created for reviewing and updating the policies on a regular basis. If changes are made to the policy or if there are deviations from the policy in practice, this should be recorded with notes explaining why such actions were taken. Where destruction of information is scheduled pursuant to retention policies, it should be routine, and to the extent possible, automated. Automating this process helps promote transparency and fosters confidence in the predictability and reliability of the information management process.

Training

Officials and employees should be trained on the retention process to understand its purpose and its functionality. When users are educated as to why a process is being implemented and the end goal, they may be more inclined to alter the way they create information to align with the intent of the policy. There are various training methods and approaches that can be employed depending on the audience. For some employees who may be responsible for managing records, training will need to be detailed. For others, the training may be conducted at a higher level. In all events, officials and employees should understand the intent of the access to information law so they can help promote its principles through information management. As discussed above, establishing and implementing a policy across an organization will help ensure consistency and compliance with the applicable law.

Suspension of Routine Destruction

In some countries, it may be necessary to suspend normal information expiration or destruction practices in response to pending litigation or some other legal request for information. In the United States, this process is often referred to as a "legal hold." For instances where this is required, steps should be taken to document the request and what information was placed on "legal hold" or otherwise withheld from the normal expiration process. In these cases, the distinction between "information" and "records" is often irrelevant, as a legal request will require the production of all information that may be available, not just records of the organization.

Easing the Implementation of Retention Policies

If this is the first time a public authority has undertaken to implement a retention policy, it should consider creating a timeline detailing by when the implementation will be completed. In many cases, this will need to occur in phases.

There are various technological solutions available that can help automate the classification and enforce the retention of information. Tools like email and file archiving can place information into a centralized repository where more granular retention policies can be applied. For example, retention periods for email can be automatically applied based on the person sending or receiving the email, or the department to which he/she belongs. Using an archive, information can automatically be run through its lifecycle such that it will be expired when it is no longer useful or necessary. In addition, an archiving tool can suspend these destruction practices in the event that information needs to be preserved pursuant to a legal or other request for information. As mentioned above, there are a variety of tools that can help make this process more efficient.

Although the process of assessing a public authority's information management strategy may be time-consuming at the outset, the benefits derived from this undertaking will far exceed the initial investment. Enabling this process not only helps control the amount of information on existing systems, it will also facilitate the identification of and access to information by making the process more efficient. Failing to implement such a process can undermine the public authority's ability to respond to requests for information, may decrease constituent confidence in the system, and may ultimately hinder public access to information.

B. Data Sources

When requests for information are made, they are usually done so without regard to the medium in which the information exists. For example, a citizen may request copies of meeting notes that were typed and exist only in hard copy. Or, these meeting notes may be recorded and stored electronically on a file server. To the requestor, it may make no difference – they simply want and need access to the information.

Hard Copy Information
Despite the rapid rise in the creation of electronic information, the existence and importance of hard copy information cannot be minimized. In public authorities in particular, historic information in hard copy form may be maintained indefinitely for historic purposes. In the request and production process, hard copy documents have their own unique challenges stemming from their inability to be electronically searched. An important first step in addressing hard copy documents within the public authority is understanding what documents exist and then creating an index or filing system to categorize them. This index should be as detailed as necessary to reduce the amount of time required to locate information relevant to a request for information. An index can be created electronically, allowing it to be searched using keywords. This can help substantially with organizing and locating relevant hard copy information.

As public authorities migrate to more digital platforms, hard copy documents will likely be created with less frequency and may become more difficult to identify and produce. Also, hard copy documents lack the inherent advantage of having a back up copy stored elsewhere in the case of a natural disaster or malfeasance. However, even though the new creation of hard copy documents may subside, demand for information currently in hard copy form will continue.

When considering the development of an information management process and the implementation of information management technology, public authorities should consider the benefits of converting hard copy documents into an electronic system for search and review. There are multiple ways to approach this process and differing degrees of specificity. For example, documents can be scanned and given an identifying title representing the content of the document. This approach is typically applied to documents containing images and few words (e.g. maps, photographs, etc.). These documents can then be searched based on their title. Many documents can also be scanned into electronic form with the help of optical character recognition or "OCR." OCR is the electronic translation of handwritten, typewritten or printed text into computer-editable and searchable text.[31] While highly valuable, this process can be time-consuming and expensive. As such, if pursuing this approach a public authority may want to determine the hard copy information that is most often requested and target that information first.

---

[31] Electronic Discovery Reference Model, http://edrm.net/wiki/index.php/OCR

Electronic Information
Information that is created and stored electronically is growing at a rapid rate. Electronic information includes just about anything that was once created only in hard copy, including reports, memos, meeting notes, and even certain types of drawings. In addition, emails, instant messages and other electronic forms of communication are all created and stored electronically.

While electronic information may be somewhat hard to control due to how quickly it can be created and distributed, because of its electronic nature, it is also more easily searchable than hard copy information. When dealing specifically with electronically stored information, capturing and categorizing the "metadata" associated with the file can provide significant benefit for the search and retrieval process. Metadata includes the basic characteristics of a particular document. Metadata may, for example, include the date the document was stored, and the identity of the user who stored it. If preserved and captured, the metadata can be queried to identify relevant information.

While much of the information created today is electronic, most public authorities will have a mix of both hard copy and electronic information and will need to develop a strategy and a process that encompasses and addresses both.

C. Information Production

When dealing with a request to produce information, whether it be in the context of a public access request or in response to litigation, an organization will need to be able to do the following: 1) identify potentially relevant information; 2) collect that information; 3) produce the information in a format that is usable by the requestor; and 4) maintain a record of the information produced and when a response was provided.

Identifying Relevant Information/Collection of Information
In order to identify relevant information, a public authority will need to implement a system by which records may be searched and ultimately retrieved. The approach to this will differ depending on whether the information is kept electronically (e.g. email, electronic files, etc.) or whether it is retained in hard copy.

When dealing with information kept in hard copy documents, public authorities typically create some sort of index depicting what categories or types of files exist and where they are located. This can be done by filing structure, author, department, etc. What is most important is that the public authority understands what documents exist and implements a practical way to locate them.

The approach with electronic information is the same. Although the amount of electronic information can be exponentially greater than what exists in hard copy, the electronic nature of this information makes it easier to categorize and identify. Indexing tools can quickly "read" information and make it accessible to electronic search methods. When evaluating how to proceed, the public authority will want to evaluate what information within a particular piece of data will need to be searched. For example, for emails, will the public authority need to search the author and recipient fields, the content of the email, or the content of any attachments to the email? There are various ways to approach this and differing degrees of complexity involved. To assess this, it may be helpful for the public authority to review the types of requests for information it typically receives. The level of detail within these requests will help inform the level of granularity to which the search capability will need to be developed. When determining

these parameters, the public authority should keep in mind that the information will need to be produced in a timely manner, often with very little lead time. To that end, search functionality should be enabled to accommodate identification and production within a short timeframe.

Production Format
In addition to the search methodology and timing issues, it is important to consider the ultimate output of the search and how this information will be used. There may be specifications within the law regarding the format in which information should be produced. If such specifications exist, the public authority should ensure that the system it uses to search and produce information is able to conform to these requirements. In many cases, a requester may not have access to a particular system in which information was created within the public authority, for example, a particular database. If that is the case, the public authority will need to take steps to produce the information in a format that is readable by the requestor, unless there is some circumstance which makes this unreasonable or impractical.

Maintain a Record of Requests
Transparency is a fundamental principle of an approach to open government and access to information. Developing a system to proactively document and track requests for information and the process and results of these requests will help instill confidence and openness between the public authority and the public. Public authorities may also consider publishing the requests and results or otherwise making them available to the public. In some cases, an exception or a requirement in the law may prohibit the production of certain information. Where this occurs, it should be documented and explained. Likewise, if requested information is not produced for any other reason, the public authority should document and explain the reason.

D. Proactive Disclosure

An access to information law may contain provisions requiring public authorities to proactively disclose certain information and documents. These requirements are generally intended to foster transparency and confidence in government and provide useful information to the public. An added benefit of these policies is that they may reduce the number of requests a public authority must process, as the information sought may already be available. This may translate into cost savings for the public authority as employees are relieved from searching for, reviewing and producing information.

A threshold issue to consider is what information should routinely be disclosed. If the law requires specific information to be proactively disclosed, policies should be memorialized to address the scope of the information to be disclosed and the schedule for doing so. In addition, proactive disclosure policies should define the person or department responsible for maintaining and updating the information. The policies should also specify where the information will be disclosed (i.e. a public website), and how (in html format, Pdf, etc.). The public authority may want to publish the policies in this location as well, as this will further aid the efforts at transparent information sharing. When information is proactively disclosed, the public authority should make every effort to organize it in such a way as to facilitate public access. Automated technology may help this process, as information can be identified for proactive disclosure based on its metadata (e.g. author, recipient, subject, etc.). In order to successfully leverage these technologies, a public authority will need to identify the metadata fields most closely associated with the requests for information the organization typically receives.

E. Technology

The effectiveness of an access to information process rests on the ability of governments to clearly organize and manage records, both paper and electronic. As described above, a public authority must have a clear understanding of the information that is being generated, the existing requirements for retention, and the parameters for organization and maintenance of the data. The preceding section clearly outlined the steps for developing a plan. Once a plan or information management strategy has been defined, there are numerous technological solutions that can facilitate the implementation of the plan and drive down the cost of managing the information to make it accessible to the public.

While the demands of an information management process can seem daunting, there are a number of technological solutions available that can address the various issues that may impede an information management program. IT experts within a public authority are frequently required to spend significant amounts of time responding to search requests, which can include restoration of backup tapes that may be stored off site, search of individual mailboxes, and other repetitive, time-consuming requirements that take them away from their daily responsibilities. Using available tools, a public authority can make the information management process more efficient and less costly, and free up human resources to work on other important projects. Most public authorities are used to handling paper documents and may be more comfortable developing information management strategies based on this experience. Paper documents should be included in the overall information management strategy, but due to its escalating volume, electronic information requires a different approach. In many cases, it is easier to manage electronic information as its very nature makes it more accessible to index, categorize and search.

Just as the development of a retention strategy should reasonably conform to the purpose of the public authority and its users, so too should the acquisition and implementation of technology enhance the functionality of the public authority. There are technical solutions available to suit almost every level of sophistication and competence. When evaluating these solutions, a public authority should identify what issues it needs to address with a tool and prioritize those issues. For example, if maintaining records is the issue, a public authority may want to focus on an archiving tool that provides the ability to retain information based on its classification. Any selected solution should be scaleable so it can meet the needs of the organization today and grow with it as needs evolve. Technology should make the process easier, not more difficult.

Archiving technology

Archiving technology provides a central repository for electronic information that allows for categorization, searching, preservation and disposition. Many different types of information, including email, files, etc. can be ingested into the archive and secured from inadvertent or purposeful destruction. Archiving technology provides immediate access to information and allows that information to be preserved in conformance with the public authority's policies and legal requirements.

Ideally, the public authority should select an archiving technology that will preserve the documents in an open document format that will be readable and accessible in the future. When adopting technological solutions to address the storage and retention of information, public authorities should consider the requirements of an access to information regime and may want to refer to existing industry standards for guidance (e.g. the International Organization for Standardization).

Some archiving technologies provide the ability to apply a retention policy to designated documents. For example, a public authority may designate that all emails created or received by a certain group (e.g. accounting) be retained for 10 years. Once this has been determined, the archive will automatically retain that information for the specified time period. The benefit of this type of system is that it relieves individual users from having to determine how long something should be kept. It also enables the automatic expiration of information that has reached the end of its normal life cycle (i.e. at the end of 10 years the information is automatically deleted unless otherwise preserved).

When specific information is requested, an archive may be searched using an electronic index of the information contained within it. The use of search technology can have a significant impact on efficiencies and response time, often reducing this time exponentially. Utilizing even basic search criteria can help refine the information that is potentially relevant to a request. For example, an archive can be searched using keywords, or using relevant metadata such as the author or recipient of an email or file. Once relevant information has been identified, it can be reviewed and extracted from the archive in response to a specific request. These individual search results can also be reviewed and marked with comments or other "tags" identifying and classifying the information prior to production. This information can be reviewed internally to help public authorities group certain types of documents, or to raise issues within the public authority around the sensitivity or confidentiality of the information prior to disclosure.

Archiving technology can also provide the capability to de-duplicate exact information and store it only once. This relieves the need for additional storage space and the associated costs. In addition, duplicate information can be removed from a search set. When responding to a request for information, this reduces the amount of information that must ultimately be reviewed in response and reduces the cost associated with processing and producing that information.

Using an archive to store the most frequently requested content can create a much more efficient and cost effective system. In addition, retention periods can be applied to information such that it is automatically expired once it has exceeded it has reached the end of its lifecycle, whatever that period is deemed to be. In essence, the archive becomes the go-to source for active information based on its ease of retrieval and search functionality.

Back up technology

Disaster recovery plans that enable back up technology allow a public authority to recreate its electronic information systems and continue to operate in the event of an unforeseen system failure. The timeframe that data should be stored for these purposes will vary depending on the public authority and the information at issue, but as a general rule, the information should be stored for as short a time period as possible. Back up technology was not designed to function as an archiving or records management system, as it can be cumbersome to categorize and ultimately retrieve information. In the event back-up technology is called upon to retrieve information or to manage preservation of content for legal hold, public authorities would be advised to use a content indexing capability. This can provide some level of targeted search and retrieval and reduce the cost and complexity associated with the back-up environment.

As with archiving technology, certain backup technology also has de-duplication capability allowing the same information to be stored only once. This has the potential to reduce storage costs and ease the search process.

Enterprise Content Management technology

Enterprise Content Management ("ECM") technology has been broadly defined as "the strategies, methods and tools used to capture, manage, store, preserve, and deliver content and documents related to organizational processes."[32] ECM technology is an all-encompassing term that includes, among many other solutions, records management software and document tracking and control systems. These technologies generally enable users and records managers, where possible, to classify records based on their content. Once classified, these records can then be organized and stored in a manner that makes sense to the public authority. Additionally, the records can then be integrated into an archiving system such that they are retained for the appropriately designated period of time.

Active Content Collection technology

As electronic information can be located anywhere within a public authority's environment, in some instances it may be necessary to collect and review information that exists outside of the typical content sources created and used by the public authority. For example, in certain instances it may be necessary to identify the files that exist on a particular employee's laptop. This information is likely outside of the public authority's visibility and may not be regularly accessed by anyone other than the individual employee.

If this functionality is required, separate tools and technology exist that can collect information outside of network systems and index that information so that it is searchable. The particular functionality of the tool will depend on the information being sought, the degree of specificity that is required in the collection process and the source of the information, for example, network servers, storage systems, application repositories, and personal computers.

Additional technology

There are additional categories of technology, including records management, security and data loss prevention technologies, that may also be beneficial to public authorities. Where appropriate, these technologies should also be considered as the public authority develops its information management strategy.

Security

Like many other large enterprises and organizations, governments are frequently responsible for certain private citizen information that requires greater levels of security and protection. Depending on the type of information being stored, there are various compliance requirements that may apply concerning the security of the information. The privacy and security requirements of personal information are generally defined in legislation. For example, there may be legislation regarding health and access to care. There may be provisions within that legislation that specify the security requirements for individual patients' health records. The same is true of financial records or tax receipts. There are many cases where governments or non-state actors working in a governmental capacity may be managing confidential information that should not be disclosed. Because of this, public authorities are encouraged to adopt and implement robust security controls to manage access, while maintaining the spirit and letter of the access to information law.

As a security precaution, public authorities should consider encrypting, or otherwise rendering unreadable without authorization, information that is not proactively disclosed. Encryption

---

[32] Association of Information and Image Management, http://www.aiim.org/what-is-ecm-enterprise-content-management.aspx

ensures that the public authority is able to secure the information held in its systems, and if the information is disclosed improperly, through carelessness or malfeasance, the encryption will render the information unreadable.

Making the Case for Technology: Cost Savings

For some governments, it may be difficult to garner the support necessary to purchase technology aimed at addressing information management concerns. However, in many cases, an investment in software can often pay for itself in a short timeframe. To garner support, a public authority may be able to identify cost savings derived from a technological solution by tracking 1) storage requirements, and 2) the time and cost associated with responding to requests for information.

Automating an information management system by using archiving and backup technology can help reduce storage burdens by moving information off higher-cost equipment to lower-cost storage. This can translate into significant cost-savings when projected year over year. To track potential savings, a public authority may want to estimate how much additional storage space is typically required every year to keep pace with the growth of its information. Comparing this with the storage savings a public authority can expect to receive from a specific technology can help quantify actual storage savings. This can help offset the cost of such a tool.

It can also be useful to look at the costs associated with searching for information in response to a request. This includes the cost associated with the time required to conduct the search and prepare a response. If a public authority is able to implement an automated system, this cost can be lowered as the search can be done electronically in a short timeframe, relieving the burden on the individual. In one example, a United States government entity was faced with a request for information concerning a public health issue. By using an archiving system, the entity was able to locate the information responsive to the request in under an hour. The entity reported that locating this information without such a system would have taken approximately seven days. The entity further estimated that it would save over $100,000USD per year in employee time by reducing the search time required to locate information in response to records requests.

If resources are limited, information management processes can be implemented using a phased approach. In these situations, public authorities can assess their biggest challenge in terms of time and cost and focus on the technology available to address that need. While technology can certainly improve efficiencies and help make the information management process easier, a lack of resources or support should not hinder progress on assessing the current environment and defining a process to manage information. Technology can come later, once the foundational elements of an information management process have been defined. For more discussion on how cost savings may affect capacity building and the determination of budget, see *Chapter 4: Allocation of Resources Necessary to Create and Maintain an Effective Access to Information System and Infrastructure.*

Implementing Technology Solutions

Implementing technology can be a time-consuming process. If installing a new system, a public authority may want to establish a timeline by which certain milestones will be reached and identify the parties who will be involved. If the timeline is made public, it will help keep the implementation team on schedule and will also encourage open communication with the public.

The roll-out of the technology and its use should be monitored so that successes and set-backs can be chronicled and shared with other agencies, providing them helpful guidance on what works and what may best be re-thought. The more communication that flows from this process, the more the spirit of the access to information law is achieved.

F. Achieving Conformity

Various public authorities may have different information management methods and processes yet still be subject to the same access to information requirements. In these instances, it may help to facilitate inter-agency communication around methods and process so there is consistency between the public authorities. Best practices documents may be drafted and internal websites may be used to disseminate this information, and it may be helpful to conduct regular meetings or audit sessions between public authorities to share information.

In addition, to the extent possible, systems across various public authorities should be able to connect with each other and transfer information. This will help streamline and standardize retention practices and reduce duplication of efforts in responding to information requests.

Checklist

Information Management – Getting Started	☑
Assess the Current Process - Where does information exist and in what format? - What are the current record-keeping practices? - How is information archived? - Is information destroyed? If so, when and how?	
Develop a Plan - Identify needs and establish goals. - Identify challenges and roadblocks. - Identify what types of information are most often requested. How is this information currently identified and produced? - Does information exist in hard-to-access formats? - What information can be proactively disclosed? - How are employees creating new information? Where is it stored? - How can information management approach be standardized and coordinated across agencies and departments?	
Consider a Data Map - What historical information exists and where is it located? - What new information is being created on a daily basis? - Designate one individual or team to lead this process.	
Determine Appropriate Retention Policies - Include hardcopy and electronic documents. - Review legal, regulatory and business requirements for retention. - Consult third party standards or experts.	
Destruction of Information - Establish policies to address information that does not need to be retained pursuant to a legal, regulatory or business purpose. - Publish these policies and create schedule for review and updates.	

- Automate this activity to the extent possible. - Develop process to suspend destruction practices when required. - Training on process.	
Information Production	☑
Issues to Consider - Identify relevant information - Collect relevant information - Produce the information - Maintain a record of information requested and produced	

Proactive Disclosure
- Identify/Collect relevant information
  o Hardcopy and electronic
  o What information needs to be searched?
- Produce the information
  o Production format
- Maintain a record of information requested and produced
  o Consider publishing requests received
  o Automate the tracking of requests
  o Document exceptions	

Technology	☑
Different solutions available depending on needs - Archiving Technology - Back up Technology - Enterprise Content Management Technology - Active Content Collection Technology - Security Technology - Various Other Technologies	

Cost Savings Derived from Technology
- Identify potential benefits from implementing technology
  o Storage savings
  o Time and cost associated with responding to requests	

Implementing Technology Solutions - Consider a phased approach - Develop and publish a timeline of implementation - Document milestones and setbacks - Coordinate with other agencies and departments – share information	

KEY POINTS

ADOPTION OF EFFECTIVE INFORMATION MANAGEMENT POLICIES AND SYSTEMS TO PROPERLY CREATE, MAINTAIN, AND PROVIDE ACCESS TO PUBLIC INFORMATION

- Public authorities should begin by establishing an information management policy so that information may be preserved and easily accessible in the future. In order to establish an information management policy, it may be necessary to: -
    - assess the current process;
    - develop a plan;
    - develop a data map;
    - determine appropriate retention policies;
    - determine appropriate destruction policies; and
    - train staff on the procedures.

- In developing policies and systems to properly create, maintain, and provide access to public information, it is important to consider all of the data sources, including, but not limited to hard copy information and electronic information.

- When dealing with a request to produce information, whether it be in the context of a public access request or in response to litigation, a public authority will need to be able to do the following: 1) identify potentially relevant information; 2) collect that information; 3) produce the information in a format that is usable by the requestor; and 4) maintain a record of the information produced and when a response was provided.

- Proactive disclosure can serve as an added benefit to public authorities as it may reduce costs and the number of requests that need to be processed and thus the time spent by employees in searching for the information.

- Once a plan or information management strategy has been defined, there are numerous technological solutions that can facilitate the implementation of the plan and drive down the cost of managing the information to make it accessible to the public.

- In many cases, an investment in technology can often pay for itself in a short timeframe. To garner support, a public authority may be able to identify cost savings derived from a technological solution by tracking 1) storage requirements and corresponding costs, and 2) the time and cost associated with responding to requests for information.

CHAPTER 6: CAPACITY-BUILDING FOR INFORMATION PROVIDERS AND USERS

The formulation of legal frameworks and the design of an institutional operating structure, while an essential part of the process for launching a public information access system, must be accompanied by the development of training initiatives that will ensure that the system can function. Those initiatives include the design and implementation of strategies and programs for education and information about the basic elements of the existing information access system and about the skills that information providers and users must acquire; also necessary are initiatives to raise awareness about its importance among leaders, public officials, and the general public. This chapter will offer a series of elements to be taken into account in developing such training strategies, based in particular on the framework provided by the Model Law that accompanies this Guide.

The importance of capacity-building initiatives has been taken on board in the national and international standards that govern access to public information. According to the judgment of the Inter-American Court of Human Rights in the *case of Claude Reyes et al. v. Chile*, "the State should provide training to public entities, authorities and agents responsible for responding to requests for access to State-held information on the laws and regulations governing this right; this should incorporate the parameters established in the Convention concerning restrictions to access to this information that must be respected."[33] In general terms, most of the region's laws on public information access contain provisions that provide for training, intended for both information users and providers.

The Model Inter-American Law on Access to Information provides that the Information Commission should assist public authorities in providing training to officials on the application of the law, while it is the duty of the Information Officer within the specific public authority to ensure the provision of the training on the application of the law. Similarly, the Model Law calls for the provision of core education modules on the right to information in schools so as to ensure that the public is informed of their rights under the law. Therefore, under the Model Law, it is the duty of the government to support, organize, and ensure proper training programs for public officials as well as to raise awareness of the right to information and the procedures for filing a request in the general public.

It should be understood that the implementation of information access laws in the region frequently encounters a dual obstacle: a deep-rooted culture of secrecy in the public sector, and the weaknesses of citizen participation in actively pursuing information. This right must therefore be promoted through training efforts and awareness-raising strategies that address its importance for both strengthening democratic institutions and for constructing a vigorous and politically active citizenry. A capacity-building strategy for access to information must include, among its basic components, initiatives and instruments that pursue objectives that are in line with this: on the one hand, developing knowledge and skills, and, on the other, working for a cultural transformation toward transparency and accountability. The combination of these elements will have a much greater and further reaching effect than applying the two of them in isolation.

When beginning implementation of a new access to information regime, capacity building should focus on setting the foundations for an effective system of access and training public officials on

---

[33] Inter-American Court of Human Rights, *Case of Claude Reyes et al. v. Chile*, Judgment of September 19, 2006, Series C No. 151, para. 165.

the rights and duties under the new law as well as on new polices and procedures that will be enacted to ensure compliance with the law. Once the initial training has been conducted and the law is in force, the Information Commission and the public authorities should shift their focus to continuing education and refresher trainings to ensure that public officials remain up to speed on the law and the policies and procedures to ensure compliance. In addition, they should work to ensure that new public officials receive training when they begin work for the public authority. Likewise, when new policies and procedures are adopted or existing policies are changed, training should be provided to those public officials whose duties, roles and responsibilities may have changed or been effected by the changes. Training information providers is only one half of the coin – in order to have a functioning access to information regime, the government must also train the information users who will be the ones filing requests for information. Activities should be organized to raise awareness in the general public so that the information users know of their rights and the procedures for requesting information and for filing appeals.

In designing and implementing training programs, public authorities should look both to the use of formal teaching methods designed to transmit information and basic concepts, but also to informal methods such as those that seek to stimulate comprehension, application of values and ethical decision making. A variety of teaching methods and materials should be utilized – for example, for some public authorities, online training modules may provide a cost saving alternative to workshops, whereas for others, an in person workshop may be more effective.

In general terms, a training program for information providers should include why access to information is important, the laws and their scope, procedures for filing and responding to requests for information, and procedures and policies for archive maintenance and access.[34] Training for information users should focus on why access to information is important, the rights guaranteed under the law, and procedures for how to file a request for information and an appeal.

While it is the duty of the government to provide training to information users and providers, experiences show that government-civil society collaborations on the development of and implementation of capacity building programs on access to information are effective.[35]

The social universe and the nongovernmental organizations, academic institutes, social organizations, etc. that it comprises are strategic allies that can assist the State in discharging the duty of training information users and suppliers. Consequently, synergies between the two sectors should be created, in order to ensure the success of implementation processes.

A. Phase 1: Initial Capacity Building

During the initial phase of training taking place after the law has been enacted and the foundation is being set for its effective implementation, it is essential for the public authority, with the support of the Information Commission, to identify what is required of different actors under the law and the policies and procedures set by the public authority to comply with the law.[36] As the

---

[34] United Nations Development Program (UNDP), Bureau for Development Policy, Democratic Governance Group. Right to Information. Practical Guidance Note, July 2004, at 29.
[35] http://www.humanrightsinitiative.org/programs/ai/rti/india/officials_guide/training_pub_officials.htm
[36] *See* Department of Constitutional Affairs in the UK, *Managing Information and Training: A Guide for Public Authorities in Implementing the Freedom of Information Act and the Environmental Information Regulations*, 7.

duties of an Information Officer under the law will vary from the duties of other public officials, the public authority and the Information Commission should work to design separate trainings on the application of the law, policies, and procedures, adapted to the roles and responsibilities of the actors. Regardless of position, trainings for all actors during this initial phase should be directed at informing all public officials of the importance of the law and of how it serves the public to strengthen democratic values including transparency and accountability.

Capacity Building on Democratic Values

When first confronted with a change in policies and procedures to implement the new law, it is important to ensure that all of the actors understand the importance of the law and how it will serve to strengthen democratic values. The widespread and effective use of practices that facilitate and encourage access to information must be accompanied by a deeper change: both in the organizational culture of public institutions and in public awareness. That change can only arise from specific actions that lead to the broad recognition of the opportunities, rights, and responsibilities that a democratic system offers. For that reason, the transformation of the culture of secrecy must be accompanied by the basic tools needed to raise awareness about, educate in, and instill the sense of access to information as a fundamental right that affords us access to economic, social, and cultural rights, as well as to civil and political rights, for the full exercise of democratic citizenship.

These tools also include the development and promotion of basic democratic values such as transparency, accountability, responsibility, ethics, and integrity in the management of public resources. However, democratic values "are not innate human values. They are learned and must be taught as explicitly and clearly as democratic knowledge and skills are taught." Education for democracy means preparing individuals for believing, thinking, and behaving as democratic citizens, by means of an "explicit and purposeful process of teaching and promoting the development of democratic knowledge, skills, values and attitudes."[37]

Encouraging values such as transparency, responsibility, and accountability among providers of state information is an effective way to bring about transformations in the organizational culture of public institutions in order to combat the culture of secrecy, prevent corruption, and raise levels of efficiency and integrity.

One potentially useful initial stage in the design of that strategy is to carry out a diagnostic study: for example, conducting a survey to generate information on public employees' values and perceptions on matters of ethics, transparency, and access to public information, and to reveal their views on shortcomings and problem areas requiring particular attention in pursuit of greater transparency and integrity.

Evaluation and monitoring also play an essential role in obtaining information on the results and impact of information access strategies, including training and outreach campaigns. These are also important mechanisms for setting goals and creating incentives.

Capacity Building on the Implementation of the Law

---

[37] Villegas Fernado-Reimers, Eleonora: "Education for Democracy," *ReVista*, Harvard Review of Latin America, Fall 2002, http://www.drclas.harvard.edu/revista/articles/view/173 (consulted: November 11, 2009).

Training on the application of the law should begin following the appointment of the Information Commissioners.[38] When the Access to Information Law has first been enacted, it is recommended that the newly appointed Commissioners seek the assistance of and draw upon the experiences of Commissioners in other countries on the effective functioning of an access to information law as well as lessons learned in training of public officials and public awareness campaigns.

Once the Information Commissioners have taken office and each public authority has appointed at least one Information Officer[39], the initial priorities of the Information Commission should be on training Information Officers who are on the front lines of both responding to and assisting requesters, as well as assisting public officials in the supplying of information. The Information Officers should be trained on the whole of the law as this will ensure they are able to respond to internal questions within the public authority as well as questions from those requesting information on the application of the law. In training the Information Officers, particular attention during the initial stages should be placed on the proactive disclosure requirements found in Article 9(1) of the Model Law, whereby every public authority shall adopt a publication scheme which will be approved by the Information Commission. An emphasis should be placed on training the Information Officer within each public authority on the production of a publication scheme if a model scheme has not been presented to that class of public authorities. This training should include an explanation of how to assess which of the key classes of information under Article 12 of the law should reasonably be made available proactively in the first year of the law entering into force as well as what sorts of methods should be employed to disseminate the information widely in an accessible format. In turn, following the training received on proactive disclosure, the Information Officer should work to identify within the parameters of the law and the information held by the public authority, "(i) what specific information needs to be collected; (ii) by whom; (iii) how often; (iv) from where/whom; and (v) how the information can best be disseminated."[40] Trainings on proactive publication should then be given to those public officials who are likely to hold information that will be released proactively pursuant to the publication scheme.

Information Officers should train the other public officials on the archival and management of existing information as well as in the policies and procedures for maintaining future information. The training on records management should draw from the system developed by the body responsible for archives and the Information Commission under Article 33 of the Model Law. For more information on the development of an effective system for records management, see *Chapter 5: Adoption of Effective Information Management Policies and Systems to Properly Create, Maintain, and Provide Access to Public Information.*

The Information Commission should train the Information Officers on the process for filing and answering a request for information, as well as how to best assist a requester in the filling of the request. As the Information Officers will need to determine if information falls within an

---

[38] For more information on the establishment of the Information Commission see *Chapter 3: Monitoring, Enforcement, and Effectiveness of the Law.*

[39] Article 30 of the Model Law requires that each public authority designate one Information Officer. In smaller public authorities, it may be that this role can be added to an existing job description. In other public authorities where it is expected that there may be a high volume of requests, it may be necessary to have more than one Information Officer dedicated exclusively to the work as such.

[40] Commonwealth Human Rights Initiative, *Preparing for Implementation: Implementing Proactive Disclosure Duties*, available at *http*://www.humanrightsinitiative.org/programs/ai/rti/india/officials_guide/proactive_disclosure.htm

exception from disclosure under the law, the Information Commission must train the Information Officers in the application of exceptions as well as how to apply the public interest harm test. The Information Officer should then train the other public officials who may deal with information falling under an exception to disclosure, on the types of information that may be withheld.

B. Phase 2: Continuing/Permanent Capacity Building

Once the initial training has taken place and the law has entered into force, trainings should shift from focusing on the establishment of a functioning system to keeping the system functioning effectively. As with the initial training, it is necessary to tailor the follow-up trainings to the specific duties and roles of the various actors in the system. In addition, the frequency of these follow-up trainings should depend upon the type and level of responsibilities each actor has under the law.

Capacity Building for Information Officers
Information Officers are on the front lines of the implementation of the law and as such, require trainings more frequently than other public officials once the law has entered into effect. It is recommended that all Information Officers receive yearly trainings on such areas as the rights and responsibilities under the law, the policies and procedures for the archival, maintenance, and disposal of documents, the process for answering a request for information, and the types of technology employed in recording, tracking, and accessing information. In terms of procedures to request and disclose public information, in addition to understanding the specific content of the regulations and the ways in which the relevant mechanisms operate, Information Officers should be trained by the Information Commission to guide citizens in the preparation and submission of requests for information. In addition, Information Officers should be trained on how to file the yearly reports with the Information Commission on the status of implementation of the law.

Capacity Building for Other Types of Public Officials
Public officials other than the Information Officers working within a public authority are typically in positions whereby they frequently create information and as such, need to be trained on the archival, maintenance, and destruction of information as well as the general importance and letter of the law. During these trainings, the public officials should be made aware of the administrative and/or criminal penalties provided for in the law as well as any incentives that may be offered by the public authority to help promote effective implementation of the law. Special attention should be placed on teaching these other public officials on why access to information is important so that they don't see their responsibilities under the law as a burden, but instead as aiding transparency and the overall strengthening of democracy.

Where resources are limited, such continued trainings should take place at less frequent intervals, such as every five years, and immediately following a change in policies relating to the functioning of the law. Trainings should also be required as a part of the initial training received by public officials when they first begin to work for a public authority.

Capacity Building for Information Users
Training in the exercise of rights and promoting a culture of access among information users and among providers are equally important and must be regarded as two sides of the same coin. In this sense, in addition to actively engaging in training and awareness-raising for public officials, the State must undertake training initiatives for users as active and potential information requesters. These trainings should be coordinated by the Information Commission and should not

be limited to formal trainings but should include additional informal education through public awareness campaigns, access to information week activities, websites, pamphlets etc.

The State must invest human and budgetary resources in the public dissemination of the right of access to information, its benefits and scope, and the mechanisms and procedures by which such access is obtained. In addition to awareness-raising campaigns targeting the public as a whole, specific trainings should seek to target the most vulnerable sectors of society. Governments must therefore include budget allocations for mass campaigns on exercising the right to information.[41] Public authorities must also create assistance and support mechanisms for information requests, using guides, on-line assistance, circular hunt lines, and so forth.

C. Incentives

It is important to create a system of incentives to promote good practices relating to transparency and access to information. If incentives are already included in the law, they should be emphasized in the training, along with the benefits to administrators who comply with this right. Other incentives for civil servants include, for example, recognition and certification of officials involved in access to public information as a discreet professional category within the civil service, and merit-based incentives for high-performing civil servants.

The recognition of the social benefits of access to information constitutes a fundamental incentive, not just for public servants who implement the norms, but also for the public who participates actively and execute their right to access to information. The public needs to know how access to information can make a difference in the taking of decisions related to public and private matters.[42] In that regard, publicity campaigns and capacity building programs should include for example, concepts and information that illustrate the importance and the implications of an effective system of access to information.

---

[41] For more information on budgeting for capacity building activities, see *Chapter 4: Allocation of Resources Necessary to Create and Maintain an Effective Access to Information System and Infrastructure.*

[42] Villanueva Ernesto y Luna Pla, Issa. Coordinadores. "La importancia social del derecho a saber: preguntas y respuestas en los casos relevantes del IFAI", LIMAC, Libertad de Información – México, A.C., México 2005.

KEY POINTS
CAPACITY-BUILDING FOR INFORMATION PROVIDERS AND USERS

- Capacity building for both information providers (those working in the public authorities) and users (the general public) are necessary and vital elements to the smooth and effective implementation of the law.

- When beginning implementation of a new access to information regime, capacity building should focus on setting the foundations for an effective system of access and training public officials on the rights and duties under the new law as well as on new polices and procedures that will be enacted to ensure compliance with the law.

- Once the initial training has been conducted and the law is in force, the Information Commission and the public authorities should shift their focus to continuing education and refresher trainings to ensure that public officials remain up to speed on the law and the policies and procedures to ensure compliance.

- A training program for information providers should include why access to information is important, the laws and their scope, procedures for filing and responding to requests for information, and procedures and policies for archive maintenance and access. Training for information users should focus on why access to information is important, the rights guaranteed under the law, and procedures for how to file a request for information and an appeal.

- In designing and conducting trainings, it is important to ensure that all of the actors understand the importance of the law and how it will serve to strengthen democratic values overall.