CFP - 004M
C.P. - PL 95
Gouvernance et gestion des ressources informationnelles

2021

Commission des finances publiques

Consultations particulières et auditions publiques sur le projet de loi n° 95, Loi modifiant la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement et d'autres dispositions législatives

MEMOIRE

CAPT(RET) STEVE WATERHOUSE, CD

INFOSECSW

Capt (ret) Steve Waterhouse, CD
Expert en cybersécurité, CISSP

Sommaire exécutif

Le présent projet de loi 95 est plus que nécessaire, il est primordial ! Témoin récemment de toutes ces fuites de données, collectivement nous nous demandons à quand cesseront ces fuites ? Comment peut-on les prévenir ? En premier lieu, c'est de réaliser qu'appliquer le principe de « sécurité par l'obscurité » n'a plus sa place au 21e siècle.

Comme dans tout plan de protection (dans n'importe quel contexte), il faut connaître ce que l'on veut protéger et contre quoi. J'apporte souvent le point que les Évaluations des Menaces et des Risques (ÉMR) sont la base des prises de décisions que tous les dirigeants à n'importe quel niveau pratiquent sur une base régulière. Le cyberrisque, quant à lui, nécessite une attention particulière, car il en suffit de peu pour créer un évènement malheureux de perte de données qui en résulte en vol d'identité ou de demande de rançon.

Il est reconnu dans l'entreprise privée à bien des égards que la classification de l'information est réalisable en 7 étapes :

A. **Réaliser une évaluation des risques liés aux données sensibles**
B. **Développer une politique de classification formalisée**
C. **Catégoriser les types de données**
D. **Découvrir l'emplacement de vos données**
E. **Identifier et classer les données.**
F. **Activez les contrôles de prévention**
G. **Contrôler et maintenir les mesures**

Ces sept étapes appliquées globalement par le Conseil du Trésor seraient à être reprises et travailler à chacun des ministères selon moi afin qu'ils procèdent individuellement à leurs propres évaluations selon leur mission. À titre d'exemple, le MAPAC n'a pas autant de données que le MSSS à protéger et gérer, mais doit appliquer les mêmes règles dans le marquage de l'information en sa possession.

L'administration publique s'est dotée d'une référence de base pour la classification des actifs informationnels du Québec en 2016 appelée « Guide de catégorisation de l'information »[1] (ou PR-057), qui à mon sens n'est nullement le format d'outil pour effectuer efficacement l'exercice de classification proprement dit. De procéder avec une évaluation par la Disponibilité, l'Intégrité et la Confidentialité (DIC) de base est un début, mais n'est nullement pratique dans la mise en application des 4 niveaux de sensibilisation adoptés au PR-057, surtout dans l'identification de

données sensible selon leur évaluation. Les provinces de l'Ontario[2], de la Saskatchewan[3], de la Colombie-Britannique[4], de l'Alberta[5], du Nouveau-Brunswick[6] et du Yukon[7] ont produit des politiques de classification d'information en inspiration du modèle du gouvernement fédéral (Annexe A) depuis 2017. Une sorte d'uniformité dans les pratiques de classification facilite le partage des « trucs et astuces » entre provinces et le fédéral (du moins, facilite l'implantation des cadres). Et récemment, les organisations qui utilisent la suite Microsoft O365[8], peuvent programmer les niveaux de confidentialité et étiquettes de rétention en fonction des stratégies et politiques décidées. L'idée est d'approcher le besoin de classifier adéquatement pour que ce soit rapide et efficace tout en appliquant une forme de prévention de diffusion non autorisée de données (DLP) vers l'extérieur du GQ. Il est important d'apporter dans cette politique comment les données seront protégées en traitement (composées et/ou modifiées), au repos (entreposage), en transit (transmission), de quelle manière les données physique et électronique seront détruites (en considération du niveau de classification).

À titre d'exemple, depuis plusieurs années existe un moyen de transmettre des courriers électroniques sécuritaires via une infrastructure à clé publique (ICP) au ministère de la Justice[9]. Cette façon de faire pourrait servir à l'ensemble du Gouvernement, voir même avec le citoyen lorsque le projet d'identité numérique sera à terme et mature. De cette façon, les informations en transit demeureraient confidentielles, un risque de fuite de moins et adresserait le besoin de signatures numériques tel que mentionné dans les notes explicatives du présent projet de loi.

Dans ce PL-95, il serait approprié d'adresser comment les contrats devraient exiger la cybersécurité pour TOUT développeur / agences qui gèrent les données citoyennes, afin d'éviter les situations récentes comme avec le portail des garderies 0-5ans[10] et du portail « Clic Santé »[11]. De ces situations, à qui revient la responsabilité de la posture de sécurité (voir de la protection des données citoyenne) de ces contractés ? Les policiers pourront-ils prendre les dépositions des citoyens lorsqu'une plainte ou divulgation pour fuite d'information leur est apportée[12] ? Un exemple comment c'est simple, l'annexe « B » présente en une page, un tableau synthèse pour guider les contractuels (tout comme les fonctionnaires). La majorité des développeurs avec des projets similaires ci-haut mentionnés, si ce n'est pas tous, n'ont pas ou très peu de ressources en cybersécurité et documente très peu les politiques publiques de protection des renseignements personnels et protection de la vie privée.

Merci à nouveau pour cette opportunité d'échanger avec vous. Je suis maintenant disponible à répondre à vos questions.

Capt (ret) Steve Waterhouse, CD
Expert en cybersécurité, CISSP

Introduction

C'est un honneur et un privilège de m'adresser à vous sur ce sujet important.

Voici une brève introduction de mes origines. Après 23 ans de service avec les Forces armées canadiennes (R22eR et CIC) et au Ministère de la Défense Nationale (MDN), j'ai eu le privilège d'être parmi les premiers « cyber-soldats » au pays, passant par la gestion des systèmes d'information en réseau de la taille d'un réseau local (LAN - 250 utilisateurs), d'un réseau de campus (CAN - 650 utilisateurs) à celle d'un réseau métropolitain (MAN - plus de 5000 utilisateurs sur plusieurs sites), jusqu'aux premières phases d'intégration de la cybersécurité à titre d'Officier de Sécurité des Systèmes d'Information (OSSI) pendant 13 ans, principalement lors de la renaissance du Collège militaire royal de Saint-Jean (CMRSJ). Plus récemment, outre les divers mandats de consultation avec mon entreprise INFOSECSW, je continue cette mission d'éduquer et former tant les novices que les professionnels des technologies de l'information (TI) et à sensibiliser le public sur la manière d'appliquer les meilleures pratiques de sécurité envers les TI, principalement avec l'Université de Sherbrooke[13] et aussi via les médias d'information (locaux et nationaux et internationaux), la participation aux consultation de comités de la Chambre des Communes du Canada ainsi qu'avec l'Assemblée nationale du Québec et par la présentation de conférences au pays et ailleurs dans le monde.

La situation

Au cours des 20 dernières années, nos habitudes de travail se sont développées autour d'une technologie vouée à nous simplifier la vie, être plus efficace. Or, la technologie a évolué, mais son administration n'a pas suivi aussi rapidement. La stratégie de transformation numérique[14] récente en témoigne du besoin criant de revoir les pratiques Dès Que Possible (DQP).

Obligations des organismes public

Depuis l'avènement des réseaux informatiques modernes en 1994 au Ministère de la Défense Nationale (MDN), chacun de ces réseaux a fait l'objet d'un processus de certification et d'une accréditation ministérielle afin de rencontrer les normes uniformisées de sécurité de l'information du Conseil du Trésor. En ce sens, il n'y a pas un réseau au MDN, sans la documentation appropriée, qui peut être branchée au Réseau Étendu de la Défense (RÉD). Ça peut paraître onéreux comme processus administratif, cependant il y a pleins d'avantages dont celui de rencontrer les exigences minimales au branchement, avoir en main une ÉMR à jour, une topologie, la liste des personnes responsables des rôles (dont le responsable opérationnel), etc. J'y vois très bien, dans un but d'uniformiser l'application de la sécurité de l'information au sein du GQ, le déploiement de ce type de processus administratif, qui à terme, rendra plus ferme la connaissance de l'état des réseaux des différents ministères.

Dans cette documentation sera retrouvé par exemple :

A. ÉMR
B. Niveau maximal de classification de l'information traitée sur ce réseau (ce qui invoquera comment la topologie sera protégée)
C. Contrôles d'accès
D. Gestion des identités
E. Mécanismes d'authentification
F. Politique des mots de passe
G. Politique des audits – internes et externes
H. Lieu du stockage de l'information
I. Sécurité des appareils de traitement de l'information (anti-virus, etc.)
J. Stratégie de mise à jour
K. Stratégie de sauvegarde
L. Stratégie et lignes directrices sur l'utilisation des courriels
M. Zonage des lieux de traitement de l'information (espaces de travail selon le niveau de sécurité traité)
N. Politique d'utilisation des réseaux sans-fils
O. Politique d'usage d'Internet
P. Normes en usage du câblage et rangement des équipements de télécommunication
Q. Politique de destruction du matériel informationnel et physique

Cadre de gestion des données numériques

L'émission du COCD (Annexe C) des 15 mesures à tous les organismes publique et parapublique du GQ permet-elle d'atteindre un seuil de cybersécurité minimal ? Est-ce que tous sont au même niveau ?

La création des cinq nouvelles fonctions aidera certainement à mieux coordonner l'implantation des nouvelles mesures et d'un point de vue externe, faciliter la mise en œuvre de la transformation numérique avec en tête la sécurité par conception (security by design) .

Recommandations

Dans l'esprit du présent projet de loi 95, je propose que ces recommandations soient considérées pour doter l'administration publique des meilleures pratiques de protections de l'information:

A. Considérer la mise sur pied d'un programme de certification et accréditation dans le genre du programme du conseil canadien des normes « cybersécuritaire »[15]. L'utilisation de ce programme de conformité offrira une solution gagnant-gagnant pour les ministères et autres organismes parapublics à adopter et maintenir de saines pratiques de cybersécurité qui directement profiteront au GQ par possiblement moins de cas de mauvaise gestion d'information menant à des compromissions d'information citoyenne;

B. Exiger des candidats aux nouvelles fonctions de sécurité de l'information qu'ils aient comme requis d'emploi, une certification professionnelle propre au rôle (CISSP[16], CISM[17], C-CISO[18]), garantissant que la personne en poste a toutes les connaissances nécessaires à jour pour remplir son mandat, mais surtout qu'ils seront tributaires d'un code d'éthique propre à la certification du domaine que la formation universitaire de base n'offre pas;

C. La CAI doit augmenter son travail de prévention tant envers la population qu'envers les entreprises en ce qui concerne les bonnes pratiques de gestion de l'information comme les meilleures pratiques au traitement et à la transmission des données sensibles. Une mise à jour de son site web attirera les gens à s'y référer au lieu des éloignés. Et;

D. Octroyer aux services policiers davantage de spécialistes en crime technologique ainsi que les ressources (techniques et financières) nécessaires à aider les enquêteurs dans les nombreuses demandes et croissants d'enquête et d'expertises judiciaires avec la technologie. Sans quoi les délais ne cesseront de s'allonger et les criminels s'en sortiront sans payer de leur crime. Et le citoyen sera mieux desservi alors c'est actuellement un manque criant, surtout dans les corps policiers municipaux et régionaux.

Au service du GOUVERNEMENT, au service des CANADIENS

Respect Intégrité Excellence Leadership

Niveaux de sécurité

Renseignements et biens de nature délicate du gouvernement

Protégé
Lorsque l'on peut raisonnablement s'attendre à ce qu'une divulgation non autorisée porte atteinte à un intérêt autre que l'intérêt national, c'est à-dire à l'intérêt d'une personne ou d'une organisation.

Protégé A	Protégé B	Protégé C
Préjudice à une personne, une organisation ou un gouvernement.	Préjudice grave à une personne, une organisation ou un gouvernement.	Préjudice extrêmement grave à une personne, une organisation ou un gouvernement.

Classifié
Lorsque l'on peut raisonnablement s'attendre à ce qu'une divulgation non autorisée porte atteinte à l'intérêt national, c'est à-dire à la défense et au maintien de la stabilité sociopolitique et économique du Canada.

Confidentiel	Secret	Très secret
Préjudice à l'intérêt national.	Préjudice grave à l'intérêt national.	Préjudice extrêmement grave à l'intérêt national.

Personnel

Cote de fiabilité
Exigée d'un employé qui travaille sur un contrat fédéral de nature délicate pour accéder aux renseignements et aux biens Protégés (A, B ou C).

Attestation de sécurité sur le personnel
Exigée d'un employé qui travaille sur un contrat fédéral de nature délicate pour accéder aux renseignements et aux biens Classifiés (confidentiel, secret, très secret) (peux aussi accéder aux renseignements et aux biens Protégés).

Organisation du secteur privé

Vérification d'organisation désignée (VOD)
Permet à une entreprise d'envoyer des employés avec un besoin de connaître et qui ont fait l'objet d'une enquête de sécurité appropriée sur des lieux de travail à accès réglementé et de leur donner accès à des renseignements et à des biens Protégés.

Attestation de sécurité d'installation (ASI)
Permet à une entreprise d'envoyer des employés avec un besoin de connaître et qui ont fait l'objet d'une enquête de sécurité appropriée sur des lieux de travail à accès réglementé et de leur donner accès à des renseignements et à des biens Protégés et Classifiés.

Organisation du Traité de l'Atlantique Nord (OTAN) : Les niveaux de sécurité classifiés du Canada correspondent à ceux de l'OTAN, mais nécessitent une séance d'information spéciale et un engagement à respecter les exigences applicables de l'OTAN.

Des attestations de sécurité supplémentaires peuvent être accordées aux organisations qui font l'objet d'une VOD ou d'une ASI.

Autorisation de détenir des renseignements (ADR) : autorisation de détenir, de traiter et de protéger des renseignements ou des biens Protégés ou Classifiés sur les lieux de travail. **Production :** autorisation de produire des biens de nature délicate. **Sécurité physique liée à la sécurité des TI et COMSEC/INFOSEC :** peut être un critère dans certains contrats.

Canada

Tableau des niveaux de sécurité de l'information du Gouvernement du Canada – mars 2021
https://www.tpsgc-pwgsc.gc.ca/esc-src/documents/niveaux-de-securite.pdf-breaches-hacks/

Annexe B

Administration canadienne de la sûreté du transport aérien – Tableau des procédures de protection des documents

Canadian Air Transport Security Authority | Administration canadienne de la sûreté du transport aérien

Non classifié

PROCÉDURES DE PROTECTION DES DOCUMENTS

Avril 2017

Exigences	Protégé A	Protégé B / Confidentiel / Divulgation non autorisée interdite (DNAI)	Secret
Mention	– Protégé A	– Protégé B, Divulgation non autorisée interdite ou Confidentiel	– Secret
Archivage électronique	– Réseau sécurisé conformément à la GSTI[1] – Support de données portatif placé dans un classeur verrouillé à clé	– Réseau sécurisé conformément à la GSTI[1] – Chiffré sur un support de données portatif placé dans un classeur de sécurité doté d'une serrure à combinaison intégrée, dans une zone de travail	– Réseau sécurisé conformément à la GSTI[1] – Ordinateur portatif secret conformément à la GSTI[1] – Chiffré sur support portatif placé dans un classeur de sécurité doté d'une serrure à combinaison intégrée, dans une zone de travail
Transmission électronique	– Courriel sur réseau sécurisé conformément à la GSTI[1] – Téléphone ordinaire, ligne terrestre – Imprimante sur réseau sécurisé conformément à la GSTI[1] – Télécopieur ordinaire, si le destinataire est au courant de la transmission	– Courriel sur réseau sécurisé conformément à la GSTI[1] – Courriel chiffré, s'il est envoyé à l'externe – Téléphone ordinaire, ligne terrestre seulement – Imprimante sur réseau sécurisé conformément à la GSTI[1] si la fonction d'impression sécurisée est utilisée – Télécopieur sécurisé, si le destinataire est au courant de la transmission	– NE PAS recourir aux courriels ou à une ligne terrestre – Téléphone sécurisé seulement – Imprimante autonome – Télécopieur sécurisé, si le destinataire est au courant de la transmission
Entreposage physique	– Classeur verrouillé à clé, dans une zone de travail	– Classeur de sécurité doté d'une serrure à combinaison intégrée, dans une zone de travail	– Classeur de sécurité doté d'une serrure à combinaison intégrée, dans une zone de travail
Transmission physique	Enveloppe: – Une enveloppe scellée comprenant une adresse de réexpédition et aucune mention de sécurité Transport: – Courrier de 1re classe – Messageries prioritaires externes et fiables (p. ex., Priorité de Postes Canada, Purolator, FedEx)	Enveloppe: Protégé B / Confidentiel – Une enveloppe scellée comprenant une adresse de réexpédition et aucune mention de sécurité DNAI – Enveloppe double, non marquée, comprenant une adresse de réexpédition et aucune mention de sécurité sur l'enveloppe extérieure; l'enveloppe intérieure porte les mentions « **Divulgation non autorisée interdite** » ET « À être ouvert par le destinataire uniquement » Transport: – Messageries prioritaires externes et fiables (p. ex., Priorité de Postes Canada, Purolator, FedEx) avec suivi	Enveloppe: – Enveloppe double, non marquée, comprenant une adresse de réexpédition et aucune mention de sécurité sur l'enveloppe extérieure; l'enveloppe intérieure porte les mentions « **Secret** » ET « À être ouvert par le destinataire uniquement » Transport: – Par porteur – Par courrier, au Canada : messageries prioritaires externes et fiables (p. ex., Priorité de Postes Canada, Purolator, FedEx), un formulaire de suivi et de transmission du document devant être remis à la réception – Par courrier, à l'extérieur du Canada : service de courrier diplomatique de sécurité
Destruction	– Bacs de déchiquetage vidés par une entreprise de déchiquetage de documents agréée qui détruira les documents classés **Protégé A** de manière sécurisée – Déchiqueteuses à coupes transversales	– Bacs de déchiquetage vidés par une entreprise de déchiquetage de documents agréée qui détruira les documents classés **Protégé B**, **Divulgation non autorisée interdite** ou **Confidentiel** de manière sécurisée – Déchiqueteuse – *au moins de type III (2 x 15 mm)*	– Bacs de déchiquetage vidés par une entreprise de déchiquetage de documents agréée qui détruira les documents classés **Secret** de manière sécurisée et remettra un certificat de destruction une fois le document détruit – Déchiqueteuse – *au moins de type II, niveau 6 (1 x 5 mm)*
Remarques		La divulgation de renseignements classés DNAI en vertu de l'article 4.79 de la *Loi sur l'aéronautique* pourrait nécessiter le consentement du Ministre des Transports ou de Transports Canada.	*Les documents classés Secret peuvent uniquement être reproduits si le BPR en donne l'autorisation. Un identifiant unique est alors attribué aux exemplaires et un registre de distribution est maintenu aux fins de contrôle.*
Habilitation de sécurité	– Fiabilité	– Fiabilité	– Secret

[1] Norme opérationnelle de sécurité : *Gestion de la sécurité des technologies de l'information (GSTI)* : http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=12328

Canada

CATSA ACSTA

Annexe C
Les 15 règles minimales du Centre Opérationnelle de Cyber Défense (COCD)

15 règles minimales COCD
1.1 - Inventaire : UCMDB
1.2 - Serveurs désuets
1.3 - Mitigation des serveurs désuets
1.4 - Postes de travail désuets
1.5 - Mitigation des postes de travail désuets
1.6 - Appareils mobiles désuets
1.7 - Équipements de télécom désuets
2.1 - Détection des vulnérabilités
2.2 - Correctifs sur les serveurs
2.3 - Correctifs sur les postes de travail
2.4 - Correctifs sur les appareils mobiles
2.5 - Télétravail (stratégie de MAJ automatisée sur postes hors site)
2.6 - Télétravail (stratégie de validation de conformité pour appareil en accès VPN)
3.1 - Antivirus EDR sur les serveurs
3.1 - Antivirus EDR sur les postes de travail
4.1 - MFA (Autentification multifacteurs)
5.1 - Prise de copies (Infrastructure isolée)
5.2 - Prise de copies (Plan de reprise documenté)
5.3 - Prise de copies (stratégie quotidienne en fonction)
5.4 - Prise de copies (exercices de recouvrement périodique)
6.1 - Données confidentielles (solution de courriel sécurisé est disponible)
6.2 - Données confidentielles (sensibilisation et formation des employés)
7.1 - Balayage de vulnérabilités externes (inscription centre cyber défense)
7.2 - Balayage de vulnérabilités externes (établir un processus de correction des lacunes découverte, en continu)
8.1 - Surveillance (accès aux systèmes exposés web sont journalisés)
8.2 - Surveillance (stratégie en place pour détecter et bloquer les tentatives de connexion aux systèmes exposés web)
9.1 - Captcha (services externes protégés par)
10.1 - Notifications (notification aux citoyens pour accès/changement compte)
11.1 - Transmissions sécuritaires (moyen mise à disposition citoyens pour dépôts sécuritaires)
12.1 - Hameçonnage (campagne de simulation)
13.1 - Directives (aux employés si menaces, courriels malicieux...)
14.1 - Gestion des accès (processus d'ajouts, révisions, retraits dans gestion mouvement du personnel)
14.2 - Gestion des accès (processus d'ajouts, révisions, retraits dans gestion accès à haut privilège)
14.3 - Gestion des accès (outil de journalisation implantée)
15.1 - Formation (plan de formation en cybersécurité capsules ATN minimum)

Annexe D
Références

[1] Guide de catégorisation de l'information – PR-057 – ver 2.1 - https://www.tresor.gouv.qc.ca/fileadmin/PDF/ressources_informationnelles/securite_information/categorisation_information.pdf
[2] Ontario Corporate policy on information sensitivity classification - https://www.ontario.ca/page/corporate-policy-information-sensitivity-classification
[3] Saskatchewan Information Protection Security Controls for Classified Data (IPSC) - https://taskroom.sp.saskatchewan.ca/Documents/Information-Protection-Security-Controls-for-Classified-Data.pdf
[4] BC Information Security Classification - https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/information-security-classification
[5] Alberta Data and Information Security Classification Standard - https://imtpolicy.sp.alberta.ca/standards/pdf/Data-and-Information-Security-Classification-Standard.pdf
[6] NB Cyber Security Directive:IT 9.02 – Data Classification - https://www2.gnb.ca/content/dam/gnb/Departments/tb-ct/pdf/OCIO/cyber/directives/e/09-02.pdf
[7] Yukon INFORMATION CLASSIFICATION TABLE - https://www.yukonombudsman.ca/uploads/media/5605aeed2eae8/Information%20Physical%20and%20Network%20Classification%20Table.pdf?v1
[8] Microsoft O365 - En savoir plus sur la classification des données - https://docs.microsoft.com/fr-ca/microsoft-365/compliance/data-classification-overview?view=o365-worldwide
[9] MJQ – Infrastructure à Clé Publique - https://www.infocles.justice.gouv.qc.ca/?nav=rubrique[@nom=%27public%27]/rubrique[@nom=%27principes%27]
[10] Radio-Canada - Des entreprises du web ont accès aux données des enfants de garderies - https://ici.radio-canada.ca/nouvelle/1792386/garderies-entreprises-web-acces-donnees-enfants
[11] Radio-Canada - Le ministère de la Santé du Québec à l'origine d'une brèche informatique - https://ici.radio-canada.ca/nouvelle/1795328/faille-informatique-clic-sante-ministere-sante-vaccination
[12] LaPresse - Une mère militante contactée par le pirate, ignorée par la SQ - https://www.lapresse.ca/actualites/2021-05-13/vol-de-donnees-a-la-place-0-5/une-mere-militante-contactee-par-le-pirate-ignoree-par-la-sq.php
[13] CeFTI - Centre de formation en technologies de l'information - Microprogramme de 2e cycle en sécurité informatique - volet prévention (À distance) (https://www.usherbrooke.ca/cefti/futurs-etudiants/microprogramme-de-2e-cycle-en-securite-informatique-volet-prevention-a-distance/)
[14] STRATÉGIE DE TRANSFORMATION NUMÉRIQUE GOUVERNEMENTALE 2019•2023 - https://www.quebec.ca/gouv/politiques-orientations/vitrine-numeriqc/strategie-numerique
[15] CyberSécuritaire Canada - https://www.ic.gc.ca/eic/site/137.nsf/fra/accueil
[16] ISC2 Certified Information Systems Security Professional (https://www.isc2.org/Certifications/CISSP)
[17] ISACA Certified Information Security Manager (https://www.isaca.org/credentialing/cism)
[18] EC Council C-CISO - https://ciso.eccouncil.org/