External Affairs and International Trade Canada

Canada

Affaires extérieures et Commerce extérieur Canada

UNCLASSIFIED

OTTAWA, August 23, 1993

CIRCULAR DOCUMENT

Admin. No. 12/93 (MST)

The MITNET external access facility (DISA) and its authorization codes

The Department is in the process of implementing its Multipurpose Integrated Telecommunications NETwork (MITNET) to provide consolidated communication facilities for mission communications. MITNET is the EAITC international digital communications network providing voice and data communications facilities between all EAITC missions and Headquarters.

2. As part of that implementation, most missions are also being provided with an off-mission access facility, termed **D**irect **I**nward **S**ystem **A**ccess (DISA). Attached as an annex are the procedures for the use of DISA and the policy surrounding DISA security insofar as the Department is concerned.

3. This circular expires on July 31, 1994, but its contents will be published in the departmental *Manual of Communications*, EAIT 4(2).

NON CLASSIFIÉ

OTTAWA, le 23 août 1993

CIRCULAIRE ADMINISTRATIVE

Admin. n° 12/93 (MST)

Le dispositif d'accès externe du MITNET (ADAS) et ses codes d'accès

Le Ministère procède actuellement à la mise en oeuvre du Réseau polyvalent intégré de communications (MITNET), afin de procurer aux missions des installations de communication unifiées. Le MITNET est le réseau international de communication numérique propre à AECEC; il assure la communication phonique et la communication de données entre l'ensemble des missions d'AECEC et l'Administration centrale.

2. Par la même occasion, le Ministère équipe aussi la plupart des missions d'un dispositif d'accès externe appelé **A**ccès **d**irect au système (ADAS). Vous trouvez en annexe les modalités régissant l'emploi de l'ADAS et la politique de sécurité du Ministère à cet égard.

3. La présente circulaire expire le 31 juillet 1994, mais son contenu sera publié dans le *Manuel des communications* du Ministère, AECE 4(2).

Le Sous-secrétaire d'État
aux Affaires extérieures

Under-Secretary of State
for External Affairs

FOR INFORMATION

Deputy Ministers

FOR ACTION

Heads of Mission
Assistant Deputy Ministers
Directors General
Directors

À TITRE D'INFORMATION

Sous-ministres

POUR SUITE À DONNER

Chefs de mission
Sous-ministres adjoints
Directeurs généraux
Directeurs

The MITNET external access facility (DISA) and its authorization codes

1. RESPONSIBILITIES

1.1 Implementation of this policy at missions is the responsibility of the Head of Mission through the mission Administration staff. The Mission Security Officer is to assure, together with the mission or regional technician (EL), that proper restrictions are applied.

1.2 Implementation of this policy at Headquarters is the responsibility of the Director of the Telecommunications Division (MST) through appropriate MST delegated administration staff.

2. DIRECT INWARD SYSTEM ACCESS (DISA)

Direct Inward System Access (DISA) is a powerful feature which permits a caller on the local commercial exchange to dial directly into a private telephone system (mission or Headquarters) without attendant assistance to gain access to telephone facilities.

2.1 Restrictions

2.1.1 DISA enables an authorized individual to access the department's telephone network and be recognized as a user. Adequate controls must be applied to prevent costly unauthorized use on this expensive network.

2.1.2 Guarding your authorization code is of utmost importance. It is proven that passwords or authorization codes are not effective control measures unless properly handled. The ease with which "hackers" can penetrate networks is well documented and presents substantial risks if the access is not well controlled. Technology available to hackers allows them to pierce through barriers made of codes which are not properly set up and administered, by using commonly available PCs and modems. Booklets are available on the market where DISA numbers are sold at a minimal price for buyers to gain access to a corporation's system to make long distance calls at that corporation's expense.

Le dispositif d'accès externe du MITNET (ADAS) et ses codes d'accès

1. RESPONSABILITÉS

1.1 À la mission, il incombe au chef de mission d'assurer la mise en oeuvre de la présente politique, par l'entremise du personnel administratif de la mission. L'agent de sécurité de la mission doit, avec l'aide du technicien rattaché à la mission ou du technicien régional (EL), veiller à l'application des restrictions appropriées.

1.2 À la Centrale, il incombe au directeur de la Direction des télécommunications (MST) d'assurer la mise en oeuvre de la présente politique, par l'entremise du personnel administratif délégué approprié.

2. ACCÈS DIRECT AU SYSTÈME (ADAS)

L'Accès direct au système (ADAS) est un dispositif qui permet à une personne composant un appel à partir d'un centre local, rattaché à un réseau commercial, d'accéder directement à un système téléphonique privé (celui d'une mission ou de l'Administration centrale), sans l'aide d'un préposé.

2.1 Restrictions

2.1.1 L'ADAS permet à une personne autorisée d'accéder au réseau du Ministère et d'être reconnue comme usager autorisé. On doit donc mettre en place des mécanismes aptes à empêcher tout usage non autorisé et coûteux de ce réseau dispendieux.

2.1.2 Il est prouvé que les mots de passe et les codes d'autorisation ne constituent pas des mesures de contrôle efficaces s'ils ne sont pas bien administrés, et il existe une importante documentation sur la facilité avec laquelle des «intrus» peuvent s'introduire dans des réseaux dont l'accès est insuffisamment contrôlé. La technologie accessible aux intrus leur permet, au moyen d'ordinateurs personnels et de modems courants, de faire échec aux obstacles composés de codes si ces derniers sont mal établis et mal administrés. On sait que pour des sommes modestes, il est possible de se procurer sur le marché des dépliants dévoilant les numéros ADAS donnant accès aux systèmes d'un organisme ou permettant d'effectuer des appels interurbains aux frais de cet organisme. Il est donc de la plus haute importance que les utilisateurs protègent adéquatement leur code d'autorisation.

2.1.3 To minimize our being targeted by unauthorized individuals and to minimize usage billing to another cost centre, certain additional restrictions are required. Since every mission with DISA becomes a gateway to all our telecommunications facilities, restrictions are to be applied directly at the DISA telephone line level. Access shall be controlled by the issuance of individually assigned authorization codes of eight digits.

2.1.3 Afin de minimiser la possibilité de devenir une cible pour les personnes non autorisées et aussi de minimiser les coûts imputés à d'autres, certaines restrictions additionnelles sont requises. Vu que chaque mission avec le dispositif ADAS devient une passerelle pour tous les dispositifs de communications du Ministère, des restrictions doivent être instituées directement sur les lignes téléphoniques réservées à l'accès ADAS. L'accès devra être contrôlé par l'attribution individuelle d'un code d'autorisation de huit chiffres.

2.1.4 A user with access to DISA will be allowed to dial over MITNET to extensions within MITNET missions plus the free calling area of the National Capital Region (NCR) i.e. area codes 613 and 819. (See special provisions of section 2.3)

2.1.4 Un utilisateur ADAS pourra emprunter le réseau MITNET pour composer des numéros donnant accès aux postes téléphoniques des missions raccordées à ce réseau et des numéros situés dans la zone d'appels gratuits de la Région de la capitale nationale (RCN), c.-à-d. dans la zone correspondant aux codes régionaux 819 et 613. (Voir les arrangements spéciaux de la section 2.3)

2.1.5 DISA **must not** be programmed to allow access to the mission's public local lines or public long distance lines.

2.1.5 La programmation du dispositif ADAS **ne doit pas** permettre d'accéder aux lignes locales ou interurbaines de la mission.

2.1.6 All missions with DISA facilities are provided with Call Detail Recording (CDR) software and printers to allow appropriate monitoring of DISA calls. Programming should be performed by the mission or regional EL.

2.1.6 Toutes les missions avec le dispositif ADAS ont le logiciel et l'imprimante pour leur permettre la surveillance des appels ADAS. La programmation doit être faite par le technicien EL de la mission ou le EL régional.

2.2 Access to DISA

2.2 Accès à l'ADAS

2.2.1 Access for Headquarters-based authorization code holders in **travel status** is through Teleglobe "Canada Direct" facilities using a Bell Canada "Call-me" card. This card allows the holder to make calls to the Ottawa DISA facilities through "Canada Direct". Further information on the use of "Canada Direct" facilities and the issuance of "Call-me" cards can be obtained through MSTH.

2.2.1 Les employés de la Centrale **en déplacement** et détenteurs d'un code d'autorisation de la Centrale ont accès à l'ADAS en utilisant «Canada Direct» de Téléglobe et la carte «Appelez-moi» de Bell Canada. Cette carte permet au détenteur de placer des appels sur l'ADAS d'Ottawa par l'entremise de Canada Direct. Pour plus de renseignements sur l'utilisation de «Canada Direct» et pour obtenir la carte «Appelez-moi», communiquez avec MSTH.

2.2.2 DISA facilities at missions are for mission staff holders of an authorization code issued by the mission administration. Special personal requests for access through a mission should be made with the mission and are authorized at the HOM's discretion.

2.2.2 Les installations ADAS à la mission sont à l'usage réservé des employés de la mission détenteurs d'un code d'autorisation délivré par l'administration de la mission. Les demandes spéciales pour accès aux installations ADAS d'une mission sont faites à la mission et sont à la discrétion du Chef de mission.

2.2.3 Access to DISA can be gained from a residence, a hotel, a telephone booth or other telephone on the public telephone network, subject to the above.

2.2.3 Sous réserve de ce qui précède, on peut employer l'ADAS à partir d'une résidence, d'un hôtel, d'une cabine téléphonique ou d'un autre appareil du réseau téléphonique publique.

2.2.4 Dialling procedures may vary from mission to mission depending on the type of telephone system installed. Users therefore need to check correct access procedures applicable to the location from which access to DISA is required.

2.2.5 It is important to note that DISA is dependent on DTMF tones; these are the tones heard when using push-button telephones. Rotary dial instruments and instruments making digit translation (such as DigiPulse) will not work. In such cases, users must use a hand-held Tone Dialler which, when held against the mouth piece of the rotary instrument, will allow tones to be transmitted, therefore simulating a DTMF instrument.

2.2.6 Many countries still do not offer DTMF facilities. The acquisition of a hand-held Tone Dialler is the responsibility of an individual. A person requiring its use must procure a unit through appropriate departmental procedures. There are several types available on the market in North America and abroad. MST will, on request, provide advice concerning the best units.

2.3 DISA Calls Off-Net

2.3 Off-net calls means calls to locations outside MITNET, e.g. communications terminating outside diplomatic missions.

2.3.1 DISA calls to off-net locations **outside North America** (for example, calls placed from a residence in Tokyo to a colleague's residence in Geneva) are not allowed to be completed directly and should not be possible if appropriate restrictions as outlined in section 2.1 are in place. A user in need of placing such calls can:

a) go to the office at the mission or Headquarters and dial from an internal extension,

b) make the call over commercial lines from a commercial instrument and then claim reimbursement,

2.2.4 Les modalités de composition pourront varier selon les missions en fonction du type de système téléphonique employé. Les utilisateurs doivent donc vérifier les modalités d'accès applicables à l'endroit où l'ADAS est demandé.

2.2.5 Il est à noter que l'ADAS fonctionne à partir des tonalités DTMF dites fréquences vocales (qui sont les tonalités que l'on entend lorsque l'on utilise un téléphone à clavier). Les appareils à cadran et les appareils effectuant la conversion numérique (comme les appareils DigiPulse) ne peuvent servir à cette fin et les utilisateurs doivent alors employer un générateur de tonalités portatif qui, tenu contre le microphone de l'appareil à cadran, permet de transmettre les tonalités et simule ainsi la composition d'un appareil DTMF.

2.2.6 Plusieurs pays ne possèdent pas encore d'installations DTMF. L'acquisition d'un générateur de tonalités portatif incombe à l'usager. Les personnes qui requièrent l'usage d'un tel générateur doivent s'en procurer un selon les modalités en vigueur au Ministère. Plusieurs types de générateurs sont offerts sur les marchés nord-américain et étranger. MST peut, sur demande, fournir des conseils sur les meilleurs modèles.

2.3 Appels ADAS hors-réseau

2.3 Le terme appel hors-réseau signifie appel donc la destination est à l'extérieur du MITNET, comme dans le cas de communications dont la destination se situe à l'extérieur des missions diplomatiques du Canada.

2.3.1 Il n'est pas permis d'acheminer directement des appels ADAS hors-réseaux à des destinations **extérieures à l'Amérique du Nord** (comme un appel émanant d'une personne qui, de sa résidence à Tokyo, voudrait rejoindre un ou une collègue à sa résidence à Genève). Ce type d'appel ne devrait pas être possible si les restrictions présentées en 2.1 ont été correctement mises en place. Un usager devant effectuer un appel de ce type peut choisir entre les options suivantes :

a) se rendre à son bureau situé à la mission ou à l'Administration centrale et acheminer l'appel à partir d'un poste interne,

b) effectuer l'appel sur le réseau commercial au moyen d'un appareil commercial et présenter par la suite une demande de remboursement,

c) dial the Government Operator (613-954-5432 for the Ottawa/Hull area) using MITNET, give the authorization code and number desired.

2.3.2 DISA calls to off-net locations **inside North America** (for example, a call placed from a residence in Tokyo to a residence in Montreal) can be completed through the Government Operator. Users can dial the Government Operator, give their authorization code and number desired. The Operator will connect the call.

2.3.3 DISA calls over MITNET to areas within the National Capital Region (area codes 613 and 819) can be dialled directly from any location.

2.4 DISA Access by OGDs

2.4.1 Authorized employees of Other Government Departments (OGDs) may be given access to MITNET DISA facilities. Access will be granted strictly on a case-by-case basis. Written requests for such access should be sent to MSTH for consideration. Individuals from OGDs must first be recipients of a Government Telecommunications Agency (GTA) valid authorization code and disclose their code to the Telecommunications Division Authority for input into the EAITC system. Departments will be responsible for payment for usage.

2.4.2 Group codes will not be accepted as this does not satisfy the Treasury Board policy on authorization codes.

3. AUTHORIZATION CODES

An Authorization Code is a numeric code issued to a DISA user for proof of authorization to use the system and as identification for billing purposes.

3.1 General Information

3.1.1 Authorization codes are intended for use by authorized personnel who are regularly on travel status or who do not have direct access to a mission telephone system or to the Departmental telephone system because of their distant physical location.

c) composer, à partir du réseau MITNET, le numéro du standardiste du gouvernement (613-954-5432 pour la région Hull/Ottawa), à qui il indiquera son code d'autorisation et le numéro désiré.

2.3.2 Il est permis d'effectuer, par l'entremise du standardiste du gouvernement, des appels ADAS hors-réseaux à des destinations situées **en Amérique du Nord** (dans le cas où une personne souhaiterait par exemple appeler, de sa résidence à Tokyo, une personne se trouvant à sa résidence, à Montréal). Les usagers doivent composer le numéro du standardiste du gouvernement à qui ils indiqueront leur code d'autorisation et le numéro à composer pour acheminer l'appel.

2.3.3 Pour les appels vers la région de la capitale nationale (codes régionaux 613 et 819), on peut effectuer des appels ADAS directement de n'importe où, par l'entremise du réseau MITNET.

2.4 Accès ADAS accordé à d'autres ministères

2.4.1 Des employés autorisés relevant d'autres ministères peuvent avoir accès, sur une base strictement individuelle, aux installations ADAS du MITNET. Toute demande à cette fin doit être présentée par écrit à MSTH qui l'examinera. Les membres des autres ministères doivent au préalable détenir un code d'autorisation valide de l'ATG, et fournir ce code aux responsables de la Direction des télécommunications en vue de son inscription dans le système d'AECEC. Les ministères devront payer les coûts d'utilisation du service.

2.4.2 On n'acceptera pas les codes de groupes, ceux-ci n'étant pas conformes à la politique du Conseil du Trésor concernant les codes d'autorisation.

3. CODES D'AUTORISATION

Un code d'autorisation est un code numérique fourni à un utilisateur ADAS comme preuve de son habilitation à employer le système, et sert à identifier l'usager à des fins de facturation.

3.1 Renseignements généraux

3.1.1 On destine les codes d'autorisation aux employés autorisés qui doivent se déplacer fréquemment ou qui ne peuvent accéder directement au système téléphonique d'une mission ou du Ministère du fait qu'ils se trouvent hors des locaux.

3.2 Authorization Code Assignment

3.2.1 Each authorization code will be issued to a single user and its use will be restricted to that user.

3.2.2 Authorization codes will be assigned to authorized individuals at Headquarters or at missions abroad on written request. At Headquarters, requests for authorization codes should be forwarded to MSTH. Issuance of authorization codes at missions is the responsibility of mission administration.

3.2.3 At Headquarters, authorization codes are issued within approximately 10 working days following receipt of the request in MSTH.

3.2.4 Receipt of the authorization code will be confirmed by signing and forwarding to the issuing office an *Acknowledgement of Responsibility for a Telephone Authorization Code* (form EXT 1411).

3.3 Protection of Authorization Codes

3.3.1 Knowledge of the assigned authorization code must be limited only to the user and the departmental staff administering the authorization codes, and not used in regular correspondence. Each authorization code has its own identifying account number for reference use. To protect confidentiality and financial accountability, the account number shall only be used to identify an authorization code on all documents. Where an authorization code appears on a document (e.g. upon issuing a code to a user), the document must be restricted to those who have a need to know and must be protected in accordance with the requirements of the government security policy and standards for sensitive information.

3.3.2 Authorization codes should not be recorded on wallet held cards or on cards such as the *Government Intercity Calling Guide*. While it is realized that the average user does not memorize the authorization code number, any recording of the number should be made in a place and in a way which does not associate the authorization code with MITNET or the government long distance network nor disclose the purpose of the code.

3.3.3 In addition, authorization code users should be aware that there is a security risk involved in placing telephone calls over radio and cellular

3.2 Attribution d'un code d'autorisation

3.2.1 On attribuera un seul code d'autorisation par utilisateur, qui en aura l'usage exclusif.

3.2.2 Les codes d'autorisation seront accordés au personnel autorisé à l'Administration centrale et aux missions à la suite d'une demande écrite à cet effet. À l'Administration centrale, la demande devrait être adressée à MSTH. Aux missions, les codes seront accordés par l'administration de la mission.

3.2.3 À l'Administration centrale, les codes d'autorisation sont attribués dans un délai d'environ dix jours suivant la réception de la demande par MSTH.

3.2.4 La réception d'un code d'autorisation sera confirmée par la signature et l'envoi au service chargé de l'assignation des codes de la *Formule d'acceptation des responsabilités du code d'autorisation téléphonique* (formulaire EXT 1411).

3.3 Protection des codes d'autorisation

3.3.1 Seuls le titulaire d'un code d'autorisation et le personnel ministériel qui en assure l'administration sont autorisés à connaître un code. La correspondance courante ne peut faire mention des codes. À des fins de référence, on attribue à chaque code un numéro de compte que l'on utilise en remplacement du code dans tous les documents afin de protéger les aspects de confidentialité du code et de responsabilité financière. Lorsqu'un code d'autorisation figure dans un document (par ex. lors du dévoilement du code à l'usager), on doit en restreindre l'accès selon le principe de l'accès sélectif et lui assurer une protection conforme aux exigences formulées dans la politique et les normes concernant la sécurité du gouvernement à l'égard des renseignements délicats.

3.3.2 On ne doit pas inscrire de code d'autorisation sur des cartes que l'on conserve dans son portefeuille, en particulier sur des cartes comme la *Carte d'accès au réseau téléphonique interurbain de l'État*. Si l'usager ne peut mémoriser son numéro de code d'autorisation, il ne doit toutefois consigner ce code qu'en des endroits et d'une manière empêchant que l'on établisse un lien entre le code d'autorisation et le MITNET ou le réseau interurbain de l'État, et que l'on comprenne l'utilité du code.

3.3.3 De plus, les utilisateurs de codes d'autorisation doivent savoir que le fait d'effectuer des appels par radio, par téléphone cellulaire, ou par l'entremise

telephones or through hotel or motel telephone operators. (Authorization codes could be compromised by unscrupulous personnel remaining online and eavesdropping on conversations.)

3.3.4 A new authorization code should be requested without hesitation if it is suspected that an authorization code has been compromised.

3.4 Financial Responsibility

3.4.1 On receipt of an authorization code, an individual assumes financial responsibility for expenditures incurred through the use of that authorization code. Accordingly, individuals are required to sign for authorization codes issued.

3.5 MITNET Codes and Government Codes

3.5.1 Codes issued by MSTH are valid for use over the GTA facilities as well as MITNET.

3.6 Cancellation Procedures

3.6.1 When an authorization code is no longer required (e.g. when an employee leaves the Department), the employee must request its cancellation by writing to the issuing authority. Authorization codes will be cancelled within 10 working days following receipt of the request.

3.6.2 In an emergency situation (e.g. loss or abuse of the authorization code), the individual should notify the issuing authority verbally to cancel the authorization code. Cancellation will be effective within 24 hours. Such a verbal request must be followed by a written request.

3.7 Abuse of Authorization Codes

3.7.1 The authorization codes are for official use only. In cases where abuse has been confirmed, appropriate recovery and disciplinary action will be undertaken.

d'un standardiste d'hôtel comporte des risques pour la sécurité (Car il existe une possibilité de révélation des codes par des employés peu scrupuleux demeurant en ligne pour épier des conversations).

3.3.4 On doit sans hésitation demander un nouveau code si l'on a des raisons de soupçonner qu'un code d'autorisation a pu être dévoilé.

3.4 Responsabilité financière

3.4.1 La personne à qui l'on attribue un code d'autorisation assume dès lors la responsabilité financière des dépenses liées à son utilisation. Par conséquent, les personnes à qui l'on fournit un code doivent signer un accusé de réception.

3.5 Codes MITNET et codes gouvernementaux

3.5.1 Les codes attribués par MSTH sont valides autant pour utilisation sur le réseau gouvernemental que sur MITNET.

3.6 Modalités d'annulation

3.6.1 La personne qui n'a plus besoin d'un code d'autorisation (par exemple dans le cas d'un employé quittant le Ministère) doit demander son annulation par écrit à l'administration qui le lui a attribué. Cette administration prendra des dispositions à cet effet dans les dix jours suivant la réception de la demande.

3.6.2 S'il y a urgence (par exemple en raison de la perte du code ou de son emploi inconsidéré), la personne peut demander verbalement à l'administration d'annuler le code. L'annulation entrera en vigueur dans un délai de 24 heures. La personne doit faire suivre sa demande verbale d'une demande d'annulation par écrit.

3.7 Emploi inconsidéré de codes d'autorisation

3.7.1 Les codes d'autorisation ne doivent servir qu'à des fins officielles. S'il a été établi qu'un utilisateurs a utilisé son code de façon inconsidérée, on exigera de lui le remboursement des dépenses injustifiées et on prendre [illegible] appropriées à son endroit.