RETURN BIDS TO:
RETOURNER LES SOUMISSIONS À:
Bid Receiving - PWGSC / Réception des soumissions - TPSGC
11 Laurier St. / 11, rue Laurier
Place du Portage , Phase III
Core 0B2 / Noyau 0B2
Gatineau, Québec K1A 0S5
Bid Fax: (819) 997-9776

SOLICITATION AMENDMENT
MODIFICATION DE L'INVITATION

The referenced document is hereby revised; unless otherwise indicated, all other terms and conditions of the Solicitation remain the same.

Ce document est par la présente révisé; sauf indication contraire, les modalités de l'invitation demeurent les mêmes.

Comments - Commentaires
This Document contains a Security Requirements

Vendor/Firm Name and Address
Raison sociale et adresse du fournisseur/de l'entrepreneur

Issuing Office - Bureau de distribution
Business Management and Consulting Services Division / Division des services de gestion des affaires et de consultation
11 Laurier St. / 11, rue Laurier
10C1, Place du Portage
Gatineau, Québec K1A 0S5

Title - Sujet EDI/LVTS	
Solicitation No. - N° de l'invitation EN891-151443/A	**Amendment No. - N° modif.** 004
Client Reference No. - N° de référence du client 20151443	**Date** 2015-04-17
GETS Reference No. - N° de référence de SEAG PW-$$ZG-410-28660	
File No. - N° de dossier 410zg.EN891-151443	**CCC No./N° CCC - FMS No./N° VME**
Solicitation Closes - L'invitation prend fin **at - à 02:00 PM** **on - le 2015-05-04**	**Time Zone** **Fuseau horaire** Eastern Daylight Saving Time EDT
F.O.B. - F.A.B. **Plant-Usine:** ☐ **Destination:** ☑ **Other-Autre:** ☐	
Address Enquiries to: - Adresser toutes questions à: Gagnon, Jocelyne C.	**Buyer Id - Id de l'acheteur** 410zg
Telephone No. - N° de téléphone (819) 956-0575 ( )	**FAX No. - N° de FAX** (819) 956-2675
Destination - of Goods, Services, and Construction: **Destination - des biens, services et construction:**	

Instructions: See Herein

Instructions: Voir aux présentes

Delivery Required - Livraison exigée	**Delivery Offered - Livraison proposée**
Vendor/Firm Name and Address **Raison sociale et adresse du fournisseur/de l'entrepreneur** **Telephone No. - N° de téléphone** **Facsimile No. - N° de télécopieur**	
Name and title of person authorized to sign on behalf of Vendor/Firm (type or print) **Nom et titre de la personne autorisée à signer au nom du fournisseur/ de l'entrepreneur (taper ou écrire en caractères d'imprimerie)** **Signature**	**Date**

See below

Amendment 004 - RFP EN891-151443/A

This solicitation amendment 004 is raised to do a modification and respond to Bidder's questions for Proposal EN891-151443/A:

Modification

Under the Annex A, Statement of Work, Appendix A3 – EDI 3010 – 820 Layout

DELETE: page 43 – S1S Security Header Level 1

REPLACE BY:

Segment: S1S Security Header Level 1

Position: 009
Loop:
Level: Heading
Usage: Optional
Max Use: 1
Purpose: To initiate the beginning of a secured area and to provide the parameters needed for authentication or encryption of a functional group

Data Element Summary

Ref. Des.	Data Element	Name	Attributes
S1S01	**990**	**Security Type** 'AA'	**X ID 2/2**
S1S02	**824**	**Security Originator Name** 'GEDIS001'	**X AN 4/16**
S1S03	**825**	**Security Recipient Name** Unique designation (identity) of the cryptographic process that performs authentication or decryption on received data, or is the destination of a cryptographic service message Note: X9 has a minimum length of 4 characters for the security recipient; no mechanism, or registration method is provided by X9 or X12 to guarantee the uniqueness of the identifier	**X AN 4/16**
S1S04	**991**	**Authentication Key Name** Name of the key used for authentication. This name is mutually known to the security originator and the security recipient, is unique for this relationship, and allows a particular key to be specified.	**X AN 1/16**
S1S05	**992**	**Authentication Service Code** '1'	**X ID 1/1**
S1S06	**993**	**Encryption Key Name** Not Used	**X AN 1/16**
S1S07	**994**	**Encryption Service Code** Not Used	**X ID 1/3**
S1S08	**995**	**Length of Data (LOD)** Not Used	**X N 1/18**
S1S09	**996**	**Initialization Vector (IV)** Not Used	**X AN 16/16**

Questions

Question 1: Statement of work p.35 - 2.15.1 Redemption of EDI payments

a. The doc. refers to the rule G12 which is for Direct Deposit. Our assumption is that we have to use the same process for EDI payment.
b. Please confirm. We would need clarification on the settlement process for redeemed items.

Answer 1: EDI redemption amounts are claimed by manually submitting a Bank of Canada form 799 (section 2.15.1 of the Statement of Work). This amount is entered into the Bank of Canada system and included in the claims for settlement. Only the wording within Rule G12 regarding settlement by LVTS payment from the Bank of Canada applies to the EDI redemption claim process.

Question 2: Can Canada provide the following Manuals

a. CMP G1-009 "Transport and Transmittal of Protected and Classified Information",
b. G1-001 "Security Equipment Guide,
c. ITSG-06 "Clearing and Declassifying Electronic Data", ITSA-11E)

Answer 2: Under the attachment 1 to Annex C – Information Technology Security Requirement (ITSR)

Delete: ID number 10, IT Media

Replace by:

IT Media

i. The Contractor must follow instructions and guidance provided in Chapter 5 of the Industrial Security Manual (ISM) "Handling and Safeguarding of Classified and Protected Information". Please refer to Chapter 5 inserted below.

Question 3: Would it be possible to provide us with an EDI sample file containing a few transactions? We would like to test this file in our system and verify if we could accept this file as is or if we would have to make to some changes which would imply doing some development.

Answer 3:

```
ISA*00*          *00*          *12*GSCA   GSCA001 *01*TESTMAILBX
*150207*1330*U*00300*000000001*0*T*:
GS*RA*SPS001*TESTF*150207*1330*1*X*003010
ST*820*0001
BPS*ZZZ*0.01*X*04*123412345*2222222***04*123412345*1111111*150207
REF*TN*275555555555
REF*IT*TEST     GEDISAAC
DTM*097*110207
N1*PR*PWGSC
N1*PE*CANADIAN TEST PAYMENT
LS*0100
N1*SU*CANADIAN TEST PAYMENT
NTE*PMT*OUR REF: 0011:0000333333/2015
RMT*OI*NA0115*0.01
NTE*PMT*TEL  A. TESTGUY 613-222-2222
NTE*PMT*NA0115 EXPENDITURES TO DEC LESS HB ADVANCE FOR JAN
LE*0100
SE*15*0001
GE*1*1
IEA*1*000000001
```

Chapter 5 - Handling and Safeguarding of Classified and Protected Information and Assets

500. General

1. The Federal Government is responsible for stipulating and applying the required level of security for its information and assets. These levels are PROTECTED A, B, or C and CONFIDENTIAL, SECRET, TOP SECRET.

   When industry is awarded a contract which calls for safeguarding at any of these security levels, the Company Security Officer is to consult the responsible government department regarding the level of security to be applied for any in-house documentation created by industry in support of the contract. The industry originator of the documentation is then to ensure it is appropriately marked and safeguarded.

2. The improper handling and safeguarding of PROTECTED and CLASSIFIED information and assets is the leading cause of difficulties that result in the suspension or revocation of an organization's Designated Organization Screening or Facility Security Clearance. The application of the procedures, detailed throughout this chapter, will help to reduce the risk of a security infraction and/or breach.

3. Access to information and assets must be limited to persons who are appropriately reliability screened/security cleared and who have a need - to - know . Precautions must be taken to ensure that uncleared persons, who may be in the proximity of information and assets, do not gain access to this information and assets.

4. Particular attention should be paid to the requirements for control and registration of information and assets and to the proper procedures for their packaging and transmittal predicated on the Government Security Policy.

5. Additional requirements exist for the handling of COMSEC information and assets, over and above those safeguards outlined in this chapter (refer to the Industrial COMSEC Material Control Manual).

501. Security Warning for Contractor Produced Publications

1. Unless otherwise specified in the contract, where a contractor is producing a publication on behalf of the Government of Canada that contains PROTECTED information, the following warning will be printed on both the front cover and title page:

   This publication contains PROTECTED information which must be safeguarded under the provisions of Canada's Government Security Policy. It has been produced by (contractor's name) under the provisions of (contract number or other authorization) on behalf of (the Government of Canada or department), as applicable. Release of this publication, or of any information contained herein, to any person not authorized by the originating agency to receive it is prohibited.

2. All CLASSIFIED publications, pamphlets, handbooks or brochures which are produced by a contractor on behalf of the Government of Canada shall have, in addition to the regular security classification markings as prescribed in this chapter, the following security warning on both the front cover and the title page:

   This publication contains CLASSIFIED information affecting the national interest of Canada. It has been produced by (contractor's name) under the provisions of (contract number or other authorization) on behalf of (the Government of Canada or department, as applicable) and is to be safeguarded, handled and transported in accordance with Government Security Policy. Release of this publication, or of any CLASSIFIED information contained herein, to any person not authorized to receive it is prohibited by the Security of Information Act.

3. Where a contractor produces CLASSIFIED publications on behalf of a foreign government department or agency, any warning will be worded as stipulated in the contractual documentation. Further advice and assistance may be obtained by contacting IISD.

502. Marking Protected and Classified Information

1. **General**

   PROTECTED and CLASSIFIED information shall be marked, as a minimum, according to the standards detailed in this Manual.

2. **Marking**

   Organizations are required to implement the following procedures for marking informati on:

   a. for PROTECTED information, mark the word PROTECTED in the upper right corner of the face of the document and where required, with the letter A , B or C to indicate the level of safeguarding;

   b. for CONFIDENTIAL information, mark the classification in the upper right corner of the face of the document;

   c. for SECRET information, mark the classification in the upper right corner of each document page;

   d. for TOP SECRET information, mark the classification in the upper right corner of each document page and show the total number of pages on each page of the document (eg. page 2 of 10);

   e. mark covering or transmittal letters or forms or circulation slips to show the highest level of classification or protection of the attachments;

   f. mark all materials used in preparing PROTECTED and CLASSIFIED information. Such material includes notes, drafts, carbon copies and photocopies;

   g. the letters used in marking should be larger than those used in the text of the document;

   h. printed forms that only become PROTECTED and CLASSIFIED when completed should be so marked, eg.:

      CONFIDENTIAL

      (when completed)

   i. in addition to marking individual pages as stipulated above, documents shall be appropriately marked on the outside of both the front and back covers;

   j. **loose documents** shall be marked on every sheet;

   k. **charts, maps, drawings, etc** . shall be prominently marked near the margin or title block in such manner that the marking is clearly visible when the document is folded; and

   l. security markings should include the applicable protection/classification and the date or event at which declassification or downgrading is to occur, if it is possible to determine this at th e time the information is created or collected.

3. **Marking Copies** Organizations are required to implement the following procedures for controlling copies of CLASSIFIED information:

   a. control cop ies of CONFIDENTIAL documents as for SECRET when warranted by a threat and risk assessment;

b. for SECRET information, number each copy, show the copy number on the face of each copy, and maintain a distribution list; and

c. for TOP SECRET information, assign a unique whole number to each copy, marking the copy number on each page, and maintain a distribution list. Recipients of TOP SECRET info rmation will not copy it without the specific authorization of CISD.

4. **Marking Microforms**

   a. Microform is a generic term for any storage medium that contains micro-images.

   b. Organizations are required to implement the following procedures for the marking of microforms

      i. assign a protection or security classification commensurate with the highest protection or classification of the information contained on the microform;

      ii. mark microforms containing PROTECTED information PROTECTED in eye-readable form with the microform number and the total number of microforms; and

      iii. mark microforms containing CLASSIFIED information with the proper classification in eye-readable form with the microform number and the total number of microforms.

5. **Marking Electronic Storage Material**

   a. Electronic material on which is stored PROTECTED and CLASSIFIED information is to be assigned a protection and security classification commensurate with the highest protection or classification of the information it contains.

   b. Where possible, the security marking should be in both eye-readable and machine-readable form. Where this is not possible, as with certain types of hard disks, the security marking should be machine-readable.

   c. Electronic storage material includes flexible disks, hard disks (both removable and permanent), storage cartridges, printed output from computers, video display units, magnetic tapes, magnetic cassettes, punched cards and punched paper tapes.

   d. Removable storage material should bear standard labels. Where bypass label processing is allowed, procedures are needed to ensure that the proper item is loaded into the computer (refer to Chapter 8 of this manual).

   e. Specific advice on how to mark various forms of electronic storage material may be obtained from CISD.

6. **International Documentation** Marking shall be in accordance with international industrial security Memoranda of Understanding, Agreements or other international standards and guidelines. Advice and assistance may be obtained from IISD.

503. Records Management

1. **General**

   Organizations shall maintain records and establish adequate facilities such as a records office, for receiving, distributing and storing information and assets.

2. **Recording of PROTECTED Information and Assets**

   Unless specifically identified in a contract, there is no requirement to keep records of PROTECTED information and assets, except for PROTECTED C, which shall be recorded in the same manner as

CLASSIFIED information and assets. Persons receiving or granted access to PROTECTED information or assets shall be briefed on their responsibilities for its safeguarding.

3. **Recording of CLASSIFIED Information and Assets**

   a. A record shall be kept of the dates, names and transactions of all CLASSIFIED information and assets indicating:

      i. receipt by the facility;

      ii. distribution within the facility;

      iii. origination within the facility;

      iv. reproduction within the facility;

      v. destruction within the facility; and

      vi. transmittal outside the facility.

      Transmittal outside the facility will be as detailed in Article 505 of this chapter. Records of distribution, circulation and return within the facility shall include receipt by signature, of the persons involved. Persons who have access to CLASSIFIED information and assets shall be briefed on their responsibilities for its protection, and any special restrictions concerning its use or further dissemination.

      vii. All records of CLASSIFIED information and assets, and

      all CLASSIFIED information and assets, shall be made available for inspection by Field Industrial Security Officers of CISD.

4. **Records Office Security** Management of records offices, or parts thereof, where PROTECTED / CLASSIFIED information is stored or processed shall ensure the following procedures are followed:

   a. as a minimum, it will be managed as a Security Zone;

   b. records office staff who have access to PROTECTED / CLASSIFIED information will hold a Reliability Status or Personnel Security Clearance to the highest level required;

   c. PROTECTED and CLASSIFIED information will be filed and circulated in marked file jackets that clearly indicate they contain PROTECTED and CLASSIFIED information;

   d. a file shall be marked according to the highest level of sensitivity retained in the file;

   e. areas where mail is opened shall be managed according to mailroom security standards (refer to Article 503.5 in this chapter);

   f. release of PROTECTED files from records offices shall be limited to employees with Reliability Status with a need-to-know;

   g. release of CONFIDENTIAL files from records offices shall be limited to security-cleared employees with a need-to-know;

   h. release of TOP SECRET and SECRET files from records offices will be limited to appropriately security-cleared employees with a need-to-know. Those personnel authorized access are to be identified on an access list approved by the responsible manager (eg. project manager);

   i. CLASSIFIED information of foreign origin shall be accorded the same protection as Canadian information of equivalent classification, (if in doubt, consult IISD); and

   j. special precautions are necessary to prevent unauthorized disclosure or access to CLASSIFIED information and assets, to non-Canadian citizens. Such persons must not be given access to

information that bears restrictive markings such as, FOR CANADIAN EYES ONLY without prior approval of CISD. Further restrictions may apply to bilateral and/or multinational contracts, programs or projects (if in doubt, contact CISD).

5. **Mailroom Security** Areas where mail is opened shall be managed as a Security Zone, or High-Security Zone where required. Mail that is marked, to be opened only by the addressee will be delivered to the intended recipient directly. CLASSIFIED mail shall only be opened by the appointed authority within the facility responsible for ensuring its registration.

504. Safeguarding of Information and Assets

1. **Storage**

   a. As a minimum, PROTECTED information and assets shall be stored in a locked container. PROTECTED C information and assets and all CLASSIFIED information must be stored in an approved security container in accordance with the RCMP Technical Security Branch security equipment guide under G1-001. PROTECTED or CLASSIFIED information and assets may be stored on open shelving in a secure room, only after inspection and approval by CISD, and only to the level approved by CISD.

   b. PROTECTED and CLASSIFIED information and assets shall not be stored in the same container as negotiables or attractive assets.

   c. Organizations required to store PROTECTED and CLASSIFIED information and assets are permitted to purchase approved security equipment through Public Works and Government Services Canada. In consultation with the Field Industrial Security Officer, the Company Security Officer or Alternate Company Security Officer should determine the equipment to meet the specific requirement, and submit this request to the Field Industrial Security Officer using the form entitled "Registering Document for Equipment Purchase" at Annex 5-A in this chapter. After endorsement by the Field Industrial Security Officer, PWGSC will process the request, although the invoicing & delivery for the equipment is between the purchaser (company CSO) and the supplier. Examples of equipment available through this procedure are listed at Annex 5-B in this chapter.

2. **Keys for Containers**

   a. Keys (devices such as instruments, cards, combinations and code numbers used to open and close containers) shall be safeguarded, commensurate with the highest level of sensitivity of the information or assets to which they provide access. This also applies to recorded information that would allow a key to be produced.

   b. When a key is issued, the recipient must sign for the key. The number of the key, the location of the container it opens, and the name of the recipient shall be recorded and kept by the Company Security Officer.

   c. The organization's security office shall maintain a record of the dates of, and reasons for all key changes.

   d. Assigned keys should be changed:

      i. at least every twelve (12) months; and

      ii. when those with access to the container are transferred, released or no longer require access.

      iii. When a container has been or may have been compromised, the key must be changed immediately.

3. **Precautions During Use**

Special care must be taken to safeguard against disclosure or unauthorized access when PROTECTED and CLASSIFIED information and assets are removed from approved storage containers. Specific points to observe are:

a. do not leave PROTECTED and CLASSIFIED information and assets unattended; and

b. ensure that PROTECTED and CLASSIFIED information and assets cannot be viewed, or discussion of it overheard, by persons not possessing reliability screening or the appropriate level of clearance, or without a need-to-know .

505. Use of Laptop Computers

1. Should laptop computers be utilized for PROTECTED or CLASSIFIED information, the laptop computers **MUST NOT** be removed from the organization which holds the Facility Security Clearance or Designated Organization Screening. Should a need arise to transport such laptops, written permission must be obtained from the Company Security Officer or an Alternate Company Security Officer by way of a Courier Certificate (refer to Annex 5D, Appendix A-1 in this Chapter).

2. Storage of laptop computers, used to handle PROTECTED or CLASSIFIED information, must be in accordance with security procedures established by the organization for the level of sensitivity of the information.

506. Packaging and Transmittal of CLASSIFIED and PROTECTED Information and Assets

1. The security of PROTECTED and CLASSIFIED information and assets during transmission depends on:

   a. proper packaging;

   b. record while in transit;

   c. record of delivery; and

   d. transmission by an approved postal service or security-cleared courier (Contact IISD regarding approved postal services and security-cleared couriers).

2. PROTECTED and CLASSIFIED information and assets will be packaged and transmitted in accordance with the standards outlined at Annex 5-C in this chapter.

3. In addition, specific procedures for the hand carriage of and/or bulk shipment of specific PROTECTED and CLASSIFIED information and assets are necessary. These procedures are detailed at Annex 5-D (with appendices) and Annex 5-E (with appendices) in this chapter.

507. Temporary Removal of CLASSIFED and PROTECTED Information and Assets

1. PROTECTED and CLASSIFIED information and assets cannot be removed from a organization, for transportation or use outside of Canada, without the prior approval of CISD.

2. In Canada, with the exception of PROTECTED, PROTECTED C and COMSEC material, TOP SECRET, and CLASSIFIED information and assets may be taken temporarily from an organization. Written permission must be obtained from the Company Security Officer or an authorized Alternate Company Security Officer by way of a Courier Certificate (*) (refer to Annex 5-D, Appendix A-1 in this chapter).

3. The Company Security Officer/Alternate Company Security Officer will record, and obtain a receipt

for the information and assets to be removed.

4. If PROTECTED and CLASSIFIED information and asset removal is authorized for overnight use, the employee shall be informed that this does not constitute continued retention authority and the information and assets are to remain in the possession of the employee at all times.

5. The Company Security Officer/Alternate Company Security Officer must account for and record the material upon its return, and give the employee a receipt for the returned material.

508. Reproduction

1. Reproductions of PROTECTED information must be marked in the same manner as the originals. Reproduction of CLASSIFIED information shall only be done with the authorization of the Company Security Officer, or an authorized Alternate Company Security Officer. Reproductions must be marked, registered and accounted for, in the same manner as for the originals.

2. Some CLASSIFIED information bears a caveat prohibiting or restricting reproduction. In such cases, authorization of the originator is required before reproduction. PROTECTED C, TOP SECRET, and COMSEC information shall NEVER be reproduced without written authorization from CISD.

3. Special precautions must be taken with the use of photocopy machines. Notices concerning the proper procedures for reproduction of information shall be placed in an obvious place close to each machine. Care should be taken to ensure that original documents are not left in the machine, and all copies, including waste, are removed.

4. Contracts for printing and/or microfiching of PROTECTED and CLASSIFIED documents shall only be awarded to commercial firms that have the appropriate level of Designated Organization Screening or Facility Security Clearance.

509. Reclassification/Declassification

1. Documents whose classification markings include a schedule for downgrading or declassification may be downgraded or declassified in accordance with the schedule, unless in receipt of notification to the contrary. Documentation that does not contain such provisions may only be downgraded or declassified upon receipt of written authorization from the originator through CISD.

2. When an organization considers that CLASSIFIED information should be downgraded or declassified, a written request shall be submitted to IISD with full details, including justification.

3. When official notification is received from CISD authorizing reclassification of a document, all copies will be re-marked with the new classification as follows:

   (Declassified)
   or
   (Downgraded to..)
   or
   (Upgraded to..)

   (by authority of..)

   (PWGSC letter dated..)
   or
   (SRCL dated..)
   or
   (Contract dated..)

510. Retention

1. PROTECTED and CLASSIFIED material and assets shall, when a bid is not accepted, or upon

completion or termination of the contract, be returned to CISD for disposal or, with the written concurrence of CISD, be destroyed by the organization or returned to the originator. Upon request, organizations may be authorized to retain such material when approved by the originator through CISD.

2. Requests for retention authority shall identify the material for which retention is requested, the period for which retention will be required and the justification for retention. If the organization has been authorized to retain PROTECTED and CLASSIFIED information for a specific period after contract completion, details of this authorization must be included with the retention request.

3. Unless retention authority is received in writing, disposal of PROTECTED and CLASSIFIED information shall be made in accordance with the provisions of this manual and instructions from CISD.

511. Destruction

1. Unless otherwise specified, PROTECTED C, TOP SECRET, COMSEC and foreign CLASSIFIED information and assets must be returned to CISD for disposal.

2. Unless otherwise specified, PROTECTED A and B, SECRET and CONFIDENTIAL information and assets, of Canadian origin, may be destroyed by the organization with the approval of CISD.

   Note: Destruction of CLASSIFIED information and assets, will be recorded on a Certificate of Destruction Form, a copy of which shall be forwarded to the Document Control Unit, CISD.

3. PROTECTED and CLASSIFIED information and assets which have been authorized for destruction must be disposed of in accordance with the following:

   a. it must be destroyed only by approved destruction equipment, or at a facility authorized by CISD;

   b. information awaiting destruction or in transit to destruction must be safeguarded in the manner prescribed for the most highly PROTECTED and CLASSIFIED information asset involved;

   c. PROTECTED and CLASSIFIED information/assets awaiting destruction must be kept separate from other information/assets awaiting destruction;

   d. an employee with a Reliability Status, or with a proper security clearance, as applicable, must be present to monitor the destruction of PROTECTED and CLASSIFIED information respectively; and

   e. surplus copies, and waste that could reveal PROTECTED CLASSIFIED and information, must be protected to the appropriate level and should be promptly destroyed.

512. Security Violations, Breaches, and Compromises

1. Organizations shall establish a procedure to ensure that suspected or actual violations of security, breaches and compromises are recorded and immediately reported to the Company Security Officer. Records should be kept by the organization for a period of two years following the incident and are subject to inspection by the Field Industrial Security Officer.

2. Upon receipt of such a report, the Company Security Officer shall immediately conduct a preliminary inquiry into the incident to determine all of the circumstances, including:

   a. What, where and when did the incident occur?

   b. Who reported it, to whom, and when?

   c. What information or asset was involved (in detail)?

d. What was the security marking and description of the information or asset involved?

e. Who originated the information or asset?

f. When, for how long, and under what circumstances was the information or asset vulnerable to unauthorized disclosure, and to whom?

g. What actions were taken to secure the information or asset and limit the damage?

h. Is any information or asset lost or unaccounted for?

3. When the results of the preliminary inquiry indicate a suspected or actual breach or compromise of information and assets, CISD is to be immediately notified by the Company Security Officer. A full report covering the preliminary inquiry and any subsequent investigative results are to be forwarded to CISD as soon as possible.

513. Verbal and Message Communication

1. Unprotected telephones or facsimiles are not to be used to communicate CLASSIFIED or special information. Requirements for secure telephones/facsimiles must be coordinated through CISD/COMSEC.

2. Any conference rooms used for discussion of CLASSIFIED matters:

   a. should be a Sensitive Discussion Area, located in a Security Zone or High-Security Zone; and

   b. should be safeguarded against acoustic or electronic eavesdropping and should not contain items such as:

      i. telephones

      ii. intercoms

      iii. radios, and

      iv. tape recorders