MEMORANDUM OF UNDERSTANDING (MoU)

BETWEEN THE

COMMUNICATIONS SECURITY ESTABLISHMENT (CSE)

AND THE

CANADIAN FORCES (CF)

(each a Party and together, the Parties)

Computer Network Defence Service

PART I – INTRODUCTION

WHEREAS the Commander Canadian Forces Information Operations Group (CFIOG) on behalf of the CF has requested in writing that CSE provide Computer Network Defence (CND) service on the networks and systems of the CF and DND (the provision of the CND service will be accomplished through a partnership between the CF and CSE where CSE will be performing the activities specified in Part III of this MoU);

WHEREAS CSE, which is part of the Department of National Defence, has the legislative mandate, *inter alia*, to provide advice, guidance and services to help ensure the protection of electronic information and of information infrastructures of importance to the Government of Canada pursuant to paragraph 273.64(1)(b) of the *National Defence Act* (NDA) (CSE's "Mandate B");

WHEREAS DND is authorized by section 161 of the *Financial Administration Act* to take reasonable measures to manage or protect its computer systems;

WHEREAS DND has, pursuant to paragraph 8(2) (b) of the *Privacy Act*, the authority to disclose to CSE personal information it has under its control for any purpose in accordance with any Act of Parliament that authorizes its disclosure and hereby authorizes CSE to collect such information solely for the purposes mentioned in and under the conditions provided in this MoU; and

WHEREAS, when a Ministerial Authorization (MA) has been issued pursuant to subsection 273.65(3) of the *National Defence Act*, CSE has the authority to intercept private communications for the sole purpose of protecting the computer systems or networks of the Government of Canada from mischief, unauthorized use or interference.

PART II – CND TERMS AND CONDITIONS

Therefore, the Parties agree as follows:

1. Purpose

The purpose of this MoU is to set out the terms and conditions according to which CSE, in partnership with the CF, will provide CND network monitoring, related analysis, and mitigation advice to the CF. Over the period of this MoU, CSE and the CF will explore the feasibility of CSE transferring, in whole or in part, the CND network monitoring and related analysis services to the CF as per Part V of this MoU.

2. Definition of CND conducted under Ministerial Authorization

As part of the CSE CND service, CND activities conducted under an MA for the sole purpose of protecting computer systems or networks, provide advice, guidance and services to select Government of Canada (GC) institutions by detecting, analyzing, and/or mitigating sophisticated cyber threats. Where activities are conducted under an MA, CSE may use knowledge and tradecraft gained from assisting one Client for the protection of other GC systems or networks.

3. CND Management – Roles and Responsibilities

The terms "Manager, Technical Threat and Analysis", "Oversight Committee", "CSE Technical Team", and "CND Team" are used to distinguish the roles and responsibilities of individuals managing the CND service. This section describes these roles and responsibilities.

(1) CF

(a) The CF will provide management personnel to work on the Oversight Committee and will assist in fulfilling the terms and conditions of this MoU.

(b) Subject to CF's and CSE's operational requirements, the CF may provide CND analysts to work on the CND Team. When part of the CND Team, CF personnel and DND employees supporting CF Operations will operate under CSE's authorities, policies and procedures when conducting CND activities.

(c) The CF will provide technical personnel to support the installation, deployment and maintenance activities related to the CND service, subject to CF's operational requirements.

(d) The CF will provide all the necessary information required by CSE to set up and activate the CND service, ensuring that the CND Team conducts the service only on computer systems and networks for which the CF and DND are the owner or authorized user.

(e) The CF will provide ongoing support, during the CND activity, keeping the CND Team informed of any network changes which could affect the CND service.

(f) The CF will be responsible for ensuring all appropriate authorizations are obtained prior to the commencement of the CND service.

(g) In order to protect classified sources, methods or techniques, the CF will not take any action on the basis of CND reports, other than following mitigation advice provided in the report, without the permission of the Manager, Technical Threat and Analysis, or for COMINT reports, CSE Operational Policy. The CND Team will obtain the necessary approvals related to mitigation advice before including it in a CND report.

(h) The CF agrees to consider implementing all mitigation advice received from CSE resulting from the CND service.

(2) CSE

(a) CSE will provide management personnel to work on the Oversight Committee and will assist in fulfilling the terms and conditions of this MoU.

(b) Manager, Technical Threat and Analysis (CSE). The Manager, Technical Threat and Analysis will oversee all aspects of the CND activities performed by the CND Team, and ensure they are performed according to this MoU and CSE policies.

(c) CND Team. The CND team will perform network monitoring, related analysis, provide mitigation advice, and generate reporting (including alerts); specific reporting details to be determined.

(d) CSE Technical Team. The CSE Technical Team (which is part of the CND Team) deploys the CND system and ensures that the CND system is functioning as intended. The CSE Technical Team will maintain and monitor the CND system and adapt its architecture during the provision of the CND service based on CF and DND network changes or CND optimizations.

(3) Oversight Committee

(a) The Oversight Committee will consist of management representatives from the CF and CSE personnel involved in the coordination and management of the CND service as agreed by the Parties (see Part VI).

(b) The Oversight Committee is responsible for ensuring the CND service is conducted in accordance with the terms and conditions of this MoU. The Oversight Committee will provide direction and guidance to the Manager, Technical Threat and Analysis with respect to legal issues and information indicating criminal activity. In dealing with legal issues, the Oversight Committee will consult with CFIOG's Legal Advisor and CSE's Directorate of Legal Services (DLS), who will work together to resolve these issues.

4. Intellectual Property belonging to Third Parties

The CF represents and warrants that CSE, when using hardware, software or technical data present on the CF and DND networks and systems, for the provision of the CND service covered under this MoU, will not be in breach of any intellectual property belonging to third parties, including copyright, trademark, patents or trade secrets.

5. Control of Computer Systems and Networks

The CF confirms that the CF and DND are is the sole owners of the computer systems and networks that will be the subject of the CND service.

6. Fees and Expenses

Each Party will be responsible for its own fees and expenses during the conduct of the CND service. Other costs associated with the CND service covered under this MOU will be handled as follows:

(1) The CF will be responsible for costs associated with communications lines (set up and maintenance) and costs associated with CF and DND facilities needed.

(2) CSE will be responsible for costs associated with the equipment needed for the provision of the CND service, including replacing and upgrading equipment as needed.

7. External Review

(1) Pursuant to subsection 273.63(2) of the NDA, all CSE activities are subject to review by the CSE Commissioner to ensure that they are in compliance with the law. Pursuant to subsection 273.63(4) of the NDA, the CSE Commissioner has all the powers of a commissioner under Part II of the *Inquiries Act* and, therefore, has the power to access all information under CSE's control related to the conduct of CND activities, and *may* request information from the CF as part of such review of the CND service. The CF will cooperate fully with any such requests from the CSE Commissioner as it pertains to CSE's area of responsibility.

(2) Pursuant to the *Access to Information Act* and the *Privacy Act*, CSE is subject to review by the Information Commissioner and the Privacy Commissioner respectively to ensure that CSE is properly discharging its obligations under the above statutes. The Information Commissioner and the Privacy Commissioner have the authority to make whatever examinations and inquiries are necessary to enable them to carry out their statutory functions. Any such examination and inquiry may include a review of information related to the conduct of the CND service, and may require an interview with or documentation from the CF as part of such review of the CND service. The Parties will cooperate fully in responding to such requests from the Information Commissioner and the Privacy Commissioner as it pertains to CSE's area of responsibility.

(3) Pursuant to the *Auditor General Act*, CSE is subject to review by the Office of the Auditor General (OAG) to ensure that CSE is meeting its obligations under the *Financial Administration Act* and other relevant statutes. The Auditor General has authority to make whatever examinations and inquiries are necessary to report as required by the Act. Any such examination and inquiry may include a review of information related to the conduct of the CND service, and may require an interview with or documentation from the CF as part of such review of the CND service. The Parties will cooperate fully in responding to such requests from the Auditor General as it pertains to CSE's area of responsibility.

8. Classified and Protected Information

(1) CF and DND's Classified or Protected Information

(a) The CF will ensure that any classified or protected information provided to CSE pursuant to this MoU, including but not limited to software, technical reports, working papers and technical data, is clearly and appropriately marked as such.

(b) All information disclosed by the CF to CSE about the CF and DND networks and systems will be marked with the appropriate classification, or marked "Unclassified".

(c) CSE will appropriately store all such information and will hold and use such information in confidence, in accordance with CSE security standards. Access to the CF and DND's classified or protected information is limited to the CND Team, IT Security management, and others within CSE who require access to conduct or support the CND service covered under this MoU. Any further access within CSE must be authorized by Director, Threat and Vulnerability Analysis in consult with the CF. The Parties acknowledge that this non-disclosure undertaking is subject to the *Access to Information Act* and the *Privacy Act*.

(d) All information classified or protected by the CF will remain the property of the CF and will be handled in accordance with this MoU, the Government Security Policy, CSE policies, or specific instructions from the CF, at the option of the CF. At the conclusion of the CND service, or when no longer necessary, information classified or protected by the CF will be returned to the CF.

(2) CSE's Classified or Protected Information

(a) CSE will ensure that any classified or protected information provided to the CF pursuant to this MoU is clearly and appropriately marked as such.

(b) The CF will appropriately store all such information and will hold and use such information in confidence, in accordance with departmental security standards. Without the prior written consent of CSE, the CF shall not provide CSE's classified or protected information to anyone other than members of the Oversight Committee. The Parties acknowledge that this non-disclosure undertaking is subject to the *Access to Information Act* and the *Privacy Act*.

(3) MoU and CF or DND CND Data Obtained during the CND Service

(a) This MoU is SECRET.

(b) All CND data obtained from the CF and DND networks and systems and remaining under the control of the CF will be appropriately classified or protected at a minimum Protected B level.

(c) Access to CND data obtained from the CF and DND networks and systems, and other information obtained by CSE from or about the CF and DND networks and systems during the provision of the CND service covered under this MoU, is limited to the CND Team. The CF agrees that access by other persons within CSE may only be authorized by the Director, Threat and Vulnerability Analysis in consultation with the CF.

(d) All CND reports resulting from the provision of the CND service covered by this MoU will be classified as appropriate.

9. Personal Information and Information About Canadians

CSE will handle personal information under its control in accordance with the *Privacy Act*.

As required by paragraph 273.64(2)(b) of the NDA, CSE will also follow established policies to protect Information about Canadians (that is, any personal information about a Canadian, or any information about a Canadian corporation), as well as information that might identify GC employees.

10. Interception of Private Communications

It is understood that for CSE to provide the CND service covered under this MoU, which may involve the interception of private communications, CSE requires an MA from the Minister of National Defence, pursuant to subsection 273.65 (3) of the NDA. CSE will only intercept private communications for the sole purpose of protecting the Government of Canada's computer systems or networks from mischief, unauthorized use or interference. Pursuant to paragraph 273.65(4)(c) of the NDA, CSE has satisfactory measures in place to protect the privacy of Canadians.

11. Control of CND Data

(1) Even though CSE is providing the data repository (see paragraph 12), the data in the repository remains under CF Control. This control of CND data consists of the CF maintaining the ability to cease the CND service at any time and starting the CND data deletion process as per paragraph 13.

(2) CND data obtained by CSE from the CF and DND networks and systems during the provision of the CND service covered under this MoU remains under the control of the CF until it is identified as being:

(a) relevant to CSE's mandate as stated in the NDA, paragraph 273.64(1)(b), to use and retain for the purpose of providing advice, guidance and services to help ensure the protection of electronic information and of information infrastructures of importance to the Government of Canada,

and in the case of Private Communications,

(b) essential to use and retain for the purpose of identifying, isolating or prevent harm to GC computer systems or networks (as required by paragraph 273.65(4)(d) of the NDA),

at which point the CND data comes under the control of CSE.

(3) CSE may make use of information that is relevant to CSE's mandate, as stated in the NDA, paragraph 273.64(1)(b), and in the case of private communications, essential to identifying, isolating or preventing harm to Government of Canada computer systems or networks (as required by paragraph 273.65(4)(d) of the NDA):

(a) By sharing it with Government of Canada departments and agencies beyond the CF, DND, and/or with CSE's counterpart organizations in the United States, United Kingdom, Australia and New Zealand, and

(b) By supporting CSE IT Security initiatives to improve security architectures, to secure technologies and to advance sophisticated cyber-defence products and services.

12. Data Repository

(1) The provision of the CND service by the CND Team requires the use of a CND data repository to store a copy that may include all tapped CF and DND traffic. As part of the CND system architecture, CSE will employ and maintain a CSE controlled repository to store this data.

(2) CND data will be classified to the highest level of network traffic tapped (the same as paragraph 8 (3) (b). All CND data from the CND system shall be stored in a TOP SECRET//COMINT repository in a suitably accredited facility.

(3) Retention time of actual CF's CND data within the repository will vary based on operational need and on physical capacity. All CND data under CF's control will be stored for a maximum of [redacted] from the date it is copied (provided a Ministerial Authorization in place, and this MoU remains in effect). This does not include data which is under the control of CSE (see paragraph 11).

13. Controls Provided for Communications Link (s)

CND data that is still under CF's control can be deleted by the CF at any time. Such a request to delete CND data under CF's control can be made by contacting members of the Oversight Committee or terminating the flow of copied network traffic on the communications link (s) between the CF and CSE. CSE will react to such a termination by immediately stopping activity, blocking access to data under CF's control and seeking further guidance from the CF.

14. Termination of CF CND Service

Within [redacted] of the termination of this MoU (either at the expiry of this MoU, or earlier at the request of the CF (see paragraph 13), or at CSE's request), CSE will provide confirmation in writing that all of CF's CND data has been destroyed in accordance with CSE policy.

15. Support to the CND Activity

Subject to operational capacities, the Parties will provide the support necessary to carry out the CND service covered under this MoU.

16. Term of this MoU

(1) This MoU comes into effect on the day it is signed by the Parties and will remain in effect for a period of four (4) years from that date. This MoU will be reviewed annually, and any changes needed to this MoU as a result of partnership expansion will be completed and initialed by both parties. The term of this MoU may be extended or shortened with the written consent of the Parties.

(2) The Parties to this MoU acknowledge that if at any point during the term of this MoU there is a period of time where no applicable MA is in force, CSE will not carry out CND activities that may intercept private communications during that period.

17. Information Indicating Criminal Activity

If, in conducting CND activities, any member of a CND Team discovers information or evidence of activity that appears to be criminal (but not related to sophisticated cyber intrusion attempts):

(1) details concerning the discovery shall be strictly controlled and shared on a "need-to-know" basis; and

(2) the Manager, Technical Threat and Analysis will notify the Oversight Committee of the relevant findings.

The CF shall have sole discretion with respect to the follow-on action(s) and notification of the appropriate authorities.

18. Termination or Suspension of Services

Either Party may terminate or suspend the CND service at any time upon providing appropriate notice in accordance with paragraph 19 of this MoU.

19. Notice

(1) Any notice to either Party hereunder must be in writing and signed by the Party giving it. Notices shall be addressed as follows:

Director Threat and Vulnerability Analysis	Commander Canadian Forces Information Operations Group
Communications Security Establishment 719 Heron Road P.O. Box 9703 Terminal Ottawa, Ontario K1G 3Z4	Canadian Forces Station Leitrim 3545 Leitrim Rd Ottawa, Ontario K1A 0K4
Fax Number: [redacted]	Fax Number: (613) 945-3199

(2) Such notice may be delivered by hand, by regular mail, by courier or by facsimile. A notice shall be deemed to have been received on the day of its delivery if delivered by hand, on the fifth (5th) business day after mailing if sent by regular mail, on the date of delivery if sent by courier, and on the first business day after the date of transmission if sent by facsimile.

20. Modification

This MoU may be modified in writing at any time with the written consent of both Parties.

21. Survival

The sections of this MoU dealing with information about Canadians (as required by paragraph 273.64(2)(b) of the NDA), Classified and Protected Information, and Control of Data, shall survive the termination of this MoU.

22. Entire Agreement

This MoU constitutes the entire agreement between the Parties.

PART III - CND SERVICE

23. Details, including the monitoring points, will be agreed upon by the CF and CSE prior to starting the CND activity. The Parties agree that, as part of the CND service covered under this MoU, the following will be provided by CSE (subject to operational resources):

(1) Setup and activation, including, hardware and software setup and configuration;

(2) Installation and deployment of the CND data repository;

(3) Equipment shall be provided by CSE and returned to CSE upon MoU termination or ownership of the equipment transferred to the CF;

(4) Communication lines setup and configuration;

(5) Installation and deployment of a "cease activity" capability, to allow the CF to terminate the CND service immediately and remotely (in accordance with paragraph 14 of this MoU) by stopping the copying of data into the CND data repository; and

(6) Provision of the CND service will include:

(a) Incident Analysis – an investigation of alerts triggered by detection capabilities, in order to determine whether the alert is a real incident or a false positive,

(b) Forensic Intrusion Analysis – detailed investigation to understand the damage caused by a malicious network intrusion, and to identify additional systems or network components that may have been infected,

(c) Anomaly Analysis – the creation of statistical profiles of client network behaviour in order to recognize abnormal or suspicious network traffic that may indicate a malicious activity,

(d) Incident Reporting – the development and transmission of reports that provide detailed analysis of successful or attempted intrusions, as well as mitigation advice, and

(e) Advanced Tool Development – the creation of sophisticated non-commercial CND tools and detection capabilities through the use of knowledge gained from analysis of malicious network traffic. These sophisticated tools will improve detection of current and future threats.

PART IV – INCIDENT RESPONSE

24. Outside of this MoU, and beyond the scope of the MA, while conducting CND activity, potential cyber incidents may take place where CSE would need to conduct further analysis on the CF or DND's computer hardware and/or information contained therein.

25. The CF will contact CSE IT Security Client Relations Management if the CF suspects a cyber incident has occurred or CSE IT Security Client Relations Management will contact the CF if CSE suspects a potential cyber incident has occurred during the period covered by this MoU.

26. For each suspected cyber incident, CSE IT Security Client Relations Management will obtain (in the form of an email) from the CF authority signing this MoU (or their designate or delegate (see paragraph 28)):

(1) consent prior to initiating analysis;

(2) confirmation that the hardware or information to be analyzed belongs to the CF or DND (if not, the CF will provide the owner's identity);

(3) approval to share beyond the CF (subject to the provisions of the *Criminal Code* and *Financial Administration Act*) the:

(a) hardware, and/or

(b) information contained therein, and/or

(c) results of analysis; and

(4) the name(s) of the CF technical representative(s) who will be able to assist CSE personnel in the analysis.

27. This arrangement will remain in place for the length of this MoU unless it is rescinded prior to that date by the CF.

28. The CF authority signing this MoU delegates, by signing this MoU, any person occupying the position of Commanding Officer Canadian Forces Network Operations Centre (CO CFNOC) to make decisions on their behalf regarding any potential cyber incidents involving CF or DND's computer systems or networks.

PART V – PARTNERSHIP DEVELOPMENT

29. CSE / DND/CF Partnership

(1) Initially, CSE, in partnership with the CF, will provide CND network monitoring, related analysis, provide mitigation advice, and generate reporting under the authorities noted in PART I of this MoU by deploying and operating the CND system on specified portions of the CF and DND's networks.

(2) The CF may provide personnel to work on the CND Team. CF members will perform Detection, Analysis and Reporting work as part of the CND Team, will receive relevant training, and will operate under CSE authorities while part of the CND Team. This training and exposure to the CND Team will help to enable future partnership possibilities.

(3) A committee will be formed, which will include members of the Oversight Committee, in addition to other CF and CSE representatives, to explore the feasibility of and the protocol for transferring the conduct of the CND activity covered under this MoU from CSE to the CF. This committee will endeavour to address equity management and report release approval as well as any other oversight aspects to allow the CF to incrementally assume control over the CND activity.

(4) This partnership will be examined at least annually, with a view to possibly expanding CF's responsibilities in the CND activity incrementally, with the ultimate goal of transferring control of the CND service entirely to the CF after the expiry or termination of this MoU.

PART VI - MEMBERS OF THE CND OVERSIGHT COMMITTEE

CSE Members	(CF/DND) Members
Director, Threat and Vulnerability Analysis	Commander CF Information Operations Group
Manager, Technical Threat and Analysis	Director General Information Management Technology
Manager, Technical Analysis and Incident Response	Commanding Officer CF Network Operations Centre
	Officer Commanding A Sqn CF Network Operations Centre

For the COMMUNICATIONS SECURITY ESTABLISHMENT:

[redacted]

20 Feb 09

Date

Acting Deputy Chief
IT Security
Communications Security Establishment

For the DEPARTMENT OF NATIONAL DEFENCE:

19 Feb 09

Date

James R. Ferron
Brigadier General
Director General Information Management Operations
Department of National Defence