DND/CAF SECURITY GUIDE FOR TELEWORKING DURING THE COVID-19 RESPONSE

Using alternatives to DVPNI to communicate during our COVID-19 response will enable us to maximize our limited bandwidth and reserve DND/CAF network access for critical activities only. The practices below will ensure we maintain our crucial security while working remotely.

Public collaboration platforms for sharing unclassified information
Collaboration platforms on the Internet can help you share information and keep in contact with colleagues and clients. Here are some important security considerations before using these public cloud services to communicate from your personal devices:

1) Select a reputable service, such as:
    a. **Microsoft (Teams):** https://products.office.com/en-ca/microsoft-teams/group-chat-software
    b. **Apple (Facetime):** https://support.apple.com/en-ca/HT208176
    c. **Google (Hangouts):** https://gsuite.google.com
    d. **Slack:** https://slack.com

2) **Share only unclassified* information**: No sensitive information (Protected A, B, C or classified) is permitted.

3) **Respect privacy** of your teammates. Ask for their consent before creating accounts for others or inviting them using their personal email address.

4) **Be inclusive**: Some people may not have Internet access, have accessibility challenges, or have concerns using certain public cloud services. Find ways to ensure everyone can participate.

5) **Monitor**: Monitor your virtual community to ensure that no sensitive information is uploaded. Report security incidents to your local ISSO or USS.

6) **Preserve and transfer:** All information records of business value (IRBV) must be preserved and transferred to a DND/CAF information system as soon as practical.

Other ways to communicate
Call-tree: Every unit has a call-tree with personal contact information. It is the primary means of getting in touch with staff and employees. You can discuss up to Protected B on phone/cellphones systems in North America.

BBM Enterprise (BBME): Some DND users have access to BBME on their mobile devices. This application is approved up to Protected B when used with GC Enterprise accounts.

GCCollab: The Treasury Board Secretariat hosts GCCollab (https://gccollab.ca), which has a messenger application, forum and WIKI. It is approved up to Protected A.

Other: Other options are being developed with improved security and should be communicated soon.

What is Unclassified Information?

Unclassified information is information that is not injurious to the national interest, or an individual, organization or government. The National Defence Security Orders Chapter 6 explains how to categorize information. The following are examples of Protected and sensitive information, which is **not** permitted on public cloud services:

- Third-party business information provided in confidence (Access to Information Act – s.20);
- Unclassified information provided in confidence from another government or international organization (Access to Information Act – s.13 and s.15);
- Defence and Security Information, such as operating instructions for Controlled Goods (Defence Production Act), Unpublished Defence Research Intellectual Property (Access to Information Act – s.18), or Defence Systems vulnerabilities (Access to Information Act – s.16) (see Defence Production Act and Access to Information Act exemptions);
- An individual's private information without their consent: date of birth, race, national or ethnic origin, colour, religion, age, marital status, academics/test scores, medical or financial information, as examples;
- Any identifying number (including PRI or Service Number [SN]), symbol, or other assigned particular, address, fingerprints, or blood type;

For further details, refer to:

- https://laws-lois.justice.gc.ca/PDF/A-1.pdf
- https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=13784

In general, remember that free services are monetized through access to user content. Information shared on these platforms is considered in the public domain. Reputable service providers have some level of protection when compliant with regulations such as General Data Protection Regulation (GDPR), or when hosted in Canada/US and governed by similar privacy laws.

Using DND equipment at home

You must be diligent in the care of your DND equipment. Laptops and mobile phones should be stored securely, out of sight. Your PKI card should also be kept secure, as it is both a sensitive security item and essential to connecting with DVPNI.

Stay cyber safe

Currently, cyber criminals are leveraging pandemic themes in phishing emails and malicious sites. For example, a known scam entices users to visit a fake COVID-19 heat map, infecting vulnerable computers. Stay alert:

- Avoid clicking on links in unsolicited emails or text messages and be wary of attachments;
- Use trusted sources, such as legitimate government websites, for up-to-date, fact-based information; and
- Do not reveal personal or financial information in email and do not respond to email solicitations for this information.

Visit the Get Cyber Safe site for more information and tips.

This message is being sent on behalf of Colonel A.M. Banville, Commandant of Canadian Forces Support Unit (Ottawa), to all recipients in the National Capital Region (NCR). Please do not reply as this mailbox is not monitored.