Office of the Chief Information Officer Directive: IT 10.05	Published: 04/2019
Chapter: Network Security	Last Review: 01/2024
Subject: **Network Intrusion Detection**	

1 DIRECTIVE

1.01 There will be a regular process in place to monitor GNB networks for unauthorized access attempts. Monitoring will be done using industry-best hardware and software that logs attempts to breach the network and analyzes network access logs and connection patterns to identify and log possible breaches for further investigation.

2 PURPOSE

2.01 The purpose of this Directive is to increase the level of security by proactively searching for signs of unauthorized network intrusions.

3 SCOPE

3.01 This directive applies to all GNB (Parts I – IV) host systems, servers, and network-connected GNB provided computing devices.

4 RESPONSIBILITY

4.01 The Cyber Security team in Treasury Board works collaboratively with the service provider's IT Security and IT Support teams. Together these teams are responsible to evaluate and implement hardware and software network intrusion detection tools.

4.02 IT Operations is responsible:

(a) To monitor systems and networks for signs of both failed attempts and successful intrusions.

(b) To track and maintain all evidence of intrusion attempts.

(c) To report security incidents of network intrusions to **[IT Security]**.

(d) To take immediate action to minimize damage from successful intrusions.

4.03 Chief Information Security Officer (CISO) and IT Technical Support are responsible to act on detected or reported intrusion attempts and recommend changes to prevent recurrence.

5 DEFINITIONS

5.01 **"TCP"** (**Transmission Control Protocol**) is a communication protocol that forms the part of TCP/IP used to send data in the form of individual data units or packets over the Internet. TCP is responsible for creating the set of packets, tracking the

packets and ensuring that all packets arrive safely and are assembled in the correct sequence at their destination.

5.02 **"UDP"** (**User Datagram Protocol**) is a less-reliable protocol than TCP that (like TCP) runs on top of IP networks. It provides very few error recovery services but offers a direct way to send and receive data over an IP network. While TCP is used for data that must arrive in perfect condition, UDP just sends out data packets for which there is no time to resend dropped or erroneous packets in real time. It is used primarily for broadcasting data over a network for streaming media, VoIP, and videoconferencing.

6 RELATED DIRECTIVE

OCIO IT 10.01 – Network Hardware Connection

OCIO IT 10.03 – Remote Access

OCIO IT 10.04 – Wireless Network

OCIO IT Chapter 13 – User Responsibilities