Proposal: Microsoft Teams Security Hardening

For Leonardo DRS Canada

Prepared by Cloudstrucc Inc.

🛍️ Executive Summary

Leonardo DRS Canada, a leading defence contractor and critical service provider for the naval electronics segment, operates under the stringent requirements of the **Controlled Goods Program (CGP)** governed by **Public Services and Procurement Canada (PSPC)**, as well as other government and international compliance frameworks.

To continue delivering secure, compliant, and mission-critical capabilities, Leonardo DRS must ensure its internal collaboration platforms align with:

- Government of Canada cybersecurity standards (e.g., **ITSG-33**, **ITSG-22**)
- International frameworks such as **ISO/IEC 27001**, **NIST 800-171**
- **Controlled Unclassified Information (CUI)** guidelines
- Defense Industrial Base Cybersecurity Program (DIB CS)
- **NATO Security Standards** for classified and restricted information

This proposal outlines how Cloudstrucc will implement a **Microsoft Teams security hardening initiative** that transforms Teams into a **fully end-to-end encrypted, CGP-, NIST-, and NATO-aligned collaboration environment**. This includes integration of multi-factor authentication, advanced threat protection, data loss prevention, customer-managed encryption keys, and **network isolation using Azure Private Endpoints and Microsoft Teams service tags**.

These enhancements prevent data from traversing the public internet and allow for strict control over Microsoft 365 traffic by restricting access to approved IPs and virtual networks — a critical control mechanism for defence sector compliance.

The end state will position Leonardo DRS Canada with a secure, modern, and scalable Teams collaboration platform — aligned with its goals of standardizing digital communication while ensuring end-to-end compliance with both national and international security regulations.

🔐 Scope of Work (Updated)

- ✅ Enable secure OneDrive for Business integration, with sync from file system
- ✅ Apply Microsoft Purview policies to OneDrive (DLP, auto-labeling, encryption)
- ✅ Configure Conditional Access and session control for OneDrive access
- ✅ Restrict OneDrive access to managed devices via compliant endpoints
- ✅ Enforce MFA for guest/external access (Entra ID)
- ✅ Prevent meeting link forwarding abuse
- ✅ Configure Sensitivity Labels, DLP, and Information Barriers
- ✅ Integrate Customer Key (CMK) and private DNS endpoints
- ✅ Enable Safe Links/Attachments in Teams
- ✅ Configure Azure Private Endpoints with Microsoft 365 service tags
- ✅ Isolate Teams traffic from the public internet
- ✅ Implement Purview audit and retention policies
- ✅ Setup Defender for O365 & XDR dashboards
- ✅ Deliver internal documentation and run KT sessions
- ✅ 60-day support period + optional support extension

▯ Duration and Phasing

Project Duration: 30 to 60 Calendar Days

Phase	Duration	Milestone	Outcome
Phase 1	Week 1	Kickoff & Assessment	Identify gaps and current posture
Phase 2	Weeks 2–3	MFA + Meeting Policy Hardening	Guest MFA, Meeting Access Restrictions live

Phase	Duration	Milestone	Outcome
Phase 3	Weeks 3–4	Security Layering (CMK, DLP, Labels)	Policies and encryption applied
Phase 4	Weeks 5–6	Audit, Testing, and Training	Audit setup, team trained, docs delivered
Final	Day 60	Handover & Review	All systems in place, support begins

💸 Implementation Cost Estimate (CAD)

*Starting from the week of **July 7, 2025**, estimated due dates are projected based on a 60-day delivery schedule.*

Item	Description	Estimated Cost (CAD)	Estimated Due Date
Discovery & Assessment	Initial audit, kickoff, stakeholder alignment	$4,500	July 11, 2025
Conditional Access & MFA Setup	Configure policies, guest restrictions	$5,500	July 18, 2025
Meeting & Collaboration Hardening	Meeting options, lobby, link lockdown	$5,000	July 25, 2025
DLP, Sensitivity Labels, IBs	Purview config, segmenting, rollout	$6,500	August 2, 2025
CMK & Private Endpoint Support	Azure setup, encryption config	$7,000	August 9, 2025
Audit, Defender XDR Integration	Logging, detection, incident setup	$4,000	August 16, 2025
Documentation & Knowledge Transfer	Wiki + live walkthroughs / training	$3,500	August 23, 2025
Support (60 days)	Response, tuning, questions	$2,500	September 6, 2025

Item	Description	Estimated Cost (CAD)	Estimated Due Date
Subtotal		**$38,500 CAD**	
HST (13%)		**$5,005 CAD**	
Total with HST		**$43,505 CAD**	

> *Optional extension at $125/hr support block (min. 10 hrs)*

📦 Licensing Requirements (CAD Pricing)

To implement the described security hardening, Leonardo DRS Canada will require the following licensing tiers:

Microsoft 365 Licensing (CAD)

License Tier	Features Required	Estimated Monthly Cost (CAD/user)
Microsoft 365 E5	DLP, Sensitivity Labels, Defender, CMK support	~$57
Microsoft Teams Premium	Advanced meeting protection, watermarking, lobby control	~$12

Notes

- E5 licensing is required for full Purview and Defender integration.
- Teams Premium enables advanced meeting security such as watermarking, lobby isolation, and end-to-end encryption policy enforcement.
- Minimum quantity and enterprise agreements may affect pricing.

📄 Appendices

Appendix C: OneDrive Security Hardening Overview

- Apply Microsoft Purview DLP rules and auto-classification labels to OneDrive
- Enforce compliance-based access controls (only compliant devices)
- Enable OneDrive sync policy for work files from corporate desktops/laptops only
- Restrict download/sharing from untrusted sessions using Defender & Purview
- Enable logging and retention policies for OneDrive access and edits

Appendix A: Detailed Microsoft Teams Security Checklist

- MFA enforcement for guests/internal staff
- Meeting policies & Teams Premium configurations
- Teams DLP and sensitivity label mappings
- CMK encryption and key rotation policy
- Azure Private Endpoint and DNS integration
- Use of Microsoft 365 Service Tags for Teams isolation
- Compliance test criteria (CGP/NIST/ITSG/NATO)

Appendix D: Compliance References (Expanded)

- Government of Canada ITSG-33 / ITSG-22
- Controlled Goods Program (CGP)
- ISO/IEC 27001
- NIST 800-171 / CUI
- NATO Restricted Information Protection Standards
- Microsoft Compliance Center (Purview)

CLOUDSTRUCC INC.