Training Workshop – 13 October 2026

Cyber Security & Digital Radio – Protecting Mission-Critical Communications

Format: Technical Workshop
Duration: 3 Hours
Audience: Critical communications professionals, radio system managers, engineers, technicians, system integrators, ICT/OT specialists, cybersecurity personnel, public safety communications staff and operational communications managers.

Workshop Objectives

Participants should leave the workshop with an understanding of:

- Cyber threats affecting mission-critical communications.
- The attack surface created by IP-connected radio systems.
- Cybersecurity considerations for P25, DMR and TETRA networks.
- Risks associated with Radio over IP, dispatch systems and remote access.
- Network segmentation between corporate IT and communications infrastructure.
- Identity, authentication and privileged access.
- Patching and vulnerability management in high-availability environments.
- Monitoring and detecting suspicious activity.
- Backup, redundancy and disaster recovery.
- Cyber incident response for operational communications.
- Secure-by-design principles for new or upgraded systems.

Workshop Outline

1. Cyber Security and the Modern Radio Network

An introduction to how mission-critical radio networks have evolved from relatively isolated systems into interconnected digital environments. This section will examine the importance of confidentiality, integrity and availability, with particular emphasis on the operational importance of system availability and resilience.

2. Understanding the Digital Radio Attack Surface

Explore cyber risks associated with:

- P25, DMR and TETRA networks air interfaces.
- Subscriber radios and programming systems.
- Repeaters, base stations and radio controllers.
- IP backhaul and network infrastructure.
- Radio over IP gateways.
- Network core infrastructure.
- Dispatch and Control Room
- Remote management and maintenance.
- Third-party connections covering connections to CAD, foreign radio networks

3. Dispatch and Control Room Security

Examine the risks created where radio systems connect with dispatch consoles, Windows servers, voice recording, GIS, telephony, corporate networks and other operational platforms. Topics will include user accounts, administrator access, passwords, patching and remote support.

4. Building a Secure Communications Environment

Practical approaches to improving security, including:

- Network segmentation and backhaul encryption.
- Firewalls and security boundaries.
- Single Sign-on, RBAC and Multi-factor authentication.
- Least-privilege access.
- Secure vendor and technician access.
- VPNs and controlled remote management.
- Secure protocols (E.g. TLS, SSH)
- Vulnerability Management, Logging, Auditing and Monitoring

- Radio Air Interface - Radio authentication, end-to-end encryption
- Demo

5. Australian and cybersecurity frameworks

Discuss Australian cyber frameworks and compliance requirements. Review NIST Cybersecurity framework and its application to Radio Systems.

6. Cyber Incident Scenario

Participants will work through a practical scenario involving radio-site outages, dispatch disruption, unusual network activity and potentially compromised remote access. The discussion will consider system isolation, maintaining communications, incident management and recovery. This will then be mapped to the NIST Incident Response Framework and IR Plan.

7. Key Takeaways

The workshop will conclude around three principles:

KNOW your System, frameworks and compliance requirements
PROTECT your infrastructure and data to be cyber resilient
PREPARE and be **Ready** for system failure or cyber incidents

The overall objective is to ensure mission-critical communications remain **secure, resilient, trusted and available when they are needed most**.