ERICSSON

Checklist: Deploying 5G and security for public safety agencies

For agencies concerned with ROI, conducting open conversations with all stakeholders, including line-level IT staff, will make the difference in creating operational efficiencies and streamlining digital transformation.

Best practices

Treat network security as a foundational consideration from the inception of the planning process, not as an afterthought.

Define your project and parameters with input from your buying team. Agencies that assemble a cross-functional buying team benefit from increased alignment and greater likelihood of successfully adopting new technology.

Do not try to implement applications using only in-house resources and IT generalists. Work with one or more trusted partners/vendors with specific expertise to drive initiatives forward effectively.

Legacy network infrastructure often requires manual, error-prone, and time-intensive network segmentation and policy orchestration. Consider whether it can really meet your technology needs. Clarify what you're trying to achieve and make sure the solution aligns to that.

Those driving adoption of new technology are IT leaders: managers, directors, and above. Non-IT leaders such as chiefs, deputy chiefs, sheriffs, etc. also play a role in driving new technology adoption, followed by line-level IT staff and officers.

ROI questions to consider

- ☐ What is the objective for implementing this technology initiative? (Mission-critical communications? Officer safety?)
- ☐ Exactly what metrics and benchmarks must the system deliver in order to be considered a success?
- ☐ Can the network support the increased traffic and computing that will occur as in-vehicle and IoT devices are added?
- ☐ Can the network guarantee the needed uptime with current infrastructure? If not, how will the company go about augmenting the network?
- ☐ Do you plan to deploy new applications on the agency network?
- ☐ If so, what are the network security strategies that need to be documented and implemented? If not, will a parallel network or a software application be implemented?
- ☐ How important is network uptime to the system's proper functioning and usefulness?
- ☐ How will the IT team manage and control in-vehicle and IoT devices, including hardware and software refreshes?
- ☐ Does the company have the resources to send IT staff on-site to do so?
- ☐ How much time and resources will be required to provision network access for these devices?
- ☐ Will the system ever scale? If so, can the network scale as quickly as needed?
- ☐ Are necessary partnerships and processes in place between the IT team and other stakeholder groups, such as operations?
- ☐ Who will lead the project? Do they have the right expertise?
- ☐ What outside expertise could benefit this project?
- ☐ To what degree will added connected devices increase the network's potential attack surface?
- ☐ How will the organization scale security efforts to match this growth?
- ☐ Does the organization currently employ a prevention focused security strategy?
- ☐ Should prevention efforts fail, how will the organization detect a security incident or breach?
- ☐ How might investment in a multi-layered security strategy impact this project?
- ☐ What is the worst-case security scenario associated with this project? How likely is that scenario? How would the company eliminate the possibility of such an outcome, and what investment would be required to do so?

Quick check: Do you have a complete solution in place to ensure constant connectivity and secure communications at the station and in the field?

Data security: **Protect against data and network breaches**	**Need to address**	**Have in place**
Isolate mission-critical information and data from other traffic		
Only allow agency-specific applications		
Whitelist websites that staff and officers can visit		
Run IDS/IPS technologies to minimize attack points		

Site-to-site transmission protection: **Provide safe network communication**	**Need to address**	**Have in place**
Air-gap or physically segment to destination where possible		
Implement network failover for maximum uptime		
Encrypt all data transmissions		

Network management: **Empower lean IT staff to spin up, spin down, and manage networks**	**Need to address**	**Have in place**
Use a centralized cloud network management tool		
Deploy zero-touch on-site routers		
Use configuration groups where possible		
Employ remote troubleshooting and test before crisis strikes		
Whitelist critical devices in vehicles where carrier coverage is thin		