17 April 2026

Rt Hon Christopher Luxon
Minister for National Security and Intelligence
Department of the Prime Minister and Cabinet
Parliament Buildings
Wellington 6160

Emailed to: criticalinfrastructure@dpmc.govt.nz

Dear Prime Minister

The Manawatū District Council thanks the Minister for National Security and Intelligence for the opportunity to provide feedback on the discussion document titled "Enhancing the cyber security of New Zealand's Critical Infrastructure System."

MDC considers that drinking water and wastewater services are among the most critical infrastructure services, given their direct impact on public health, environmental protection, and the functioning of communities and local economies.

MDC generally supports the intent of the proposed measures to improve cyber resilience across critical infrastructure. However, MDC considers that their effectiveness will depend on being implemented in a risk-based and proportionate manner, with clear guidance, alignment to existing frameworks, and recognition of the capacity constraints facing smaller councils.

Introduction

MDC's critical infrastructure consists of extensive roading and three waters networks, which underpin essential service delivery across a largely rural district. The Council is responsible for approximately 1,368 kilometres of roads (including both sealed and unsealed), supported by associated assets such as bridges, culverts, and footpaths. Its water supply network extends over 326 kilometres of mains and includes multiple treatment plants, while wastewater services are delivered through a district-wide network of pipes and treatment facilities servicing key settlements. MDC is progressing a significant wastewater centralisation programme, which will consolidate treatment across the district into fewer, more efficient facilities, increasing reliance on interconnected digital and operational systems.

MDC's infrastructure also supports regionally significant users, including RNZAF Base Ohakea, which relies on Council for water supply and discharges wastewater into the

centralised network, meaning disruption could have consequences beyond the district's resident population. These factors demonstrate that the scale of impact and level of risk associated with MDC's infrastructure are not adequately reflected by connection numbers alone, particularly where services are increasingly centralised and support critical regional assets.

MDC's critical infrastructure serves a population of approximately 34,000 residents (as at 30 June 2025). Approximately 52% of the population resides in Feilding, with the remaining 48% of the population living rurally or in our rural villages. MDC has elected to retain delivery of drinking water, wastewater, and stormwater services in-house as a dedicated water services business unit, reinforcing local control but also concentrating operational and cyber risk within Council-managed systems. Collectively, these roading and water services assets are fundamental to community outcomes, economic activity, and public health, and their scale, interdependence, concentration, and increasing digital integration highlight the importance of a risk-based approach to cyber security protections to ensure service continuity and resilience.

MDC notes the development of Te Utanganui inland port near the district boundary. While this infrastructure may be regionally significant, MDC's expectation is that cyber security responsibilities for such assets would appropriately sit with national operators (such as KiwiRail), rather than with territorial authorities.

Parts of Council infrastructure that could be affected by a cyber attack

MDC's water and wastewater infrastructure relies on a range of interconnected operational and information systems to monitor, control, and maintain essential services. These systems are increasingly digitally enabled and remotely accessed, which improves efficiency but also expands the potential cyber attack surface. The most critical and vulnerable components are operational technology systems, particularly telemetry and control systems that directly manage the delivery and treatment of water and wastewater.

The following systems are understood to be within scope of potential cyber impact:

- **Operational control systems**, including SCADA, telemetry, PLCs, and other remote monitoring and control technologies
- **Water infrastructure controls**, including treatment plant systems, reservoir controls, and pump station operations
- **Wastewater infrastructure controls**, including treatment plants and pump stations
- **Communications and access pathways**, including networks and remote access used by staff, contractors, and service providers
- **Supporting systems**, such as asset management, GIS, maintenance, outage, and incident response platforms that enable service continuity

- **Backup and recovery systems**, which are critical for restoring services following a disruption

Of these, telemetry and operational control systems represent the most direct pathway for service disruption if compromised. Other systems, such as corporate or administrative platforms, are generally of secondary relevance unless they are required to support incident response, customer communication, or service restoration.

While MDC has not undertaken a detailed technical assessment in this context, common vulnerabilities for local government infrastructure of this nature are well understood. These typically include:

- **Legacy systems**, particularly older telemetry or SCADA components that may not support modern security controls
- **Remote access risks**, including access by operators, vendors, or third-party support providers
- **Constraints on patching and updates**, particularly for operational technology where uptime requirements limit maintenance windows
- **Single points of failure**, especially within communications networks or centralised systems
- **Reliance on third parties**, including for hosting, monitoring, maintenance, or system support
- **Gaps in asset visibility**, including incomplete records of critical systems and their interdependencies
- **Unproven recovery capability**, where backup, recovery, and restoration processes have not been fully tested under realistic conditions

Addressing these risks requires a layered and proportionate approach to cyber security. Key areas for strengthening resilience include access controls (such as multi-factor authentication and privileged access management), network separation between IT and operational systems, improved monitoring and logging, robust patching practices where feasible, secure and tested backup arrangements (including offline or immutable backups), incident response planning and regular testing, and stronger assurance of third-party providers through contractual and operational controls.

MDC considers that the depth of cyber security controls should be proportionate to the consequence of failure, with higher expectations applied to systems that are centralised, lack redundancy, or present significant public health or environmental risk.

Thresholds for Critical Infrastructure

MDC's drinking water and wastewater networks do not meet the proposed threshold of at least 25,000 connections. However, this threshold does not adequately reflect the importance of networks that serve concentrated urban communities such as Feilding, where a service outage could have significant public health, environmental, and

community impacts. As wastewater services become increasingly centralised in Feilding, the consequences of a cyber security failure are amplified, with the potential to disrupt services across multiple communities.

MDC considers that consequence of failure, rather than network size alone, is a more appropriate basis for defining critical infrastructure. A simple national threshold based solely on connection numbers risks excluding infrastructure that is regionally significant, highly centralised, or associated with high-consequence failure. This includes infrastructure that, while smaller in scale, plays a critical role in maintaining essential services and supporting economic activity.

MDC's infrastructure also supports regionally significant users whose importance is not captured by a connection-based threshold. RNZAF Base Ohakea, for example, relies on Council for water supply and discharges wastewater into the Sanson Centralisation Line, which ultimately conveys flows to the Manawatū Wastewater Treatment Plant. Disruption to these services could therefore have impacts beyond the district's residential population, reinforcing the need for a broader, consequence-based assessment of criticality. On this basis, MDC considers that it may fall outside the proposed thresholds while still representing infrastructure with significant regional and national consequence risk.

MDC acknowledges that its infrastructure may be of greater significance than a simple connection-based threshold would suggest. However, MDC is concerned that classification as critical infrastructure could introduce significant cost, capability, and compliance requirements that may be disproportionate to the scale and resourcing of a rural territorial authority.

The proposal would benefit from greater clarity on how it intends to account for factors such as concentration risk, reliance on single treatment or conveyance systems, lack of redundancy, and the potential public health and environmental consequences of service failure.

MDC considers that recognising infrastructure as critical does not necessarily mean that all associated cyber security obligations should be placed at the level of individual councils, particularly where capability and control sit more appropriately with national or system-level providers.

Decisions sought:

1. That rather than relying solely on a connection threshold, that the definition of critical infrastructure be replaced with a risk-based framework that considers factors such as service criticality, degree of centralisation, interdependencies, consequence of failure, and the presence (or absence) of redundancy.
2. That where smaller councils are captured within a risk-based definition of critical infrastructure, implementation requirements are scaled appropriately and supported to ensure compliance is achievable without disproportionate cost or capability uplift.

Information Sharing and Reporting

MDC supports improved information sharing and situational awareness across the critical infrastructure system. Should local authority networks such as water supply and wastewater networks be classified as critical (such as under a risk-based approach), this will have implications for how councils manage cyber risk, and is likely to introduce additional reporting requirements, including for third-party service providers. To support practical implementation, MDC recommends:

- Alignment with and use of existing regulatory and reporting frameworks, to avoid duplication and unnecessary compliance burden
- Clear guidance and expectations for territorial authorities, particularly where infrastructure is regionally significant but below national thresholds
- A phased implementation approach, allowing councils time to assess gaps, prioritise investment, and build capability
- Clarity on the role of third-party providers, including shared responsibilities
- A proportionate approach to compliance, reflecting the scale, resources, and risk profile of smaller councils

This would help ensure that any new requirements improve cyber resilience outcomes without imposing disproportionate costs or duplicative obligations on local government.

MDC notes the proposed requirements for reporting cyber incidents, including the expectation to provide early notification within 24 hours and a full report within 72 hours. While MDC supports timely reporting, the ability for smaller councils to meet these timeframes will depend on the scope and level of detail required, particularly where incidents involve third-party systems or where information is still being verified.

MDC seeks clarity on the expected standards and processes for handling sensitive cyber incident information, including secure transmission methods and confidentiality requirements to ensure consistent practice across the sector. It is important that reporting mechanisms provide assurance that sensitive information will be protected to minimise security risks and avoid unintended reputational impacts, particularly where incidents are still being assessed or managed.

To support effective implementation, MDC considers that clear, nationally consistent guidance and assessment frameworks would be beneficial. This could include a decision-making matrix to assist councils in determining the significance of incidents and whether reporting thresholds have been met, similar to existing tools used for assessing notifiable privacy breaches. Such tools would support more consistent and efficient reporting without requiring significant additional capability at the local level.

MDC also notes that the extent of reporting and compliance requirements, including system capability and assurance expectations, may create additional cost pressures for councils. It is therefore important that the framework is designed to ensure equitable and consistent application across the sector, supported by clear benchmarks or maturity

expectations to avoid variability or unintended double standards between organisations of different scale and capability.

Decisions sought:

1. That implementation of cyber security requirements is proportionate to risk and council capability, avoids duplication with existing regulatory frameworks, and is supported by clear guidance, consistent benchmarks, and phased timeframes to manage cost and resourcing impacts.
2. That incident reporting requirements are supported by clear guidance, confidentiality protections, and standardised assessment frameworks, to enable consistent and practical implementation without imposing unnecessary additional costs on councils.

Capability, cost, and allocation of responsibility

MDC considers that the proposed framework, as currently framed, appears to be oriented toward larger, nationally significant infrastructure providers and may not adequately reflect the scale, capability, and resourcing constraints of rural and provincial councils.

For councils such as MDC, implementing and maintaining the level of cyber security capability implied by the proposed measures would require significant investment in specialist skills, systems, and ongoing operational support. Given the current level of organisational maturity across the local government sector, achieving and sustaining compliance would likely involve material and ongoing cost increases, which would ultimately be borne by ratepayers.

MDC also considers that the proposed approach places a significant portion of responsibility on infrastructure owners and operators, rather than on the technology and service providers that design, supply, and maintain many of the core systems relied upon by councils. This includes systems such as SCADA platforms, telemetry systems, and enterprise software (e.g. ERP and SaaS platforms), where there are a limited number of providers operating nationally.

In MDC's view, there is a strong case for placing greater emphasis on provider-level obligations, where capability, scale, and technical expertise are more concentrated. For example, requiring system providers to meet defined cyber security standards, monitor threats, and report vulnerabilities could deliver more consistent and cost-effective outcomes than expecting each individual council to develop equivalent capability independently.

MDC is also concerned about the potential future introduction of audit or assurance requirements. While not proposed in the medium term, such requirements are signalled as a possible future step. If implemented, these could impose significant additional costs on councils, particularly where external assurance is required. In a local government

context, these costs would ultimately be borne by ratepayers, which raises affordability concerns.

MDC notes that the proposed framework enables the Minister to specify additional measures as part of an entity's risk management programme, including requirements to address single points of failure. While improving resilience is important, meeting such expectations may require increased staffing, duplication of roles, or access to scarce specialist expertise, all of which carry significant cost implications for smaller councils.

This reinforces MDC's view that requirements of this nature are more appropriately directed at national-level system and service providers, where capability and resources are more concentrated, rather than at individual councils with limited scale and capacity.

In addition, MDC notes that the proposed regime includes significant penalties for non-compliance, including for relatively minor breaches. This reinforces the need to ensure that obligations are aligned with the level of control and capability that councils can reasonably maintain, particularly where systems and risks are shared with third-party providers.

Decisions sought:

1. That the framework gives greater consideration to the role of technology and service providers in managing cyber risk, including the potential for provider-level obligations to deliver more efficient and consistent outcomes across the sector.

2. That any requirements placed on councils are aligned with their scale and capability, and that compliance expectations, including any future audit requirements, are proportionate and affordable.

Third-party services and assurance requirements

MDC relies on a range of third-party providers to support the delivery, operation, and maintenance of its water and wastewater systems, including for software, telemetry, hosting, and specialist operational support. While Councils retain overall accountability as asset owners, delivery of cyber security outcomes is often dependent on third-party systems and providers. As a result, cyber security risk is not solely within Council's direct control but is shared across the systems and services that Council depends on. This raises questions about liability where cyber incidents arise from systems or services managed by third parties.

The proposed framework would benefit from greater clarity on how responsibilities are allocated where critical systems or services are delivered or supported by third parties. In particular, it is important that expectations placed on councils are aligned with the level of control they can reasonably exercise over external providers.

MDC also notes that any audit or assurance requirements relating to third-party systems must be realistic, proportionate, and affordable, particularly for smaller councils. Requirements that rely on extensive third-party certification, auditing, or contractual

enforcement may create significant cost and administrative burden, without necessarily improving cyber resilience outcomes.

Decision sought:

1. That Government provides clear guidance on the allocation of cyber security responsibilities between councils and third-party providers, and that any associated audit or assurance requirements are proportionate, practical, and aligned with councils' ability to influence and manage vendor risk.

Yours sincerely

Michael Ford

Mayor