Cybercrime Bill 2026

Explanatory Note

Clause 1 states that the Act is the Cybercrime Act 2026.

Clause 2 provides that the Act comes into force on the day after the date on which it becomes law in accordance with Article 34 of the Constitution.

Part 1
Preliminary matters

Clause 3 defines key technical terms used throughout the Bill. Because cybercrime investigations frequently involve specialised technology and digital evidence, it is important that commonly used terms such as "computer system", "computer data", "traffic data", "interception" and "service provider" are clearly defined. The definitions are designed to ensure the legislation remains technologically neutral and can continue to apply as technology evolves.

Clause 4 clarifies how penalties set out in the Bill are to be interpreted. The clause confirms that references to penalty units operate in accordance with existing legislation and explains how penalties apply to individuals and bodies corporate. The clause also preserves the court's discretion to impose imprisonment, fines or both where this is authorised by the legislation.

Clause 5 Cybercrime frequently crosses national borders and may be committed remotely from anywhere in the world. Clause 5 extends the Act beyond conduct occurring physically within Niue. It enables the Act to apply to conduct occurring outside Niue where there is a sufficient connection to Niue, including where the conduct affects computer systems, computer data, property, citizens or residents of Niue. This ensures that offenders

cannot avoid liability simply because their activities were carried out from another jurisdiction.

Clause 6 makes it clear that the Government is also subject to the Act. The provision promotes accountability and ensures that the protections and obligations established under the legislation apply equally to public authorities.

Part 2
Cybercrime offences

Clause 7 creates the offence commonly known as "hacking". The offence applies where a person intentionally obtains access to a computer system or computer data without permission. More serious penalties apply where the unauthorised access is undertaken for a fraudulent or dishonest purpose, such as stealing information or obtaining financial gain.

Clause 8 creates an offence for unlawfully intercepting electronic communications or computer data while it is being transmitted. The provision is intended to protect the confidentiality of communications and prevent conduct such as unlawfully monitoring, capturing or eavesdropping on data transmitted across networks.

Clause 9 creates an offence for intentionally damaging, deleting, altering or otherwise interfering with computer data without lawful authority. The offence is designed to address conduct such as malware attacks, ransomware attacks and other forms of digital sabotage that result in significant harm. Higher penalties apply where the offending creates a risk to life or causes particularly serious consequences such as substantial financial losses, threats to public safety or threats to national security.

Clause 10 creates an offence for intentionally disrupting the operation of a computer system or preventing authorised users from accessing it. The provision is intended to address conduct such as denial-of-service attacks and other deliberate disruptions of critical systems and services.

Clause 11 creates offences relating to tools used to facilitate cybercrime. These offences apply to the production, sale, importation, distribution or possession of software, hardware, passwords or access credentials intended to be used for committing offences under the Act. The

provision is intended to disrupt cybercrime before an attack occurs by criminalising the intentional supply and possession of cybercrime tools.

Clause 12 creates an offence of computer-related forgery. The offence applies where a person manipulates computer data to create information that is false or inauthentic and intends for that information to be treated as genuine for legal purposes. The offence is designed to address situations where digital records, documents or data are altered or created in a way that could mislead others into relying on them as authentic. This provision modernises traditional forgery offences by ensuring they apply to electronic records and digital information, regardless of whether the data is immediately readable or intelligible to a person. Higher penalties apply where the offending is committed on a larger scale, including through the use of multiple electronic communications.

Clause 13 creates an offence of computer-related fraud. The offence applies where a person manipulates computer data or interferes with the operation of a computer system in order to obtain a financial or economic benefit through dishonest or fraudulent means. The offence may include conduct such as altering electronic records, manipulating online transactions, or interfering with computer systems to obtain money, goods, services or other benefits. The provision ensures that fraudulent conduct committed through digital means can be effectively investigated and prosecuted, even where traditional fraud offences may not adequately address the technological methods used.

Clause 14 creates an offence relating to the misuse of another person's identity information through a computer system. The offence applies where a person possesses, transfers or uses another person's identifying information in connection with criminal offending and uses a computer system as part of that activity. The offence is intended to address forms of identity theft and identity fraud that increasingly occur through online platforms, electronic communications and digital services. The provision recognises the significant harm that can result from the unauthorised use of personal information, including financial loss, reputational damage and the facilitation of other criminal offending.

Clause 15 ensures that persons who assist, organise, direct or attempt cybercrime can be held criminally liable even where the principal offence is not completed. The provision recognises that cybercrime is often committed through organised groups involving multiple participants performing different roles.

Part 3
Enforcement

Clause 16 requires service providers that become involved in a cybercrime investigation to maintain the confidentiality of the investigation. The provision applies where a service provider is required to comply with a court order, notice, warrant or other requirement under the Act. It is intended to prevent investigations from being undermined by premature disclosure and to protect the integrity of criminal investigations. The clause also creates an offence for intentionally disclosing protected information relating to an investigation.

Clause 17 sets out the limited circumstances in which information relating to an investigation may be disclosed. The clause recognises that, despite the need for confidentiality, some disclosures are necessary for operational purposes. Service providers may disclose information to Police officers, relevant employees or contractors, and legal advisers where necessary to comply with their obligations or obtain legal advice. Safeguards are included to ensure that information is not disclosed beyond what is reasonably necessary.

Clause 18 allows a Police officer to apply to the High Court for a warrant authorising the search and seizure of computer systems and computer data relevant to an investigation. The Court must be satisfied that there are reasonable grounds to believe the material may provide evidence of an offence or has been obtained as the result of an offence. The clause also establishes procedures for recording and managing items that have been seized and provides limited rights of access to seized data in appropriate circumstances.

Clause 19 requires persons who have possession or control of a computer system or computer data to provide reasonable assistance to Police executing a search warrant. Assistance may include providing passwords, access codes and technical information necessary to access or copy computer data. The provision recognises that electronic evidence is often inaccessible without the cooperation of persons who control the relevant systems.

Clause 20 empowers the High Court to issue production orders requiring specified computer data or subscriber information to be produced for the purposes of a criminal investigation or criminal proceeding. The provision provides investigators with a means of obtaining electronic

evidence without requiring a physical search and seizure of equipment. It also allows subscriber information to be obtained from service providers where necessary to identify persons relevant to an investigation.

Clause 21 enables Police to require specified computer data to be preserved where there is a risk that it may otherwise be altered, destroyed or become inaccessible. The provision is intended to prevent the loss of important electronic evidence before a warrant, production order or other investigative process can be completed. Preservation notices may remain in force for up to 90 days, with a further extension available by order of the High Court.

Clause 22 enables the High Court to authorise the lawful collection and recording of electronic communications where the information is reasonably required for a criminal investigation or proceeding. The provision provides an investigative tool for obtaining communications evidence while ensuring that such activity occurs only under judicial supervision. The Court may authorise the assistance of service providers or authorise Police to undertake the activity directly through technical means.

Clause 23 enables the High Court to authorise the use of remote forensic tools in cybercrime investigations. A remote forensic tool may be installed on a suspect's computer system for the purpose of collecting evidence where less intrusive investigative methods would be ineffective. The Court may only grant an authorisation if it is satisfied that the evidence cannot reasonably be obtained through other means and that appropriate safeguards are in place. The provision includes detailed requirements relating to authorisations, record keeping, the protection of evidence and oversight of the use of remote forensic tools.

Clause 24 creates an offence for intentionally refusing or failing to comply with a warrant, order, notice or assistance requirement made under the Act. The provision supports the effective operation of the Act by ensuring that lawful investigative powers can be exercised and that persons are required to comply with obligations imposed by the Court or by law.

Clause 25 allows the High Court to order the disclosure of traffic data relevant to a criminal investigation or criminal proceeding. Traffic data does not generally include the content of communications, but rather information such as routes, destinations, times and other technical data associated with electronic communications. This information can assist

investigators in identifying connections between persons, devices and communications.

Clause 26 enables the High Court to authorise the collection or recording of traffic data associated with specified communications. The provision allows traffic data to be collected prospectively where it is reasonably required for an investigation and provides mechanisms for obtaining assistance from service providers where necessary.

Clause 27 creates an offence for intentionally refusing or failing to comply with an order requiring the disclosure, collection or recording of traffic data. The provision supports the effectiveness of the investigative powers established under clauses 25 and 26.

Part 4
Failure to comply with traffic data orders

Clause 28 establishes circumstances in which a body corporate may be held criminally liable for offences under the Act. The provision recognises that cybercrime may be committed by individuals acting on behalf of companies or other organisations. A body corporate may therefore be held liable where offending is committed by senior individuals acting within the scope of their authority or where inadequate supervision or control contributed to the offending. The clause ensures that organisations are encouraged to maintain appropriate oversight and compliance measures.

Clause 29 limits the criminal liability of service providers where their systems or services are used by third parties to commit offences. The provision recognises that service providers generally act as intermediaries and should not automatically be liable for unlawful conduct undertaken by users of their services. However, service providers remain subject to obligations imposed by court orders and are expected to take appropriate action where they become aware of illegal activity occurring through their services.

Part 5
Miscellaneous

Clause 30 protects specified officials from criminal and civil liability for actions taken in good faith while performing functions under the Act. The protection applies to specified members of the Crown Law Office, Police officers and persons assisting Police. The provision is intended to ensure that officials can properly carry out their lawful duties without fear of personal liability where they act honestly and reasonably.

Clause 31 requires the Chief of Police to provide annual reports to the Minister on the operation of the Act. The reporting requirements promote transparency and accountability by requiring information on the use of investigative powers, cybercrime investigations and criminal proceedings to be provided annually. The clause also includes safeguards to protect sensitive information and national security interests.

Regulations

Clause 32 empowers Cabinet to make regulations for the purposes of the Act. The regulation-making power provides flexibility to prescribe procedures, forms and administrative requirements necessary for the effective operation of the legislation and to respond to future technological developments.

Related amendments

Clause 33 introduces the Schedule, which contains consequential amendments to the *Mutual Assistance in Criminal Matters Act 1998*. The amendments strengthen Niue's ability to cooperate with foreign countries in investigating cybercrime and obtaining electronic evidence located across international borders. They also modernise mutual legal assistance procedures to reflect the unique challenges presented by cybercrime investigations.

Schedule
Related amendments to the Mutual Assistance in Criminal Matters Act 1998

The Schedule updates the *Mutual Assistance in Criminal Matters Act 1998* to support the investigation and prosecution of cybercrime.

The amendments introduce references to computer data and traffic data, provide new mechanisms for requesting and obtaining electronic evidence from overseas

jurisdictions, establish procedures for urgent requests, and update restrictions relating to the use, custody and disclosure of information obtained through mutual legal assistance arrangements.

The amendments are intended to ensure that Niue can effectively participate in international cooperation arrangements, recognising that cybercrime investigations frequently involve evidence and offenders located outside national borders.