PILON

MUTUAL LEGAL ASSISTANCE HANDBOOK

CYBERCRIME & ELECTRONIC EVIDENCE

PILON CYBERCRIME WORKING GROUP

PACIFIC ISLANDS
LAW OFFICERS' NETWORK

The Pacific Island Law Officers' Network (PILON) is a network of senior law officers from Pacific countries.

PILON has identified cybercrime as a strategic priority in its 2019-21 Strategic Plan. The Cybercrime Working Group supports PILON to address this strategic priority and has prepared this handbook for the benefit of PILON member countries. It is part of broader efforts to tackle cybercrime from a regional perspective focussing on the evidence gathering powers and international cooperation mechanisms with regional and international partners in line with the best practices.

Members of the Cybercrime Working Group are:


Tonga (Chair)


Australia


Fiji


New Zealand


Solomon Islands


America Samoa


Cook Islands


Nauru


Papua New Guinea


Vanuatu

November 2020

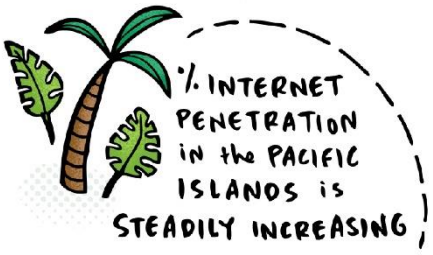
Australian Aid

This publication has been funded by the Australian Government through the Department of Foreign Affairs and Trade. The views expressed in this publication are the author's alone and are not necessarily the views of the Australian Government.

PACIFIC ISLANDS
LAW OFFICERS' NETWORK

Foreword

As the world becomes increasingly borderless, and crime increasingly transnational in nature, the provision of international assistance is becoming ever more essential. It can be an effective law enforcement tool, as it ensures that an offender cannot evade prosecution if evidence of their conduct is located in a foreign country. Mutual legal assistance is increasingly important for cybercrime investigations and prosecutions and is not well understood, or often used, in our region. During the unparalleled times we have experienced this year, it has become evident more than ever how heavily the world relies on technology and cyber space to remain connected whilst being physically apart. Unfortunately, we have seen that the increased connectivity has also led to an increase in transnational crime, with technology making criminal activity easier and more pervasive.



Even though this handbook has been specifically designed for PILON members, the foundations of international cooperation in criminal matters are universal and can be applied across the globe. The information contained in this resource builds on the discussions and learning from the 2019 PILON Cybercrime Workshop, hosted by Vanuatu, which focussed on international cooperation to share electronic evidence to combat cybercrime. This handbook sheds light on the domestic and international mechanisms in place so that the international community of criminal justice practitioners is able to provide cross-border assistance in the most efficient and effective way. Assistance of this sort is essential, and of increasing importance, given the nature of transnational crime, and cybercrime in particular, which knows no boundaries or jurisdiction.

This handbook provides you with practical information and a first port of call when a criminal investigation or proceeding requires cooperation with our neighbours. It is a practical tool for criminal justice practitioners - police, investigators, lawyers, central authorities, policy makers, and judicial officers – all the relevant stakeholders involved in international cooperation on criminal matters. It provides a range of accessible tools including country profiles, contacts and templates that are readily available and accessible via the PILON website (www.pilonsec.org).

I would like to thank each of the working group members and other partners who contributed to this Handbook. I hope it will be a useful tool for us to continue working together as a team to continue the fight against cybercrime, and all transnational crime.

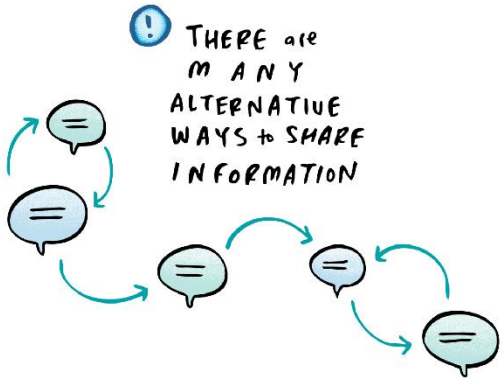
Ms Linda Simiki Folaumoetu'i
Attorney General, Kingdom of Tonga
Chair, PILON Cybercrime Working Group

CONTENTS

CHAPTER 1 – Introduction to International Cooperation

1.1 Informal International Cooperation

Informal international cooperation in criminal matters can take several forms: police-to-police, or agency-to-agency. This assistance may occur at any stage of a criminal investigation but usually before, or in parallel to, formal cooperation.



Police-to-police and other agency-to-agency assistance can be an effective way to determine what material is held by a foreign country prior to making a mutual assistance request (MAR). Informal cooperation may not be subject to specific legislative frameworks, but can be governed by policy and practice, often on the basis of reciprocity.

There are many agencies involved in the sharing of information through informal assistance

Police-to-Police Assistance

Police-to-police assistance is a form of cooperation between police in one country and police in another country. Police-to-police assistance is often used at the early investigation stage or to obtain evidence that does not require the use of coercive powers or the provision of a MAR. Evidence provided on a police-to police basis generally cannot be admitted into evidence in criminal prosecutions.

- E.g. Exchange of intelligence information.
- E.g. Preliminary enquiries to determine whether evidence of an offence is located in a foreign country.

Agency-to-Agency Assistance

Agency-to-agency assistance is a form of cooperation between non-police agencies, such as financial intelligence agencies. For example, the Australian Transaction Reports and Analysis Centre (AUSTRAC), the Cook Islands Financial Intelligence Unit (CIFIU) and the Fiji Financial Intelligence Unit (FIU)) have information sharing arrangements with their counterparts in foreign countries. The information sought through agency-to-agency assistance often does not require a MAR.

1.2 Formal International Cooperation

Formal international cooperation in criminal matters generally occurs between the governments of two or more countries and can include:

THE EXTRADITION FROM ONE COUNTRY TO ANOTHER OF A PERSON SUSPECTED OF A CRIME TO FACE PROSECUTION, OR A PERSON CONVICTED OF A CRIME TO SERVE A SENTENCE

THE PROVISION OF MATERIAL RELATING TO CRIMINAL PROCEEDINGS IN ONE COUNTRY AT THE REQUEST OF ANOTHER THROUGH MUTUAL LEGAL ASSISTANCE (MLA)

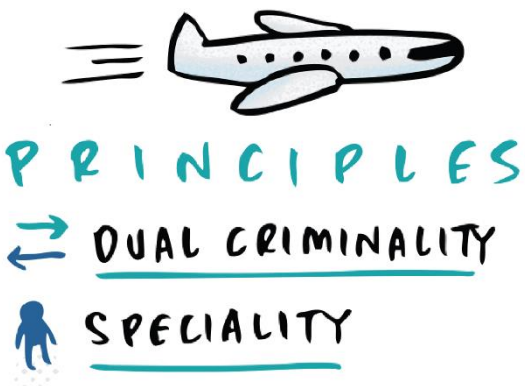
THE TRANSFER OF SENTENCED PRISONERS FROM ONE COUNTRY TO ANOTHER

Formal cooperation is governed by national legislation and bilateral or multilateral treaties and involves formal diplomatic and/or judicial functions. These mechanisms are highly effective tools for combating transnational crime, ensuring that an offender, or evidence of an offence, can be pursued despite being in a foreign jurisdiction.

Extradition

Extradition is the formal, government-to-government process used to return people to another jurisdiction to either face prosecution for a criminal offence, or to serve a sentence of imprisonment for a crime for which they have already been convicted in that jurisdiction. Extradition is an administrative, not criminal, process that is initiated at the request of a foreign government. The requested country must have a legal basis on which to accept the extradition request. The country's domestic laws alone might allow a request to be accepted, or there might need to be a bilateral extradition treaty, or a multilateral treaty with extradition obligations in place between the two countries.

Two key principles that underlie a successful extradition request from one country to another are dual criminality and speciality.



While an extradition request may be granted for serious criminal offences, there are some important bars (or grounds of refusal) that each requested country must consider. Such bars include a request for extradition for an alleged political offence, military offence, an ulterior purpose, or the risk of prejudice at trial. If an extradition request relates to an offence that concerns one of these bars, the request will normally be considered by a Minister or judicial officer of the requested country to determine if the request can be accepted. Another important bar to extradition is double jeopardy

Usually, a requested country's laws will set out a number of mandatory requirements that must be met before a requested country can accept an extradition request. These requirements may be supplemented by requirements contained in a bilateral or multilateral treaty.

Extradition is not deportation. It is a government-to-government process for achieving criminal justice purposes initiated by formal request and includes human rights safeguards to protect people (e.g. an extradition request may be rejected where there is the risk of the death penalty, torture, cruel, inhuman or degrading treatment). Unlike extradition, deportation is a unilateral determination made by a country to remove a person on the basis that they have no right to be in that country for immigration purposes. Depending on domestic law and procedure, some countries make a distinction between these processes in regard to a criminal prosecution. That is, there may be ramifications for a prosecution if a requested country deports rather than extradites a person wanted for a criminal justice purpose.

Mutual Legal Assistance (MLA)

MLA is the formal government-to-government process to obtain international assistance in criminal investigations, prosecutions, and to recover proceeds of crime. MLA is generally used for obtaining material that cannot be obtained through informal international cooperation mechanisms. It generally involves the provision of evidence that will be relied upon in court as part of a criminal prosecution.

More detailed information is provided in chapters 3, 4, and 5.

International Transfer of Sentenced Prisoners

Another specialised and growing area of international cooperation between countries is the international transfer of sentenced prisoners. This is where arrangements can be made between countries to transfer persons sentenced to terms of imprisonment in one country so that they serve their sentences in their country of citizenship.

1.3 Legal Bases for International Cooperation in Criminal Matters

Treaties

International cooperation in criminal matters can be effected on the basis of a bilateral treaty on MLA, or on the basis of a multilateral treaty that deals with other subject matter but contains MLA obligations on the parties to the treaty. Examples of such multilateral treaties include:

- Council of Europe Convention on Cybercrime (Budapest Convention)
- Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime
- United Nations Convention against Corruption (UNCAC)
- United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances
- United Nations Convention against Transnational Organised Crime (UNTOC)

Domestic Law

Where no treaty exists between countries for the purpose of international cooperation in criminal matters, the domestic law of a country may provide a basis for cooperation. Civil law is the most prevalent legal system found around the world and is premised on the system of codification of laws. Common law is the second most prevalent legal system and it is premised on the law being developed through jurisprudence of the courts. Common law jurisdictions are typically found in Commonwealth countries of the former British Empire. Domestic law is often used as the primary basis for cooperation in common law legal systems.

The distinction between civil law and common law becomes very apparent at the evidence gathering stage. In civil law systems, a magistrate gathers the evidence and no rules of evidence bar admissibility. In common law systems, a law enforcement investigator gathers the evidence and there are usually many evidentiary rules that affect all aspects of an investigation.

Reciprocity

The principle of reciprocity, also known as 'comity', is a long established principle in the relations of countries with respect to matters of international law and diplomacy. The principle of reciprocity means that where one country requests assistance or cooperation from another, that second country is generally expected to provide future similar assistance or cooperation, to the fullest extent permitted under its domestic law, to the first country in the in respect of equivalent criminal offences.

This principle is usually incorporated into treaties, memoranda of understanding and domestic law. Reciprocity is particularly prevalent in states with a civil law tradition, where it is viewed as a binding covenant. In common law countries, it is not viewed as an obligatory principle.

Reciprocity can also be a useful tool in the absence of a treaty, as it can be taken to be as a stand-alone promise that one country will do the same for another country in the future should the need arise.

1.4 Key Principles of International Cooperation

Dual Criminality

The dual criminality (or double criminality) principle requires that the conduct which is the subject of the request for international cooperation must be criminal in both the requesting and recipient country. This is often assessed at the time a request is received from a foreign country. Countries are required to treat this requirement as being fulfilled if the conduct underlying the offence is criminalised in both countries, irrespective of whether the countries attach the same kinds of legal nomenclature to the offence in their domestic laws. This principle reflects the fact that the bulk of MLA and extradition between countries still takes place via bilateral treaties and seeks to limit the artificial restrictions based on domestic law that would counteract international cooperation.

Double Jeopardy

Double jeopardy (*non bis in idem* or *ne bis in idem*) is a procedural defence that prevents an accused person from being tried twice on the same charges or another charge constituted by the same conduct following a valid acquittal or conviction. The recipient country may refuse assistance when it is clear that an accused has already been convicted and, for extradition, undergone punishment or acquitted for the same offence or another charge constitute by the same conduct set out in the request.

Confidentiality

The confidentiality principle requires that any information shared by the requesting country in a request, including communications between central authorities about the request, will be treated as confidential by the receiving state. This is recognition of the general understanding and expectation of confidentiality that is expected between countries in the mutual assistance process. Using this information without the requesting country's agreement or after consultation of the requesting country may seriously harm the criminal investigation, national security or international relations.

Speciality

The speciality principle requires that a person may only be prosecuted, or serve a sentence, for the offences in relation to which the request for international cooperation is granted. For example, if Country_A provides Country_B with evidence about a person in relation to one offence, that evidence cannot be used to prosecute that person, or any other person, in relation to another offence unless Country_B seeks the permission of Country_A to use the material for alternative purposes, and Country_A specifically agrees.

CHAPTER 2 – Cybercrime & Electronic Evidence

Cybercrime is by its very nature a transnational crime and it is critical that resilient, cooperative measures are available to combat this crime type.

Attacks launched by a person in one country can affect persons in multiple other countries. Even a relatively straightforward email communication sent to a person in the same country may generate electronic evidence in another Country_And data may be transmitted through servers located in several other countries. It is difficult to estimate the overall cost of cybercrime, which often involves the investigation response, repair and loss of resources and productivity. In 2018, cybercrime was estimated to cost the global economy approximately USD 600 Billion.[1]

Government, service providers (including internet service providers (ISPs) and communication service providers (CSPs) play a crucial role in building trust in information and communication technologies (ICT) and helping societies around the world make best use of these technologies. Cooperation between the government and private organisations is critical to ensure an effective criminal justice response.

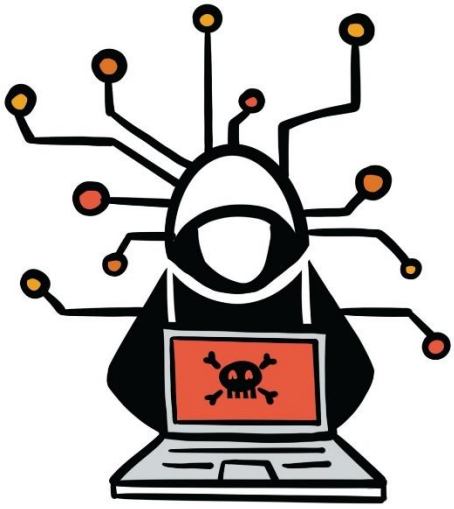
Internet data has become increasingly important in the investigation and prosecution of criminal offences. MLA is a complex and often-lengthy process that contrasts with the often very fast-paced nature of cybercrime. Electronic evidence moves quickly, and MLA can be a slow process, often taking months or even years to complete. As transnational crime increases and electronic evidence is routinely located across borders, it is essential that criminal justice systems are able to capture this evidence.[2]

2.1 What is Cybercrime?

Cybercrime is criminal activity that captures a wide range of behaviour in which computer technology is used as a tool, target or accessory of criminal activity. Cybercrime can be broadly broken down into two categories:

Use technology to enable traditional offences

Pure 'cybercrime' offences, made possible only by the technology itself



1 UNODC Op Ed on Cybercrime, 2018 (https://www.unodc.org/westandcentralafrica/en/2018_04_24_oped-on-cybercrime.html)

2 UNODC guide (vii) UNODC Practical Guide for Requesting Electronic Evidence Across Borders, 2019 (vii)

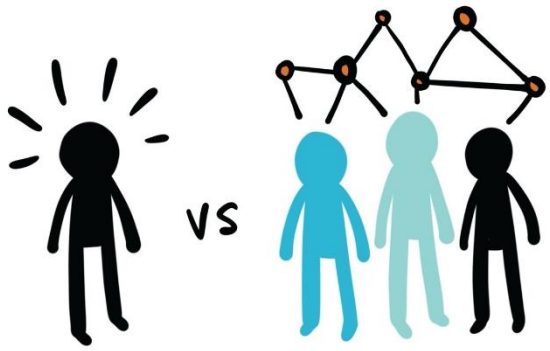
Technology-enabled offences use the internet and ICT as a force multiplier. These crimes use the internet to increase the scale and reach of victims using computers, computer networks or other forms of information communications technology. Examples of technology-enabled offences include fraud, theft, sexual exploitation and harassment offences.

Pure cybercrime offences differ from technology enabled crimes, as they require the use of ICT. That is, crimes against computers and information systems where the aim is to gain unauthorised access to a device or deny access to a legitimate user (typically with malicious software such as WannaCry and Industroyer). Other examples include hacking[3], the production and dissemination of malware for the purpose of criminal activity, botnets[4] and phishing.

2.2 Cybercriminals

There is no single 'type' of cybercriminal. Historically, criminal prosecutions and investigations reveal that cybercriminals can vary significantly in terms of age, sophistication, resources, objectives, opportunities, and technical abilities. Other elements constituting the criminality may also significantly differ, such as:

Whether it is done solely by an individual, or may involve sophisticated, organised and serious crime elements



What motivations may be, including financial, political or ideological, reputational or information gathering

This can make investigating and prosecuting cybercrime incredibly difficult. While sophistication, technical ability and resourcing can go a long way in disrupting law enforcement efforts to detect, prevent, investigate and prosecute these kinds of crimes, the availability and increasing simplicity of disruption technologies, platforms and services, enhances the ability for even non-technical criminals to find success in criminal activity online. For example, the use of anonymising browsers and platforms (such as The Onion Router) may significantly increase the difficulty for law enforcement to determine who may be accessing child sexual exploitation or abuse material online.

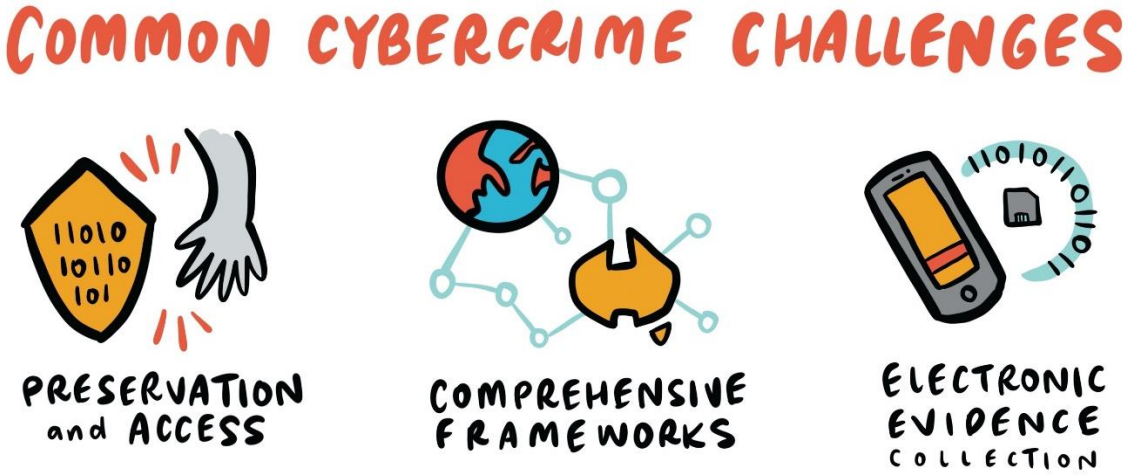
3 Please note that hacking is not necessarily an illegal activity. Hacking is simply the act of accessing a computer system through unconventional means. It is effectively the act of picking a digital lock. However, like the real-world lock smith, picking a lock is not necessarily an illegal activity depending on why it is done.

4 Like hacking, botnets are often considered to be malicious. A botnet is simply a number of internet-connected devices. Such a network can be used for malicious purposes.

2.3 Under Reporting of Cybercrime

Cybercrime is widely believed to be underreported.[5] Victims may report criminal activity if they personally sustain loss or some kind of damage. However, there are numerous reasons why victims of cybercrime may choose not to report, including:

The underreporting of cybercriminal activity may mean that law enforcement and policy makers do not fully appreciate the impact of certain types of cybercrime. Underreporting or lack of reporting may also make it difficult for law enforcement agencies to identify evidence to support investigations and prosecutions, including having a sufficient evidence base for supporting international crime cooperation mechanisms, such as MLA.



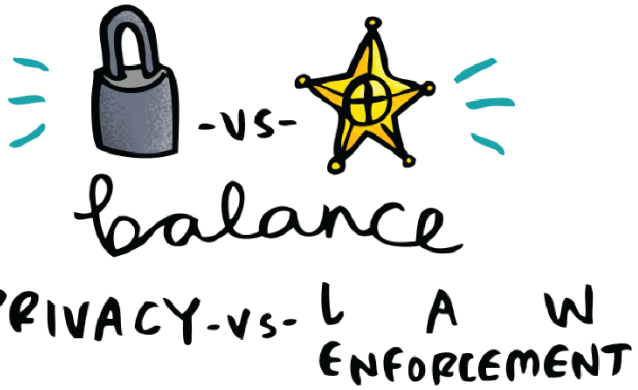
5 CoE Electronic Evidence Guide, 2020, p129

2.4 Electronic Evidence

Electronic evidence, also known as e-evidence or digital evidence, is 'any information generated, stored or transmitted in digital form that may later be needed to prove or disprove a fact disputed in legal proceedings'.[6] This can include information that is obtained from a device (such as a computer hard drive or mobile phone), directly from the internet (such as an email account or information retrieved remotely from a cloud storage account), or from a service provider that is storing the information.

The intangible nature of information stored electronically makes it more volatile and fragile than traditional forms of evidence. Electronic evidence, when on devices with computer memory is volatile because it can easily be altered, overwritten, corrupted or even destroyed – on purpose, or through normal use. This creates new challenges for our criminal justice systems and, as with other types of forensic evidence, proper processes for obtaining and handling electronic evidence is critical. Digital forensics is a branch of forensic science that has developed in response to this need in our criminal justice response and encompasses the recovery and investigation of material found in digital devices. Specialised procedures, tools and techniques are essential to investigate various cybercrimes and to ensure electronic evidence is handled appropriately in order to ensure the evidence is obtained in compliance with existing legislation and can be used in court.

In many ways, electronic evidence is no different from traditional evidence (such as documents, photographs, witness testimony, and DNA). If electronic evidence is to be introduced as 'evidence' in legal proceedings the court must be satisfied the evidence has not been altered or changed in any way from the time it was obtained.



6 CoE Electronic Evidence Guide, 2020, p.12

Technology and electronic evidence have become regular features in criminal investigations. This is due to the way technology has become an integral part of every aspect of our lives. For example, most of the ways we interact or conduct business involve a computer or some type of electronic device. Cybercriminals use technology in much the same way and use the technology itself to commit the crime.

Due to the shift of criminal activity from the real world to the online sphere, evidence of the criminal activity is regularly discovered on personal computers, websites, social networks, emails or cloud storage. Courts have accepted emails, ATM transaction logs, social media posts, audio files as evidence in cases and are generally becoming more familiar with the unique value electronic evidence can have to proving the occurrence of crime.

Electronic evidence is generally dealt with in court in the same way as any other type of evidence and is subject to the same rules and laws that apply to traditional forms of documentary evidence. That is, the onus is on the prosecution to demonstrate the evidence has not been altered or changed since it was first obtained by law enforcement. In words, the defence can challenge its admissibility and the prosecution will need to provide sufficient evidence to the court showing that the electronic evidence is trustworthy and reliable. Common challenges made by the defence in relation to electronic evidence include: challenging the search of persons property or the electronic device where the evidence was seized (e.g. search warrant not properly obtained or executed), and challenging the integrity of the evidence itself (e.g. has been altered, the defendant using the profile at that time). Prosecutors need to be aware of and ready for these kinds of challenges.

Types of Data

Electronic data is typically classified as either content or non-content. Data can also be categorised by whether it already exists (i.e. stored data) or is being captured as it is generated (real-time collection or interception). The types of data captured from both content and non-content data is instrumental to the investigation of modern crime types as it can be used to identify the perpetrator through the cross analysis of the contents of the message as well as the geo-spatial details from which the message was sent and received.

NON-CONTENT DATA

Non-content data includes transactional data such as whom a communication was to or from, the time it was transmitted, and the duration or size of the communication. It also includes subscriber information such as a customer's name, address, billing information, and any subscriber identifier such as a username, email address or IP address.

Dependant on the Country_And the laws governing the disclosure of data to foreign countries, service providers may provide non-content data to law enforcement for investigative use where possible, it is highly recommended that law enforcement obtain non-content data prior to making a MAR. Law enforcement may be able to seek this data through informal police-to-police channels or directly from the service provider.[7]

However, non-content data can be very useful to assist, confirm or dismiss targets in an investigation, to confirm the evidence is available and/or as supporting grounds for making a MAR for content data. Non-content data can also be useful to meet the relevant legal threshold for seeking content data in a MAR (e.g. probable cause if seeking content data from the US).

SUBSCRIBER DATA/ INFORMATION/BSI

Subscriber data includes personal details provided by the user at registration of service. This could include the name and address of a subscriber, internet connection records, length and type of internet service, a subscriber's assigned IP address, network address assigned to a specific internet session, and/or payment information (bank account, credit card details).

Subscriber data could assist an investigation if the person who up the account used their real details. Remember the subscriber data may not be verified by the company when it is collected from the subscriber.

7 Please note different countries have different rules on the disclosure of non-content data without authorisation.

TRAFFIC DATA / TRANSACTIONAL DATA / IP LOGS

Referred to by a few different names, transactional data, traffic data or IP logs show when an internet account has been accessed by a particular IP address. An IP address is the unique number assigned to a computer or device which is used to route traffic to or from the device. IPI og data shows when an internet account has been accessed by a particular IP address. This transactional data about when, and from what computer, a message was sent might help identify who has used a particular internet account or profile. You can then trace the IP address back to a physical location or match it up with times when the suspect was known or believed to be online. This information may help identify who has used a particular internet account at a specific time.

IP addresses and IP logs are helpful in the identification of user details and can be used to ascertain when an account was accessed. Seeking this type of non-content data directly from the service provider may be useful to include in the MAR. However, mobile phones (and other internet enabled devices) are allocated a new IP address every time the internet is accessed (referred to as dynamic allocation) and records of which IP address were allocated to which phone may not be kept for very long dependent on domestic data retention laws and business practices. While this may confuse the MAR process, it is still useful data to include in a MAR to help the service provider in finding the information requested.

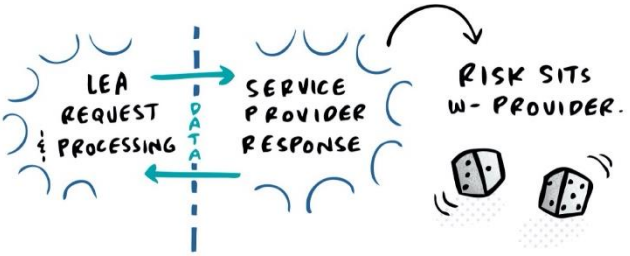
CONTENT DATA

Content data means information that reveals the content of the communication, or the message or information being conveyed by the communication, whether or not any interpretation, process, mechanism or device needs to be applied or used to make the meaning of the communication intelligible. It refers to the stored content of emails, posts, comments, address books, photos.

There is no universal definition or common understanding of what is considered content data or non-content data. For example, in some jurisdictions IP logs would be considered to be a type of non-content data, whereas as in others it would be content data. What is important is to consider whether a coercive power (e.g. a search warrant) will be required in order to obtain the data, which is almost always the case with content data.

2.5 Working with Service Providers

Cooperation with internet service providers is essential to law enforcement's ability to effectively investigate cybercrime. Consideration must be given to balance personal protections and online freedom with the need for law enforcement to access data needed to successfully investigate alleged cybercrimes. Both industry and government have roles in maintaining the safety of the internet and preventing online harm. Therefore, government cooperation with industry is a shared interest and the creation and maintenance of productive working relationships is of the utmost importance. The question is how both can best cooperate with each other to make the internet safer, while at the same time respect their different roles and the fundamental rights of users. Many service providers are often willing to provide some non-content data (e.g. subscriber, traffic data) on a police-to-police basis. However, most require a formal MAR to provide content data, and some will require a formal MAR before providing any data at all.



2.6 Where are the Records?

If seeking records from a service provider, the first question to ask yourself is 'where are the records?' Most service providers are located in the US and consequently, the requirements of US law need to be met when seeking to obtain internet records (non-content or content) from those service providers. However, as a number of these entities are moving servers and records from the US, it is important to check that the evidence you are trying to obtain through MLA is located in the country you are making the request to. Identifying an account by reference to the domain name (e.g. '.com.au') is no guarantee that the records are located in the same Country_As the domain suggests.

Please refer to Service Provider Profiles and Search-ISP list for more information on specific service providers.

2.7 Preserving Internet Records

Service providers store electronic evidence in the form of internet records (non-content and content), however they generally do not store data indefinitely. Service providers will usually only keep data for as long as they need it for typical internal administrative purposes (such as billing), or as required by law under any data retention scheme[8]. It can also easily be deleted or changed by a user. In recognition of the fact that electronic evidence is fragile and volatile, a process to 'preserve' data has been established and is an essential part of the MLA process and domestic electronic evidence collection.

A preservation request takes a 'snapshot' of data relating to a particular account or profile at the time the preservation takes effect. Preservation requests can usually only be made by law enforcement and should be actioned straight away. After processing a preservation request, the service provider will usually send an automated response with a reference number within 1-2 business days. Most service providers have information on how law enforcement can make a preservation request in their law enforcement guidelines. It is a relatively simple process for law enforcement to preserve internet records, and most of the major US service providers have specific websites or 'portals' for this exact purpose. Though police-to-police cooperation, 24/7 Networks or MARs *can* be used to seek preservation of data, law enforcement should use the specific websites or portal.

Preservation requests can last for anywhere from 90 to 180 days and thereafter automatically lapse or expire unless an extension is sought. The law enforcement agency is responsible for maintaining and extending preservation requests, and it should be extended until the original material requested in the MAR has been received.

Most major service providers do not notify accountholders upon the receipt of a preservation request, however some do. If notification may be harmful to the investigation, prior to making the preservation request law enforcement should, if possible, confirm with the relevant service provider whether the account holder will be notified. If the service provider will notify the account holder, law enforcement may wish to request that the service provider refrain from doing so where the notification itself risks harming the investigation.

The date of preservation, any extensions and the preservation reference number should be included in the MAR. Indeed, some countries will not accept a MAR for internet records without proof that the data is preserved.

Further information on making emergency requests from particular service providers can be found in Chapter 7.

8 Data retention is the mandated minimum period of time that a CSP has to keep data and is different in each Country_According to their legislation, if there if such legislation. It is different to preservation.

2.8 Emergency Situations

It is important to consider what options are available where electronic evidence could assist in an emergency situation where there is a risk of death or serious harm. Many service providers specifically provide for emergency situations in their law enforcement guidelines which allow for law enforcement to request data (content and non-content) directly from the service provider without delay. Clearly setting out the timeframe and 'imminence' of the risk or danger in an emergency request is critical to demonstrate that there is no opportunity to follow the standard MLA process.

Urgent MARs requesting assistance can also be made between countries. In some circumstances, an oral MAR could be made with a written MAR to follow. Strong relationships with counterparts in foreign law enforcement and central authorities are particularly important in emergency situations. The 24/7 Network of contact points, INTERPOL and the Pacific Transnational Crime Network (PTCN) are all useful contacts to seek advice on handling emergency requests. If making an emergency request to the US, it is recommended that the requesting Country_Also contact the relevant FBI attaché who should be able to assist in following through the process with the service providers and Office of International Affairs in the US Department of Justice.

Further information on making emergency requests from particular service providers can be found in Chapter 7.

2.9 Child Sexual Abuse Material (CSAM)

The fast-paced technological innovation and widespread accessibility of ICT has allowed great gains in our society. However, it has also provided a new mechanism by which sexual abuse of children can occur, including providing an avenue for online offender communities to encourage one another and produce and share child sexual abuse material (CSAM)[9]. While not a new phenomenon, unprecedented access to technology through the internet has allowed the demand for and access to CSAM to flourish. CSAM is any representation, by whatever means, of a child engaged in real or simulated explicit sexual activities or any representation of the sexual parts of a child, the dominant characteristics of which is depiction for a sexual purpose.[10] Child sexual abuse can take many other forms in the online world and includes: grooming including of third parties such as parents or carers to gain access to a child; procuring, creating, controlling or accessing CSAM; engaging in live-streamed child sexual abuse; and conduct which facilitates these crimes (e.g. creating and administering online websites and forums to engage in child abuse offences online).

Unfortunately, a significant number of MARs relate to online child abuse investigations and prosecutions. Familiarise yourself with the criminal offences and procedural frameworks in your country that address CSAM, and related child abuse offences, so that you are able to assist should a MAR relating to CSAM arise. If records sought through a MAR are likely to contain CSAM it should be specifically noted in the MAR and specific handling protocols will apply. These protocols will be agreed between the requesting and recipient country. For example, before CSAM which has been requested in a MAR can be brought into Australia, it is mandatory for officials to first obtain an important certificate for those requested materials, otherwise they are prohibited.

Service providers located in the US are required by US law to report identified or suspected instances of child exploitation appearing on their sites or platforms from anywhere in the world to the National Centre for Missing and Exploited Children (NCMEC). NCMEC refers matters to law enforcement authorities from around the world in order to help victims.

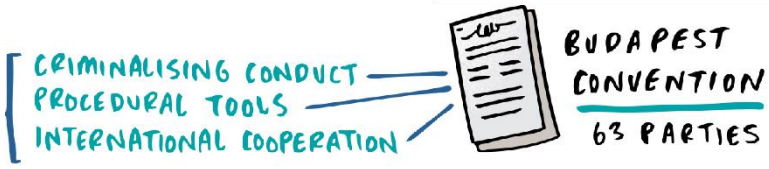
9 Use of the phrase "child pornography" benefits child sex abusers because it indicates legitimacy and compliance on the part of the victim and therefore legality on the part of the abuser and does not recognise the horrific abuse suffered by victims. Every photograph or video captures an actual situation where a child has been abused. The term Child Sexual Abuse Material (CSAM) more accurately reflects what is depicted – the sexual abuse and exploitation of children. Not only do these images and videos document victims' exploitation and abuse, but when these files are shared across the internet, child victims suffer repeat and ongoing re-victimization each time the image of their sexual abuse is viewed.

10 Optional Protocol, UN Convention on the Rights of the Child

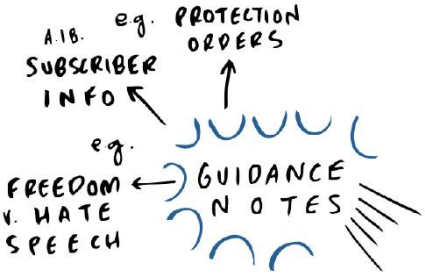
This is a complex area that cannot be comprehensively covered in this handbook. For further information we recommend the following resources:

- www.cybersafetypasifika.org/
- www.thinkuknow.org.au/
- virtualglobaltaskforce.com/
- www.accce.gov.au/
- www.missingkids.org/theissues/csam
- inhope.org
- onlinesafetycommission.com/
- www.netsafe.org.nz/

2.10 The Budapest Convention



The Budapest Convention seeks to harmonise national laws to address a range of criminal conduct such as computer related fraud, CSAM and violations of network security. The Convention serves as a guideline to member states for developing comprehensive national legislation against cybercrime. It also deals with the domestic collection of electronic evidence for the purpose of international crime cooperation between the 64 countries currently signatories to the convention. The development of effective substantive and procedural laws, and the facilitation of effective international crime cooperation between foreign governments and law enforcement agencies, is crucial to overcoming the modern challenges faced domestically when combatting serious criminal activity both online and offline. A number of guidance notes have been developed aimed at facilitating the effective use and implementation of the convention and represent the common understanding of the Parties regarding use of the convention.



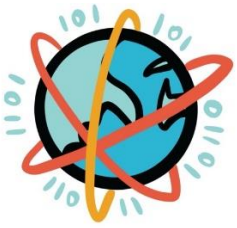
Second Additional Protocol

Parties to the Convention (by way of the Cybercrime Convention Committee) continue to assess how to modernise the frameworks under the Convention to tackle the challenges posed by the impact of the digital age on crime and law enforcement. Over the years, the T-CY Committee has reported on the ongoing challenges associated with international crime cooperation. For example, significant delays in MLA processes, and not knowing the location of data sought. Accordingly, to address those challenges the T-CY Committee decided that a new additional protocol was required for the Convention.

On 9 June 2017, the terms of reference for the preparation of the draft Second Additional Protocol were published in order to address these urgent challenges and provide solutions for a more efficient international criminal justice response to cybercrime and crime involving electronic evidence. The Second Additional Protocol aims to include:

Provisions for streamlining and creating a more effective mutual legal assistance regime

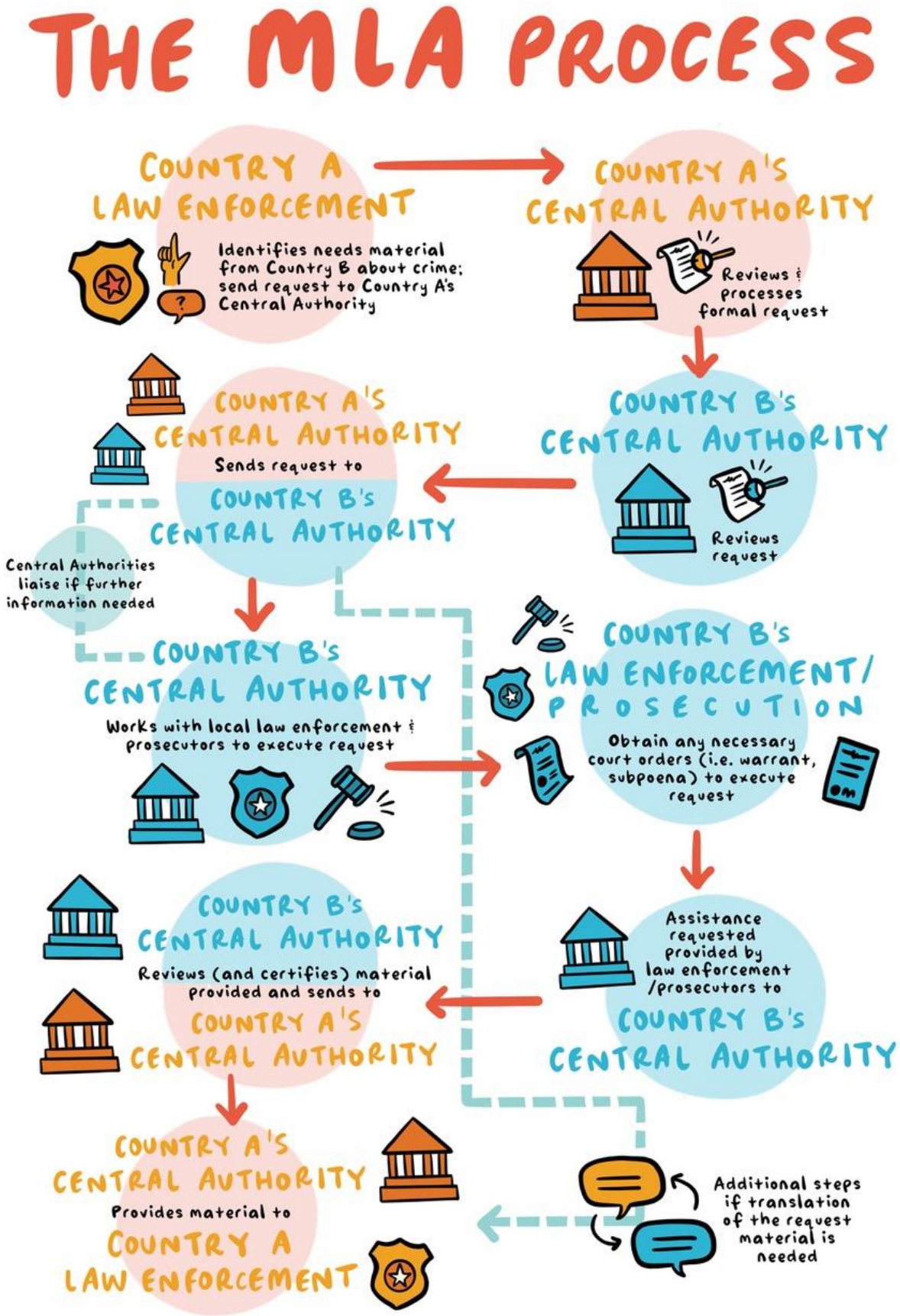
Provisions allowing for direct cooperation with communications service providers in other party jurisdictions



More effective and secure trans-border access to data for member states

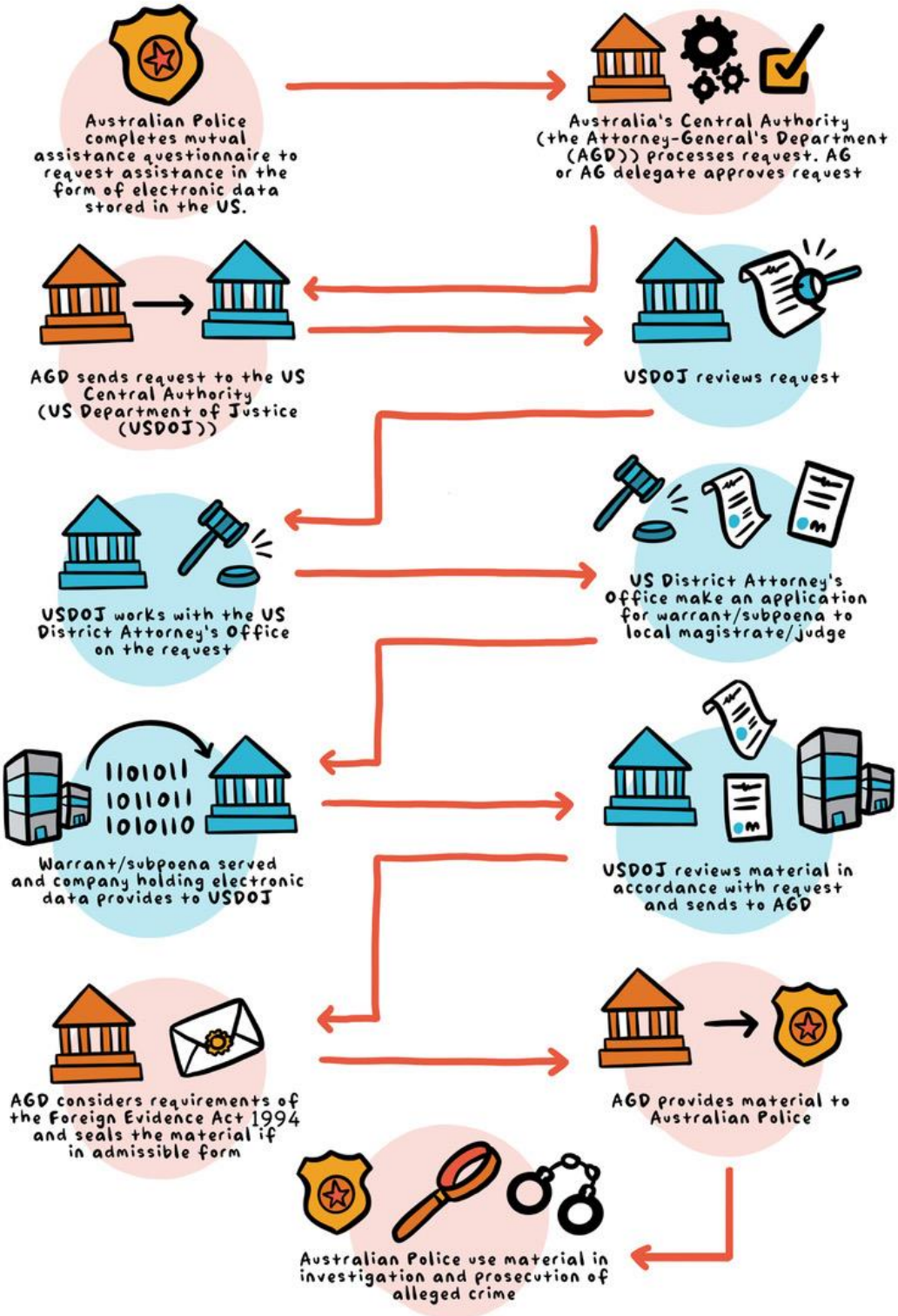
The significant growth in the transnational nature of cybercrime and cyber-enabled crime and the ease in which electronic data can be stored overseas, continues to place a significant burden on formal and informal international crime cooperation processes (especially MLA processes). The Second Additional Protocol stands as a timely update to the procedural laws within the Convention. The T-CY Committee aim for the Second Additional Protocol to be finalised by the end of 2020.

CHAPTER 3 – Mutual Legal Assistance (MLA)



EXAMPLE MLA PROCESS

MAR from AUSTRALIA to USA for INTERNET DATA



3.1 What is MLA?

MLA is the process countries use to provide and obtain formal government-to-government assistance in criminal investigations and prosecutions where evidence or proceeds of crime are in a different country. Most countries have specific legislation governing the MLA process within that country, often called the Mutual Assistance in Criminal Matters Act ("MACMA"). MLA is based on the principle of reciprocity. Mutual Assistance requests (MARs) may be made under country's' MLA legislation and also pursuant to bilateral MLA treaties or multilateral agreements, including international conventions such as the Council of Europe Convention on Cybercrime (Budapest Convention), United Nations Convention against Transnational Organised Crime (UNTOC), United Nations Convention against Corruption (UNCAC) and the Revised Scheme Relating to Mutual Legal Assistance in Criminal Matters within the Commonwealth (the Harare Scheme).

MLA legislation varies from country-to-country, but frequently includes a catch-all clause specifying that it does not limit the provision of other types of country-to-Country_Assistance (see for example Fiji s4 MACMA; Tonga s5 MACMA). This clause means that types of assistance not specifically listed in the legislation can still be provided. A country may impose limits on the extent to which a catch-all clause can fill the gaps in MLA legislation.

For example, New Zealand takes the approach that coercive or court sanctioned powers need to be expressly provided for in legislation. Accordingly, the catch-all clause in New Zealand's MACMA can be used to authorise MARs involving non-coercive powers only (such as requests to interview witnesses on a voluntary basis and requests for information available without requiring a search warrant). These requests tend not to involve much of an intrusion on privacy or use of domestic resources.

3.2 Central Authorities

Each country should have a designated 'Central Authority' through which formal MLA requests are directed and dealt with. Most countries will not accept MARs made directly by law enforcement officials, prosecutors or judges, and expect requests to come through the designated Central Authority.

Central Authority contact details for PILON members, Canada, UK and US can be found in the country profiles in Chapter 6 on the relevant Central Authority website or on the UNODC Online Directory of Central Authorities (available to central authorities and government agencies with a user account).

The International Institute for Justice and the Rule of Law Good Practices for Central Authorities are designed to guide the important work of these institutions and set forth the institutional, legal and practical considerations needed to create and support durable legal institutions. The top ten good practices are:

1. Each country should establish and designate a single Central Authority to facilitate international cooperation in criminal matters through MLA and extradition.
2. A Central Authority should be adequately resourced and properly staffed with specialized and well-trained legal experts so that it may carry out its functions effectively.
3. A Central Authority should be able to communicate directly with other Central Authorities.
4. A Central Authority should be able to transmit and receive MLA requests directly to and from other Central Authorities.
5. A Central Authority should maintain confidentiality of MLA and extradition requests to protect the integrity of investigations and prosecutions.
6. A Central Authority should be empowered to take action on or coordinate the execution of requests from and to international counterparts for MLA.
7. A Central Authority should serve to ensure that requests for MLA from domestic law enforcement and judicial authorities are sufficient and comply with the terms of the applicable law, treaty or convention before such requests are transmitted.
8. A Central Authority should be able to facilitate the judicial aspect of extradition requests and follow the status of such requests.
9. A Central Authority should be able to ensure that extradition requests from domestic law enforcement and judicial authorities are sufficient and comply with the terms of the applicable law, treaty or convention before such requests are transmitted.
10. A Central Authority should not serve to inhibit other informal cooperation by and/or between governmental law enforcement entities.

3.3 Common Types of Assistance

This section sets out the common types of assistance that are requested in a MAR. Officers in a Central Authority will be responsible for progressing both 'outgoing' and 'incoming' MARs. Understanding the different types of assistance is an important part of MLA to be able to facilitate your domestic law enforcement obtaining assistance from another country (outgoing); as well as facilitate a request from another country to obtain assistance from your country (incoming).

For the purpose of this section, Country_A is the requesting country making an outgoing request and Country_B is the recipient country receiving an incoming request.

Locating or Identifying a Person

Where Country_A sends a MAR seeking assistance in locating or identifying a person, the relevant clause in Country_B's MLA legislation is likely to require that:

- the MAR relates to a criminal matter in Country_A, and
- there are reasonable grounds for believing that the person to whom the request relates:
    - is in Country_B, and
    - is/might be involved with, give evidence in court, or provide assistance relevant to, the criminal matter.

This is not a very exacting test to meet. To determine that the person is actually in Country_B by contacting the agency responsible for monitoring border movements such as customs.

Service of Process

A MAR may request assistance in arranging service of process (i.e. documents). The test for this type of assistance is unlikely to be onerous and is usually satisfied if there are reasonable grounds for believing that the person to be served is in Country_B. Country_B can probably instruct police to serve the person and then arrange for the police officer to provide an affidavit of service to be sent back to Country_A. Service of process on a person can likely be done even when no court proceedings have begun and regardless of the seriousness of the offence.

Executing a Search Warrant or Production Order

Often information needed for an investigation or prosecution in Country_A is held in another country (i.e. Country_B). In the digital age, it is increasingly common for information to be located in another country. Information could include bank records, company registration records, telephone records, internet records (e.g. email, social media posts, and subscriber details), computers, physical documents or objects. Often electronic evidence will be held by a communication service provider based in the US (e.g. Facebook, Google).

If the information sought by Country_A is subject to a reasonable expectation of privacy (which most of those listed above are), it will probably need to be obtained by a coercive power – usually a search warrant or production order. Where a search warrant is required to obtain evidence or information requested in a MAR, Country_B will have to satisfy the test for a search warrant as set out in Country_B's MLA legislation. The test to authorize and issue a search warrant is likely to mirror the test for requesting a search warrant in Country_B's domestic criminal procedure legislation. This test often requires there to be "reasonable grounds to believe" an article or thing relevant to the criminal matter is in Country_B. Be aware that the country receiving the MAR (i.e. Country_B) will be bound by its own test to obtain a search warrant in order to provide the assistance.

Most countries will have a high threshold for obtaining information by search warrant. For example:

- New Zealand has a "reasonable grounds to believe" test to obtain a search warrant. This means there must be an objective and credible basis for thinking a search will discover the items identified in the warrant. There must be more than surmise or suspicion that something is inherently likely.
- United States has a "probable cause" test for obtaining a search warrant. This is similar to the "reasonable grounds to believe" test but has a higher threshold and can be challenging to meet.

To assist Country_B to meet the requisite test and obtain a search warrant, the MAR from Country_A should clearly outline what particular evidence is sought, the reasons for believing the evidence is in the place where it is sought, and the link between the evidence sought and the offence. Unless this can be clearly shown, it may be difficult for the recipient country to obtain the necessary search warrant or production order from the court and provide the assistance requested.

Requests for electronic data should include a specific date range for the information sought, and reasons why those dates have been identified. Date ranges should correlate to the alleged offending, and not be a broad 'fishing expedition'.

Requests for bank or financial records should identify the nature of the records, the name and location of the institution where the records are located, the account number, and a date range for the information sought, with reasons why those dates have been identified.

Obtaining Evidence from Witnesses

In many criminal prosecutions the critical evidence that decides the case is that obtained from witnesses, either voluntarily or by compulsion. 'Witnesses' should be read broadly here and could include those who saw the offence take place, the victim, an expert or, in some cases, even the suspect or defendant. If the person asked to give evidence is the suspect or defendant it is likely they will be considered competent, but not compellable, to give evidence. In other words, a defendant can give evidence voluntarily, but cannot be compelled. This is because the common law privilege against self-incrimination provides that a person cannot be required to give information that would tend to incriminate him or herself.

Where a witness refuses to give evidence (either in person or by providing a voluntary statement), it may be open to Country_A to request that Country_B compel the witness to do so, often by summonsing the witness to provide evidence before the court in Country_B.

Domestic legislation usually sets out the process for taking evidence – whether it is to be taken before a court, or by way of a written statement (e.g. a sworn or affirmed affidavit) – but may not expressly provide for taking voluntary evidence.

Taking evidence in court (testimony in person or via video link)

Country_A may request that a witness located or resident in Country_B give evidence in court either in person or by video link. Both of these options can become expensive and if it appears that costs involved will be excessive, countries may discuss whether Country_A is able meet some, or all, of the costs.

Giving evidence in person would involve the witness travelling to Country_A in order to give evidence in court. Frequently the requesting country will provide an undertaking to meet the witness's travel expenses in this type of case. Domestic legislation will usually set out any other relevant conditions, such as that the witness has freely consented to attend, and that the person will be returned to the original country in accordance with agreed arrangements.

Alternatively, Country_A may request that the witness give evidence via video link from Country_B, and that this be facilitated by Country_B. Depending on Country_A's domestic legal requirements, Country_A may require the witness to give evidence via video link from a court in Country_B to a court in Country_A. However, it may be sufficient for the witness to give evidence via a video link platform. If permitted under both Country_A and B's respective domestic legislation, this can be a much simpler and more cost-effective solution. The requesting country, Country_A, may need to consider whether counsel from Country_B can be present and actively participate in the court hearing (e.g. conduct the examination of the witness), or whether counsel from Country_A will examine the witness (e.g. either in person by travelling to Country_B, or via video link).

Depending on the respective countries' legislation, it may also be possible for Country_A to request evidence from a prisoner in Country_B either by travelling in person or via video link. The former may present significant logistical challenges.

Voluntary Witness Statement

MARs requesting a voluntary statement from a witness are very common. If agreeable to both countries, a request for a voluntary witness statement may be dealt with informally outside of the MLA process on a police-to-police basis. However, sometimes Country_A may require the formal MLA process to be followed to ensure the evidence will be admissible in accordance with their own domestic procedural requirements. In such a case, Country_B can execute the MAR by liaising with their police to interview the witness and obtain a statement.

If Country_A requires a voluntary witness statement, the following details should be included in the MAR:

Name, nationality & location of the witness(es)

Their status in the case (suspect accused or simply a witness)

Explanation of how the information sought from the witness is relevant to the case

An indication of whether the witness is likely to cooperate in providing the statement testimony (if known)

Material Lawfully Obtained

Country_A may make a request for material that was previously lawfully obtained by Country_B's law enforcement in its own domestic investigation, where Country_B is still lawfully in possession of that material. This can often be useful when Country_A's law enforcement becomes aware that a foreign law enforcement agency has previously, or concurrently, carried out investigations involving the same suspect or offence and may have material to assist. This material may be shared on an informal police-to-police basis or through intelligence channels, however, may need to be formally requested through MLA in order for that material to be admissible in court.

For example, in Australia, s13A of the MACMA deals with requests made from foreign countries for material lawfully obtained by Australian law enforcement agencies (such as the Australian Federal Police) pursuant to an investigation or proceeding.

Assistance Related to Proceeds of Crime

Another common form of assistance may be when Country_A needs assistance with the restraint and recovery of the proceeds of crime from Country_B. The process for this will usually be set out in both countries' MAR legislation. It is likely the regime will allow for assistance at four stages of the confiscation process:

INVESTIGATION

RESTRAINING

FORFEITING

DISPOSAL

Country_A may request that Country_B obtains an examination order, a production order, or a search warrant on its behalf.	Country_A may request Country_B to obtain an interim foreign restraining order, or to register a foreign restraining order.	Country_A may request Country_B's authorities to authorize the Commissioner of Police to make an application for registration of the foreign forfeiture order to the relevant court. This stage is also referred to as confiscation.	Unlike the other stages in the confiscation process, it is possible that the assistance that Country_B provides at the disposal stage may not be prescribed by legislation.


CHECKLIST
PROCESSING an OUTGOING MAR
1 REVIEW MLA QUESTIONNAIRE
received from instructing agency (usually police)
Details for all offenders and offences ?
Any timeframes for receipt of evidence (e.g. court dates)?
Sufficient facts to link the alleged conduct to the assistance sought?
Is it clear what assistance is sought?
If seeking internet records:
• Proof of preservation request(s)?
• Sufficient information to satisfy "probable cause" (for content records from the US)?
Check whether assistance can be obtained informally before proceeding
2 ACKNOWLEDGE RECEIPT of MLA QUESTIONNAIRE
and provide officer contact details. Liaise if require further information.
3 DRAFT the MAR
Always start with a template
If seeking internet records: include account identifiers for each account requested and a specific date range
4 SEND COPY
Send draft MAR to instructing agency for confirmation it covers what they require
5 REVIEW DRAFT
Consider asking recipient country's central authority to review a draft of the request via email to ensure it is sufficient for their purposes
6 HAVE MAR SIGNED
by appropriate authority / delegate
7 TRANSLATE
If applicable, translate MAR into recipient country's language
8 TRANSMIT
Transmit to recipient country and provide a copy to instructing agency

4.1 Drafting a MAR

The preferable way of formatting a MAR is by way of letter with subheadings. It is important to provide as much relevant detail as possible.

A template for drafting a MARt is available on the PILON website

Suggested MAR Format

Purpose

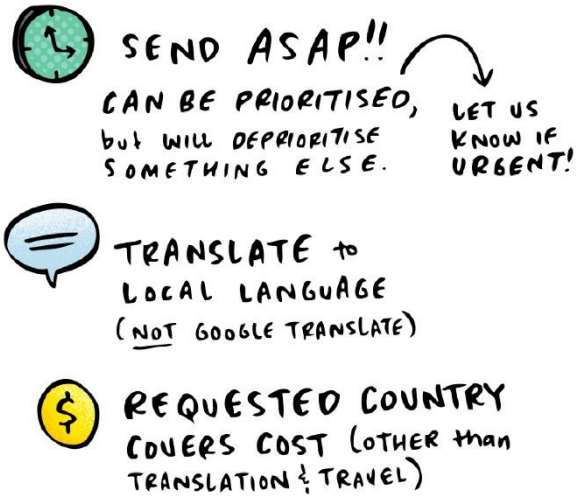
Briefly outline the purpose of MAR (i.e. the offence and type of assistance sought).

Current Situation

Provide a short statement on the current status of the matter (i.e. investigation stage, charges laid, relevant court dates). It is important to indicate any time constraints in relation to providing the assistance.

Facts

Provide a full summary of the background, investigation and evidence of the alleged offending. You do not need to include actual evidence with the request. However, it would be useful if you summarised the facts in narrative form. There should be sufficient detail that it is clear to anyone reading the request what has occurred and what the allegations are. The facts presented in the MAR need to be relevant to the specific matter - think about the information that the foreign country needs in order to provide the requested assistance and consider whether any information provided by the instructing agency could be omitted. It is important to be as clear and simple as possible and avoid technical jargon where possible.



You should need to explain how law enforcement has learned about the facts you are providing (e.g. whether evidence was obtained by search warrant, or through witness interviews or expert analysis).

Where the MAR will require the exercise of coercive powers, sufficient information will be required for the recipient country to obtain any necessary court orders. For example, if needing to meet the legal threshold of 'probable cause' in the US in order for a court to issue a warrant, ensure you provide information to satisfy that threshold.

Offence

Indicate the offence that is being investigated or prosecuted and the maximum penalty for that offence. It is helpful to identify how the evidence is required from the recipient country to establish a particular aspect or element of the offence.

Include a copy of the offence provisions from your legislation as an annexure to the MAR. Where the relevant penalty is contained or explained in separate provision/s, also attach these.

Subject of Investigation or Prosecution

Provide details of the suspect or accused (i.e. full name, date of birth, nationality, current location, passport number, any known alias).

Assistance Sought

This is the most vital part of the request. Clearly outline the particular assistance that is required and how the evidence sought is relevant to the investigation or prosecution. If the request involves contacting, serving process, or interviewing people in the recipient Country_Be sure to include their contact details, a copy of any information to be given to them, and/or a list of any questions to be asked.

Further information on commonly sought types of assistance can be found in 3.3.

Clearly set out any special requirements of the requesting country (e.g. form of statement, particular signature or jurat requirements). It is helpful to provide templates (e.g. template business records affidavit) to the recipient country for witnesses, company employees and law enforcement/government officials showing the formal requirements for affidavits to be admissible in your courts. These templates can be annexures to the MAR.

Procedural Requirements

State what action is required by the recipient country once they have obtained the information sought. You must consider who you need statements/affidavits from to accompany any documents obtained, and any particular requirements. It is recommended including a template affidavit with your MAR showing the formal requirements for affidavits to be admissible in your courts. The template affidavits can usually be adapted for most MARs.

Transmission of Material Obtained

Include instructions on where and how the material obtained should be sent. Generally, the material will be couriered to the Central Authority of the recipient country and will then be forwarded to the requesting country.

Where material comprises CSAM, it may be a prohibited import under your country's law. In this case, the requesting country may need to seek an importation certificate and send this to the recipient Country before the recipient country sends the material to the requesting country.

Confidentiality

Subject to the requirements of the requesting country's law, it may be appropriate to ask that the MAR and any information obtained pursuant to it be kept confidential, other than from appropriate law enforcement agencies. Specify if there are particular reasons for confidentiality. Note there are specific confidentiality requirements for MARs made to the US (See US country profile in Chapter 6 for further information).

Urgency

If you are working to any particular court date or other deadline, it is important that you say so. Requests for urgency should be saved for genuinely urgent matters. Central Authorities receive a large number of MARs and can usually only prioritise genuinely urgent requests (e.g. the trial is about to start or when an investigation will be jeopardized if evidence is not obtained quickly). It is worth noting that many countries do not consider 'urgency' to include where the requesting country has failed to make the request in a timely manner.

Assurances

Most countries require a range of assurances from a requesting country regarding the purpose of the evidence obtained from the request. You will likely need to provide an assurance that the evidence will only be used for the purposes of the criminal prosecution and investigation to which the request relates. A range of other assurances are also standard and may be set out in your legislation and may be set out in the relevant treaty obligations which govern the request. The recipient country will let you know if they require any further assurances under their domestic law or a treaty.

Use of Information

Any information obtained from another country can usually only be used for the purpose stated in the request, unless permission is given for it to be used for another purpose. In other words, if the information is also relevant to a different criminal matter, permission will need to be given by the recipient country for the information to be used for that other matter.

Reciprocity

You should provide an assurance that your country could provide assistance of the type you are requesting if the recipient country made a similar request to your country. Before providing that assurance, consider whether you really can provide the type of assistance you are requesting. If there are gaps in your legislation meaning you cannot provide certain sorts of assistance (e.g. surveillance warrants) you will not be able to provide an assurance of reciprocity and it may mean the recipient country cannot provide this type of assistance to you. Most countries require an assurance of reciprocity before they will agree to provide assistance.

Contact Details

State the contact details of your country's Central Authority and the instructing agency contact. While correspondence from the recipient Country_About the MAR should generally be addressed to your Central Authority to ensure MLA processes are properly adhered to, it is also often helpful for the recipient country to be able to liaise directly with the requesting agency's contacts when making arrangements about operational matters.

Where you have already had direct contact with an official or relevant person (such as a foreign witness) in the recipient country, it is often helpful to identify them as being someone who can provide the recipient Central Authority with information or assistance about the matter.

4.2 Sending the MAR and Related Procedural Matters

Send the MAR with a short cover letter to the relevant Central Authority. It is good practice to simultaneously send a copy of the MAR to your instructing agency for their records, so they are aware the MAR is now with the recipient country for processing.

WHERE to SEND MARs

MARs are sent to the Central Authority of the foreign country. Some countries may require MARs to be sent through diplomatic channels though most will accept MARs by email. You should check country specific requirements or preferences with the relevant Central Authority.

Contact details can be found in Chapter 6, on the relevant Central Authority website or on the UNODC Online Directory of Central Authorities (available to central authorities and government agencies with a user account).

WHEN to SEND MARs

Send your request as soon as possible! Depending on the nature of the request and the recipient country, obtaining a response may take many months and requests for electronic evidence from the US can often take up to a year or more. While you can request urgency, this should be reserved for the most serious and genuinely pressing cases.

You can often seek comments on a draft MAR from the recipient country's Central Authority before sending through the final version – in fact, most central authorities strongly encourage this! This is particularly the case for requests seeking the enforcement of proceeds of crime action. Certain countries, including Australia, can provide preliminary advice on a foreign restraint or forfeiture order to determine whether it can be enforced. Doing this will often avoid a lot of back and forth asking questions or seeking clarification on details and will save time.

The recipient country will contact you with any queries once they have received the request.

TRANSLATIONS

The requesting country is required to translate the MAR into the language of the recipient country. Check with the recipient country in advance to confirm what languages they will accept. You will also need to clarify which domestic agency is paying for the translation (i.e. the instructing agency, the Central Authority or another agency), noting it should be done by an official translator.

Generally, the recipient Country_Bears the costs of responding to a request. There are some associated costs the requesting country will cover, in particular any costs of translating the request into the language of the recipient country (if required), and associated costs for a witness to travel to the recipient country to give evidence. Bilateral MA treaties often prescribe how the costs of executing the request are to be apportioned between the requesting and recipient countries.

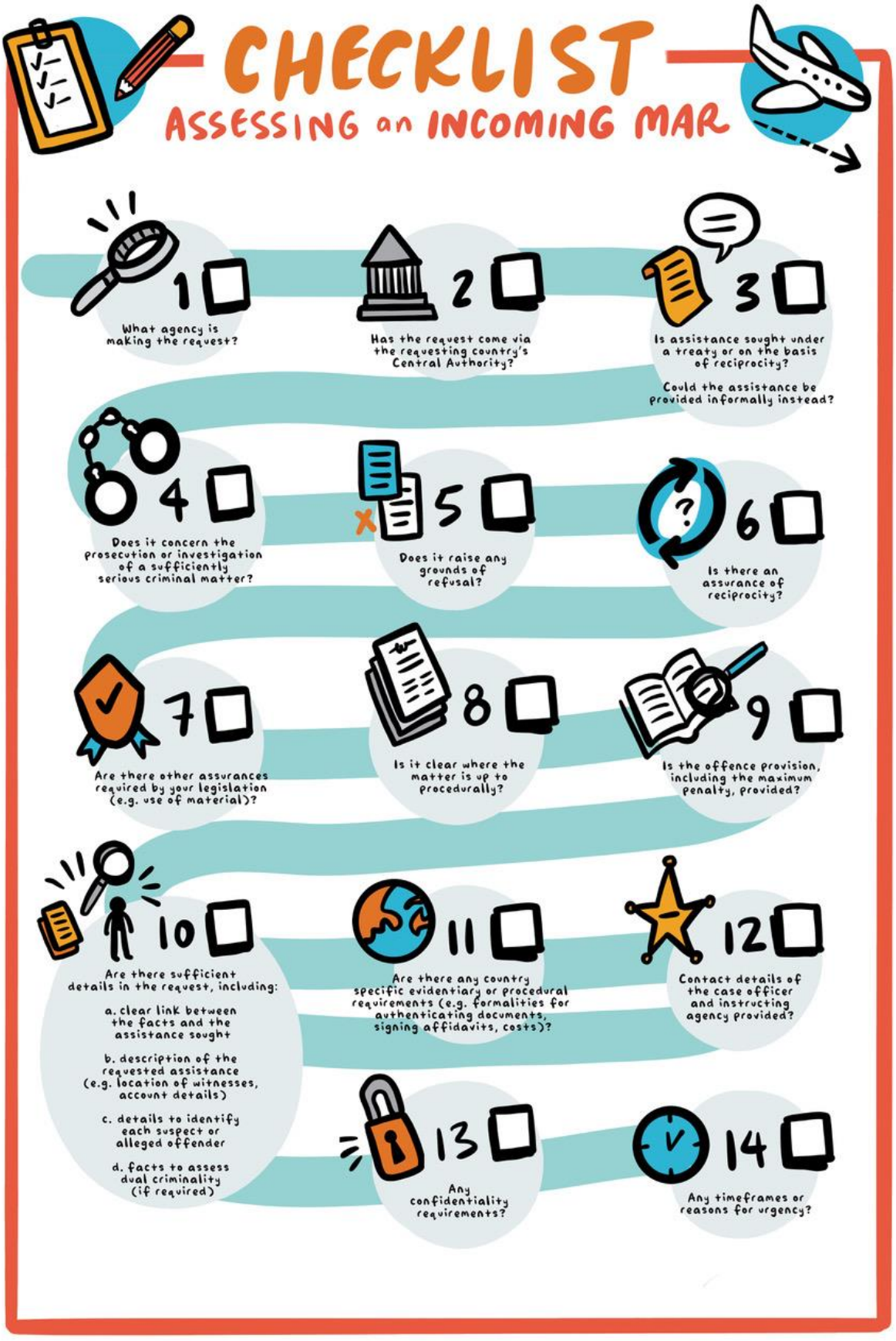
4.3 Material Obtained from Recipient Country

Once the recipient country has actioned the MAR it will have material to send to the requesting country Central Authority. On receipt of the material, you should assess whether the material is in a format that will be admissible to your courts.

Some things to think about in assessing the material are:

- does the material obtained include material that was not requested in the MAR?
- are translations needed?
- does the material need to be certified? (i.e. certify or authenticate that the evidentiary material was obtained lawfully pursuant to a MAR)
- if certification or sealing of the material is requested, are there any internal requirements in order for the material to be admissible?

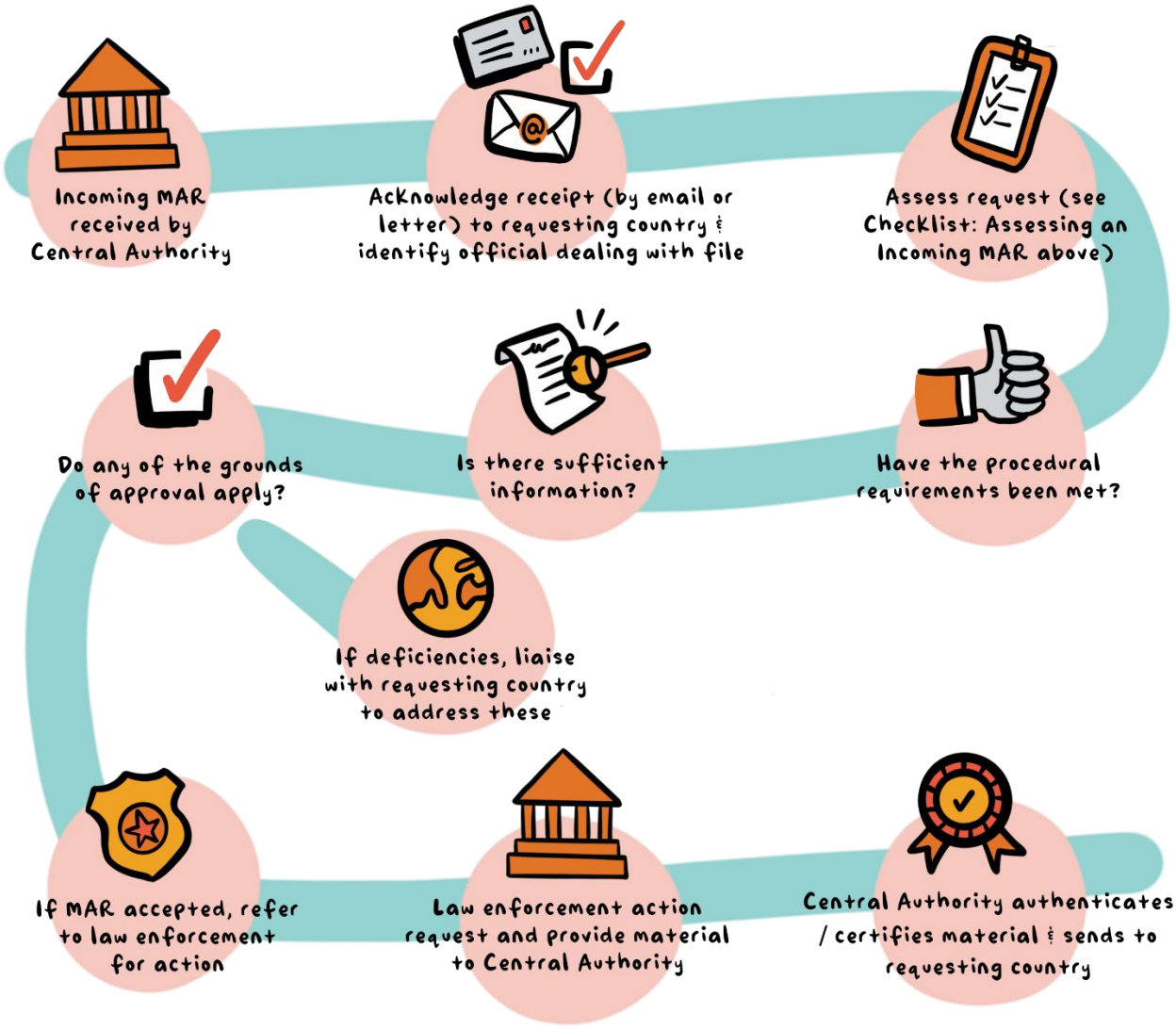
CHAPTER 5 – Incoming MAR



5.1 Receiving an Incoming MAR

As the recipient country, it is important to send a reply to the requesting country soon after receiving their MAR to acknowledge receipt and provide contact details for the legal officer within the Central Authority dealing with the file.

The following flowchart sets out the general process that a recipient country follows after receiving a MAR from another country seeking formal assistance.



5.2 Assessing an Incoming MAR

Once an incoming MAR is received it should be assessed for compliance with your country's MLA legislation. Each MAR should be scrutinised and then accepted or refused on a case-by-case basis. Your country's MLA legislation is likely to contain details on what an incoming MAR must include.

As the legal officer dealing with the file, you may wish to prepare a memorandum for your decision-maker setting out your assessment and make a recommendation of whether the MAR should be accepted or refused. The information below sets out some of the key factors you should consider and include in the memorandum. In addition, the checklist at the beginning of this chapter is a useful tool to assist officers in this assessment process and to ascertain whether all the necessary information has been provided.

Procedural Requirements

During the course of assessing the request, you may notice areas where the request is clearly deficient. If further information is required before a decision can be made, liaise with the requesting country to obtain the necessary information. This can be done by letter or email depending on your relationship with the requesting country and how deficient the request is.

Common deficiencies in requests include:

- has not come from the Central Authority
- does not include a summary of all relevant facts/the alleged offending
- does not include copies of the legal provisions that cover the offence and penalty
- does not clearly detail the nature of the assistance sought
- does not include a statement as to any specific or special confidentiality requirements
- does not detail any special requirements with respect to authenticating documents to be sent to the requesting country
- does not detail the time within which the country requires the assistance sought to be provided
- does not include appropriate assurances from the Central Authority

Procedural Requirements

Consider and briefly address the procedural requirements as set out in your MACMA. In assessing whether your country can provide the requested assistance, you may need to consider factors such as:

- does your MACMA specify which foreign countries your country may accept a MAR from? (e.g. the MACMA may specify that MARs can only be accepted from prescribed foreign countries, bilateral treaties or countries party to a bilateral or specified multilateral conventions)
- is there an assurance of reciprocity given by the requesting country that it will entertain a similar request by your country for assistance in criminal matters
- the seriousness of the offence to which the MAR relates (you will often need to assess whether the offence meets a threshold of being a 'serious offence' determined by the maximum penalty), and
- the object of your legislation.

Your MACMA may also require certain information be included in an incoming MAR. For example:

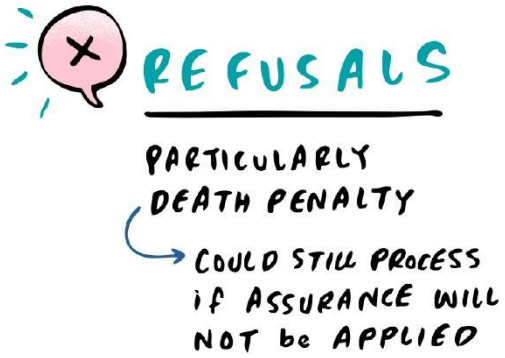
- who the MAR should be made to (usually the Central Authority of your country)
- the purpose of the MARS and the nature of the assistance being sought (See more at 3.3)
- the identity of the person, agency, or authority that initiated the MAR, and
- the basis on which the foreign country is making the MAR (i.e. bilateral MA treaty or multilateral convention).

Your MACMA may also require that the MAR must be accompanied by:

- a certificate from the Central Authority of the foreign country that the request is made in respect of a criminal matter
- a description of the nature of the criminal matter and a statement setting out a summary of facts and the relevant law
- details of the procedure to be followed in giving effect to the request, including details of the form of any information to be supplied
- an explanation of any confidentiality requirements
- an explanation of any time constraints
- if the request involves a person travelling from your country to the foreign country, details of the proposed practicalities (e.g. allowances, accommodation etc.), and
- any other information required to be included with the request under a treaty or other arrangement between your country and the foreign country.

Strict compliance with these requirements may not be a pre-requisite to agreeing to accept a MAR, so you may need to use your judgement in deciding whether you will insist on a particular factor or not. Regardless, you should ensure that any non-compliance with the requirements in your MACMA is identified and briefly addressed in your memorandum to the decision-maker.

Grounds for Refusal



The grounds for refusing a MAR will be set out in your legislation and are often divided into two categories: mandatory and discretionary. If a request is refused, in whole or in part, the foreign country must be formally notified and provided with reasons. Alternatively, if the decision-maker is concerned that the matter may contravene a ground/s for refusal, but does not want to refuse the request, it may be possible to grant the request subject to conditions.

The following are common mandatory or discretionary grounds for refusal:

- It previously referred to political partoes which is not a good example
- Discrimination: requests involving prejudice to a person on account of their colour, race, ethnic origin, sex, religion, nationality or political opinions
- Double jeopardy: requests involving previous acquittal, conviction, pardon or punishment for the same offence, act or omission
- Military offence: requests involving an offence that would amount to an offence against military law but not also an offence against ordinary criminal law
- Prejudice to sovereignty, security, or national interests: requests that, if granted, would prejudice the sovereignty, security, or national interests of your country
- Unlawful or unauthorised: requests for assistance of a kind that cannot be given under the Act or would require action that could not lawfully be taken
- Dual criminality: the request relates to conduct that, if it had occurred in your country, would not have constituted an offence against your country's law
- Time barred: the request relates to proceedings involving forfeiture or restraint of property or the prosecution or punishment of a person, which could not have been brought in similar circumstances in your country due to a statutory time limit or any other reason
- Death penalty: the request relates to the prosecution or punishment of a person facing the death penalty in the requesting country. You may wish to consider whether your country could consent to the request if the foreign country satisfies your decision-maker that the death penalty will not be imposed or, if it is or was imposed, will not be carried out
- Where the provision of assistance could prejudice a current investigation or proceedings in a criminal matter or a proceeds of crime proceeding in your country
- Where the provision of assistance would be likely to prejudice the safety of any person (in your country or not), and/or
- Where the provision of assistance would impose an excessive burden on your country (e.g. in terms of resources, financial costs) or relates to a matter that is trivial in nature.

Unable to Assist

In some circumstances the recipient country will not be able to provide the assistance sought in a MAR. This could include situations where:

- witness details cannot be confirmed, or the witness is not located in the jurisdiction
- person does not wish to provide a voluntary witness statement or voluntarily attend court to give evidence
- insufficient time has been given for the service of documents, and/or

- the relevant court date has passed by the time the MAR was received.

In these cases, you should advise the requesting country that you are unable to provide the assistance sought. This can be done by writing a letter to the authorities from the requesting country explaining the situation, briefly outlining why you are able to assist in the particular circumstances.

5.3 Referring the Request to Law Enforcement

Refer the request to the authority that is responsible for providing assistance, usually the police. You may continue to supervise the progress of the request and liaise between the police and the requesting country with any updates or questions.

5.4 Providing Material Received in Response to MAR

In most cases any documentation obtained pursuant to the request will be returned by law enforcement to you at the Central Authority office so you can provide the material to the requesting country.

Before forwarding the material to the requesting country, it is good practice to check the documentation to ensure it complies with any evidentiary or procedural requirement of the requesting country. This may include a requirement for your Central Authority to certify or authenticate that the evidentiary material was obtained lawfully pursuant to a MAR. The requesting country may even specify a particular form of words for the recipient country's Central Authority to attach to the material when sending it.

Depending on your MLA legislation, you may need to prepare an authorization before releasing the material to the requesting country.

If the material received includes child exploitation material, you may need to follow particular handling procedures acknowledging the sensitivity of such material.

CHAPTER 6 – Country Profiles

6.1 - PILON Member

AUSTRALIA

CENTRAL AUTHORITY

International Crime Cooperation Central Authority
Attorney-General's Department

3-5 National Circuit
BARTON ACT 2600
AUSTRALIA

P. +61 2 6141 6666
F. +61 2 6141 5457

ICCCA@ag.gov.au

ag.gov.au

LEGISLATION

Mutual Assistance in Criminal Matters Act 1987

INCOMING MA REQUESTS

Basis for MARs:	Treaty (bilateral or multilateral), letters rogatory, any foreign country on the basis of reciprocity
Method of receiving MARs:	By email preferred. Will also accept hardcopy or through diplomatic channels (least preferred)
Requirements:	See s11 MACMA
Definition of 'serious offence':	Maximum penalty for an offence which is death, imprisonment exceeding 12 months or fine exceeding 300 penalty units (fine exceeding AUD$66,600)
Assistance can provide:	• Voluntary assistance (e.g. voluntary witness statement) • Taking of evidence or production of documents (s13) • Providing material lawfully obtained (s13A) • Search and seizure (s15) • Stored communications (s15B) • Surveillance devices (s15CA) • Telecommunications data (s15D) • Arranging for persons in custody to give evidence or assist investigations (ss26-28) • Forensic procedures (ss28B, 28C) • Proceeds of crime actions (Part VI, Division 2)

Grounds of refusal:	See s8 MACMA
	• Mandatory grounds:
	  ○ political offence
	  ○ offence on account of rate, sex, religion, nationality or political opinions
	  ○ military offence
	  ○ granting of the request would prejudice the sovereignty, security or national interest of Australia or the essential interests of a State or Territory; or
	  ○ double jeopardy
	  ○ death penalty may be imposed (unless special circumstances)
	• Discretionary grounds:
	  ○ dual criminality
	  ○ double jeopardy
	  ○ could prejudice investigation/proceeding in relation to domestic criminal matter
	  ○ would, or would be likely to, prejudice the safety of any person (whether in or outside Australia)
	  ○ would impose excessive burden on the resources of the Commonwealth/State/Territory
	  ○ appropriate in circumstances of the case that assistance not be granted

Other:	• Assistance may be subject to conditions (s9) • Restriction on use of information (s43B) • Australia is obliged to maintain confidentiality of incoming requests (s43C)

OUTGOING MA REQUESTS

Assistance can request:	See s10 MACMA and dependent on laws of recipient foreign country • Taking of evidence and production of documents or other articles (s12) • Search and seizure (s14) • Surveillance devices (s15C) • Persons in custody to give evidence or assist in investigations (ss16-25A) • Forensic procedures (s28A) • Proceeds of crime actions (ss32,33)
Admissibility requirements:	Foreign Evidence Act 1994 (Commonwealth) (FEA) The FEA also applies to proceedings in any Australian court that is a criminal proceeding for an offence against the Commonwealth or against the law of a State or Territory, a related civil proceeding, or a proceeding under a proceeds of crime law.

COOK ISLANDS

CENTRAL AUTHORITY

Crown Law Office

PO Box 494
Avarua, Rarotonga
COOK ISLANDS

P. +682 29337
F. +682 20839

stuart.baker@cookislands.gov.ck

LEGISLATION

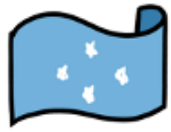
Mutual Assistance in Criminal Matters Act 2003 (amended 2003, 2004 & 2017)

INCOMING MA REQUESTS

Basis for MARs:	Cook Islands can provide for assistance without treaty, agreement or other arrangements between CI and foreign country. The kind of assistance to be provided is not limited to that provided in MACMA (s4).
Method of receiving MARs:	Diplomatic channels, followed by direct discussions with requesting country by email
Requirements:	See s7 MACMA for assistance generally, s11 for taking evidence, s18 for search and seizure, s30 for giving evidence in foreign countries, s38 requests for enforcement of foreign orders
Definition of 'serious offence':	Offence punishable by imprisonment for not less than 12 months or fine more than $5,000
Assistance can provide:	• voluntary assistance (e.g. voluntary witness statement) • taking evidence and production of documents or other articles (ss11-16) • search and seizure (ss18-20) • arrangements for persons to give evidence or assist investigations (ss30-33) • proceeds of crime actions (ss38-46)
Grounds of refusal:	Discretionary grounds (s9): • prejudice the sovereignty, security or other essential public interest of the Cook Islands • postpone request if granting the request immediately would be likely to prejudice domestic investigation/proceedings • cannot refuse or postpose request solely on grounds would involve breach of secrecy or confidentiality obligation, or requirements relating to one or more financial institutions, or the relevant offence involves fiscal matters • Note also that, though not a ground of refusal, there is no obligation to consider a request until the requirements of s7(2) are complied with (see s7(3))
Other:	• assistance may be provided in whole or part and subject to conditions (s8) • dual criminality is mandatory and is conduct-based (s3) • requests must not be intentionally disclosed (s61)

OUTGOING MA REQUESTS

Assistance can request:	See s6 MACMA and dependent on laws of recipient foreign country • taking evidence and production of documents or other articles (s10) • search and seizure (s17) • arrangements for persons to give evidence or assist investigations (ss21-29) • proceeds of crime actions (ss36-37)
Admissibility requirements:	See Part 9 (ss49-57) MACMA



FEDERATED STATES OF MICRONESIA

CENTRAL AUTHORITY

Secretary
Department of Justice

PS 105 Palikir, Pohnpei
FM 96941
FEDERATED STATES
OF MICRONESIA

P. +691 320 2644/2608
F. +691 320 2234

jrg.fsm@gmail.com

doj.gov.fm/justice/fsm_doj

LEGISLATION

Title 12 Criminal Procedure, Code of the Federated States of Micronesia, Chapter 17 Mutual Assistance in Criminal Matters (ss1701-1719)

INCOMING MA REQUESTS

Basis for MARs:	Treaty (bilateral or multilateral), letters rogatory or any foreign country on the basis of reciprocity
Method of receiving MARs:	Email, hardcopy by post, or by diplomatic channels
Requirements:	See s1708 of the Code
Definition of 'serious offence':	Offense punishable by imprisonment for more than one year
Assistance can provide:	• evidence gathering order or a search warrant (s1709) • transfer order of detained persons (s1710) • restraining order (s1713) • enforcement of confiscation order (s1714) • proceeds of crime actions (s1715)
Grounds of refusal:	Discretionary grounds of refusal (s1705) • prejudice the sovereignty, security or other essential public interest of the FSM • postpone request if granting the request immediately would be likely to prejudice domestic investigation/proceedings
Other:	• assistance may be provided in whole or part and subject to conditions (s1705) • Supreme Court must be satisfied that there is probable cause to believe that a serious offence against the laws of the foreign country has been committed and that evidence relating to that offence may be found in the FSM or given by a person believed to be in the FSM • limits on use of information obtained and provides safeguards against inappropriate or unofficial use (s1718) • requests must not be disclosed unless authorised by the Secretary, or necessary to execute request

OUTGOING MA REQUESTS

Assistance can request:	See s1707 and dependent on laws of recipient foreign country • taking of evidence and production of documents or other articles • search and seizure • surveillance devices • persons in custody to give evidence or assist in investigations • proceeds of crime actions
Admissibility requirements:	FSM Rules of Evidence 1991

FIJI

CENTRAL AUTHORITY

Office of the Attorney-General

Level 7, Suvavou House
Victoria Parade, P.O. Box 2213
Government Buildings Suva, FIJI

P. +679 3309 866
F. +679 3310 807

sgoffice@govnet.gov.fj

LEGISLATION

Mutual Assistance in Criminal Matters Act 1997

INCOMING MA REQUESTS

Basis for MARs:	Any foreign country (s5)
Method of receiving MARs:	In writing (e-mail or hardcopy by post). Not necessary to send through diplomatic channels.
Requirements:	A request must include the following information (s9): • name of the central authority; • description of nature of criminal matter • statement setting out a summary of the relevant facts and laws; • description of the purpose of the request and nature of assistance sought; and • other useful information that may assist with the request.
Definition of 'serious offence':	Offence for which maximum penalty is death or imprisonment for not less than 6 months or a fine of not less than $500
Assistance can provide:	• taking evidence and production of documents or other articles (s11) • search and seizure (s13) • persons to give evidence or assist investigations (ss23-25) • proceeds of crime actions (ss31-34)
Grounds of refusal:	Discretionary grounds of refusal (s6): • prejudice the national, essential or public interests of Fiji • result in manifest unfairness or a denial of human rights • it is otherwise appropriate, in all the circumstance of the case, that the assistance requested should not be granted
Other:	• assistance may be subject to conditions (s7) • restriction on use of information (s49) • requests must not be intentionally disclosed unless necessary in performance of duties or Attorney-General has approved disclosure (s50)

OUTGOING MA REQUESTS

Assistance can request:	See s8 and dependent on laws of recipient foreign country • taking evidence and production of documents or other articles (s10) • search and seizure (s12) • persons to give evidence or assist investigations (s14-22) • proceeds of crime actions (ss29-30)
Admissibility requirements:	See Part 8 (ss37-46)

KIRIBATI

CENTRAL AUTHORITY

Attorney-Generals Office

P.O. Box 62
Bairiki, Tarawa
KIRIBATI

P. +686 21242
F. +686 21025

pauline@legal.gov.ki

legal.gov.ki

LEGISLATION

Mutual Assistance in Criminal Matters Act 2003

INCOMING MA REQUESTS

Basis for MARs:	Treaty (bilateral or multilateral), letters rogatory or any foreign country on the basis of reciprocity
Method of receiving MARs:	Email, hardcopy by post or diplomatic channels
Requirements:	See s8 MACMA
Definition of 'serious offence':	Offence for which maximum penalty is imprisonment for 12 months or longer
Assistance can provide:	• voluntary assistance (e.g. voluntary witness statement) • taking evidence and production of documents or other articles (ss14-19) • assistance for search and seizure (ss21-23) • arrangements for persons in custody to give evidence or assist investigation (ss32-35) • assistance regarding proceeds of crime (ss41-49) • any other matters which we can provide assistance to although not stated in the law
Grounds of refusal:	Mandatory grounds: • political nature, contravene Chapter II of the Constitution (protection of fundamental rights and freedoms of the individual), made in support of discrimination on racial, sexual, religious, national or political grounds, prejudice the sovereignty, security or national interest of Kiribati, or double jeopardy (s10) • death penalty, unless special circumstances (s11) Discretionary grounds: (s12) • prejudice law enforcement or personal safety in Kiribati • compromise human rights • impose an excessive burden on Kiribati's resources • if assistance would not be appropriate
Other:	• assistance may be subject to conditions (s9) • dual criminality is a discretionary ground for refusal • limits for the use of information obtained under the Act and provides safeguards against inappropriate or unofficial use • if the AG makes request, must tell the Minister for Foreign Affairs, though failure will not invalidate the request (s6)

OUTGOING MA REQUESTS

Assistance can request:	See ss6 and 7 MACMA and dependent on laws of recipient foreign country • taking evidence and production of documents or other articles (s13) • assistance for search and seizure (s20) • arrangements for persons in custody to give evidence or assist investigation (ss24-31) • assistance regarding proceeds of crime (ss39-40)
Admissibility requirements:	Documentary evidence: Usually the person who makes the document will be invited to give evidence in court; however, the Court may also allow documents certified by foreign courts; JPs or Magistrates to be admitted in court. See also Evidence Act 2003

NAURU

CENTRAL AUTHORITY

Minister for Justice
Department of Justice and Border Control

Government Office
Yaren District
Republic of Nauru

P. +674 557 3505

jjjjudit4@gmail.com

LEGISLATION

Mutual Assistance in Criminal Matters Act 2004

INCOMING MA REQUESTS

Basis for MARs:	Treaty (bilateral or multilateral), letters rogatory or any foreign country on the basis of reciprocity
Method of receiving MARs:	Through diplomatic channels is preferred. Will be accepted by email, or in writing (s7(2))
Requirements:	See s7 MACMA
Definition of 'serious offence':	Offence punishable by imprisonment for not less than 12 months or imposition of fine of more than $5,000 – (as defined in the Proceeds of Crime Act 2004)
Assistance can provide:	• taking evidence and production of documents or other articles (ss11-16) • search and seizure (ss18-20) • arrangements for persons in custody to give evidence or assist investigation (ss27-33) • assistance regarding proceeds of crime (ss38-46)
Grounds of refusal:	• would likely prejudice the sovereignty, security or other essential public interest of Nauru (s9a) • may delay if granting the request immediately would be likely to prejudice the conduct of an investigation or proceeding in Nauru (s9(b))
Other:	• assistance may be subject to conditions (s8) • limits for the use of information obtained under the Act and provides safeguards against inappropriate or unofficial use (s60) • requests for international assistance must not be disclosed (s61)

OUTGOING MA REQUESTS

Assistance can request:	See s6 MACMA and dependent on laws of recipient foreign country • taking evidence and production of documents or other articles (s10) • search and seizure (s17) • arrangements for persons in custody to give evidence or assist investigation (ss21-26) • assistance regarding proceeds of crime (ss36-37)
Admissibility requirements:	See Part 9 MACMA (ss49-57)

NEW ZEALAND

CENTRAL AUTHORITY

Attorney-General
Crown Law Office Te Tari Ture o te Karauna
Direct queries to Manager of Mutual Assistance

PO Box 2858
Wellington 6011
NEW ZEALAND

P. +64 4 472 1719

criminal@crownlaw.govt.nz

crownlaw.govt.nz

LEGISLATION

Mutual Assistance in Criminal Matters Act 1992

INCOMING MA REQUESTS

Basis for MARs:	Bilateral treaty, prescribed foreign country, pursuant to a relevant convention, and any country (see s24)
Method of receiving MARs:	Email followed by hard copy. Diplomatic channels are also acceptable
Requirements:	See s26 MACMA
Definition of 'serious offence':	Not applicable
Assistance can provide:	• voluntary assistance (e.g. voluntary witness statement) • locating or identifying persons (s30) • taking evidence in court or production of documents or other articles (ss31-36) • arranging attendance of persons (ss37-42) • serving documents (ss51-53) • search and seizure (ss43-50) • proceeds of crime actions (ss54-62)
Grounds of refusal:	See s27 MACMA (some grounds of refusal are mandatory and some discretionary) • political character • prosecuting, punishing, or otherwise causing prejudice to a person on account of the person's colour, race, ethnic origin, sex, religion, nationality, or political opinions • double jeopardy • would have constituted an offence under the military law of New Zealand but not also under the ordinary criminal law of New Zealand • would prejudice the sovereignty, security, or national interests of New Zealand; or • if request for attendance and the person to whom the request relates does not consent to transfer • the assistance cannot be given under MACMA, or would require steps to be taken for its implementation that could not be lawfully taken. • conduct would not have constituted an offence or significant criminal activity against New Zealand law • could not have been the subject of proceedings of that kind because of lapse of time or for any other reason • death penalty (and unable to sufficiently assure the Attorney-General that the person will not be sentenced to death; or if that sentence is or has been imposed, it will not be carried out; or certain other matters if request relates to a prisoner in New Zealand • assistance requested could prejudice a criminal investigation or criminal proceeding in New Zealand or certain other types of proceedings • the assistance would prejudice, or would be likely to prejudice, the safety of any person (whether that person is in New Zealand or not) • the assistance would impose an excessive burden on the resources of New Zealand • relates to a matter that is trivial in nature (subject to further consultation with requesting country) • the request does not comply with the requirements of section 26 (subject to further consultation with requesting country)
Other:	• Assistance may be provided subject to conditions (s29)

OUTGOING MA REQUESTS

Assistance can request:	See Part 2 MACMA and dependent on laws of recipient foreign country • locating or identifying persons (s9) • taking evidence or production of documents or other articles (ss10, 11) • arranging attendance of persons (ss12-18) • serving documents (s19) • search and seizure (ss20) • proceeds of crime actions (ss21-22)
Admissibility requirements:	• documentary records must be produced in affidavit form, attached to a sworn statement • procedural details will be provided in the request together with precedent cover affidavits

NIUE

CENTRAL AUTHORITY

Attorney-General,
Crown Law Office

PO Box 40
Fale Fono, Alofi
NIUE

P. +683 4200
F. +683 4206

Niue.CLO@mail.gov.nu

LEGISLATION

Mutual Assistance in Criminal Matters Act 1998

INCOMING MA REQUESTS

Basis for MARs:	Treaty (noting no such treaties have been entered into to date), letters rogatory (noting no such letters have been issued to date) or any foreign country on the basis of reciprocity
Method of receiving MARs:	By email preferred, though will accept hardcopy through diplomatic channels
Requirements:	See s10 MACMA
Definition of 'serious offence':	Offence the maximum penalty for which is death, or imprisonment for not less than 12 months
Assistance can provide:	• voluntary assistance (e.g. voluntary witness statement) • identifying and locating person (ss10B) • taking evidence and production of documents or other articles (ss11, 12) • search and seizure (ss13,14) • arrangements for persons to give evidence or assist investigation (ss24-26) • assistance regarding proceeds of crime (Part 6, ss32-35A)
Grounds of refusal:	Discretionary grounds of refusal (s7): • prejudice the national, essential or public interests of Niue • result in manifest unfairness or denial of human rights • if appropriate, in all circumstances of the case, that the assistance requested should not be granted
Other:	• Assistance may be provided subject to conditions (s8) • Restriction on use of evidence (s50) • Requests not to be disclosed (S51) • The Act imposes limits for the use of information obtained under the Act and provides safeguards against inappropriate or unofficial use.

OUTGOING MA REQUESTS

Assistance can request:	See s9 MACMA and dependent on laws of recipient foreign country • Taking evidence and production of documents or other articles (s11) • Search and seizure (s13) • Arrangements for persons to give evidence or assist investigation (ss15-23) • Assistance regarding proceeds of crime (Part 6, ss30-31)
Admissibility requirements:	Part 8 MACMA

PALAU

CENTRAL AUTHORITY

Office of the Attorney-General

PO Box 1365
Koror 96940
PALAU

P. +680 488 2481/2487
F. +680 488 3329

agoffice@palaunet.com

Requests to
ministrymos.rop@gmail.com

palaugov.pw

LEGISLATION

Mutual Assistance in in Criminal Matters Act of 2001, 18 PNC §§ 1301 - 1333

INCOMING MA REQUESTS

Basis for MARs:	Treaty, letters rogatory or any foreign country on the basis of reciprocity
Method of receiving MARs:	See 18 PNC § 1311(b) Email preferred, hardcopy by post and diplomatic channels also accepted
Requirements:	See 18 PNC § 1314
Definition of 'serious offence':	An offence punishable by imprisonment for more than one year (see 18 PNC § 1302(p))
Assistance can provide:	• voluntary assistance (e.g. voluntary witness statement) • evidence-gathering order or search warrant (18 PNC § 1315) • arrangements for persons in custody to give evidence or assist investigation (18 PNC §§ 1316-18) • proceeds of crime actions (18 PNC §§ 1319-1322)
Grounds of refusal:	See 18 PNC § 1311 • would likely prejudice the national, essential or public interests of Palau • would likely prejudice the conduct of an investigation or proceeding in Palau • does not afford reciprocity to Palau or upon determination that refusal of such a request in the public interests of Palau
Other:	• limits for the use of information obtained under the Act and provides safeguards against inappropriate or unofficial use (18 PNC § 1332) • saving provision for other requests or assistance in criminal matters (18 PNC § 1312) • privilege for foreign documents (18 PNC § 1331)

OUTGOING MA REQUESTS

Assistance can request:	See 18 PNC § 1313 and dependent on laws of recipient foreign country • have evidence taken, or documents or other articles produced • search and seizure • proceeds of crime actions (i.e. locate, restrain or confiscate property) • arrangements for persons in custody to give evidence or assist investigation • provide any other form of assistance that involves or is likely to involve the exercise of a coercive power over a person or property; or • permit the presence of nominated persons during execution of request
Admissibility requirements:	Rules of Evidence for the Courts of the Republic of Palau (2014), ROP.R.Crim.P

PAPUA NEW GUINEA

CENTRAL AUTHORITY

Minister for Justice & Attorney General
Department of Justice & Attorney General
Queries to Director, Legal Policy & Governance Brand

P.O Box 591,
WAIGANI National
Capital District
PAPUA NEW GUINEA

P. +675 301 2956
F. +675 325 6304

international.cooperation
@justice.gov.pg

justice.gov.pg

LEGISLATION

Mutual Assistance in Criminal Matters Act of 2005 (amended 2015)

INCOMING MA REQUESTS

Basis for MARs:	Any foreign country on the basis of reciprocity Requests can be made relying on UNCAC however MACMA will take precedence
Method of receiving MARs:	Will accept by email, in hardcopy or by diplomatic channels
Requirements:	See s7 MACMA
Definition of 'serious offence':	Referred to as an 'indictable offence', meaning an offence that may be prosecuted on indictment and for which the maximum penalty is death or a term of imprisonment for at least 1 year.
Assistance can provide:	Provision of material lawfully obtained (s11) Assistance with taking evidence and production of documents or other articles (ss13-18) Assistance for search and seizure (ss20-22) Arrangements for persons to give evidence or assist investigation (ss32-35)) Proceeds of crime actions (ss41-49)
Grounds of refusal:	Mandatory grounds (s9): • Request relates to a political offence • Request made for purpose of prosecuting a person on account of the person's race, sex, religion, nationality or political opinion • Request relates to a military offence which would not also be an offence under the ordinary criminal law of PNG • Provision of the assistance would prejudice the sovereignty, security or national interest of PNG • Double jeopardy Discretionary grounds (s10): • dual criminality • passage of time • prejudice investigation or proceeding in PNG • prejudice safety of any person (whether in PNG or not) • result in manifest unfairness or denial of human rights • impose excessive burden on resources of PNG • appropriate in all circumstances of the case that assistance should not be granted
Other:	• Assistance may be provided subject to conditions (s8) • Restriction on use of information etc (s63) • Requests not to be disclosed (s64) • Constitutional rights protecting the freedom from arbitrary search and entry, right to privacy, right to freedom of movement, and unjust deprivation of property. • The Act provides for the Minister for Justice's discretion to refuse a request if the assistance could prejudice the constitutional rights of a defendant

OUTGOING MA REQUESTS

Assistance can request:	See s6 MACMA and dependent on laws of recipient foreign country • Assistance with taking evidence and production of documents or other articles (s12) • Assistance for search and seizure (s19) • Arrangements for persons to give evidence or assist investigation (ss24-31)) • Proceeds of crime actions (ss39-40)
Admissibility requirements:	See Part 9 (ss52-60) MACMA

REPUBLIC of MARSHALL ISLANDS

CENTRAL AUTHORITY

Office of the Attorney General

PO Box 890
Majuro 96960
MARSHALL ISLANDS

LEGISLATION

Mutual Assistance in Criminal Matters Act 2002 [32 MIRC Ch.4] (Amended 2011)

INCOMING MA REQUESTS

Requirements:	See s408 MACMA
Definition of 'serious offence':	Criminal offence punishable by imprisonment for term of more than one year
Assistance can provide:	Evidence gathering or search warrant (s410) Consensual transfer of detained persons to give evidence or assist in investigation/proceeding (s411-413) Proceeds of crime actions (ss414-417)
Grounds of refusal:	See s409 MACMA Mandatory grounds: • Request is likely to prejudice the sovereignty, security or other essential or public interest of the RMI or would result in manifest unfairness or a denial of human rights, or it is otherwise appropriate not to grant the request • Postpone Discretionary ground if the assistance would not be appropriate
Other:	Assistance may be provided subject to conditions (s409(1)(a)) Restriction on use of evidence and material obtained by MLA (s419)

OUTGOING MA REQUESTS

Assistance can request:	See s406 MACMA and dependent on laws of recipient foreign country • having evidence taken or documents or other articles produced in evidence • search and seizure • proceeds of crime action (restraints, confiscation etc) • transfer detained persons to RMI to assist in investigation/proceeding • any other form of assistance involving coercive power over person or property in foreign country • permit presence of person during execution of any request

SAMOA

CENTRAL AUTHORITY

Attorney-General's Office

PO Box 27
Apia
SAMOA

P. +685 20295/20296
F. +685 22 118

attorney.general@ag.gov.ws

ag.gov.ws

LEGISLATION

Mutual Assistance in Criminal Matters Act 2007

INCOMING MA REQUESTS

Basis for MARs:	Treaty (bilateral or multilateral), letters rogatory, any foreign country on the basis of reciprocity (diplomatic channels)
Method of receiving MARs:	Email correspondence, Letter/Hardcopy (including fax or email), or diplomatic channels
Requirements:	See section 22 – 23 of MACMA
Definition of 'serious offence':	Definition not in MACMA, however "serious offence" is defined in s2 Proceeds of Crime Act 2007(PCA) as follows: "serious offence" means an offence: against a law of Samoa that would constitute unlawful activity; or against the law of a foreign State that, if the relevant act or omission had occurred in Samoa, would be an offence that would constitute unlawful activity against any laws of Samoa. Note: "unlawful activity" is also defined in s2of the PCA to mean an act or omission that constitutes an offence and that is punishable, under the laws of Samoa, for a maximum period of not less than 12 months.
Assistance can provide:	• locating or identifying persons (s27) • obtaining evidence (ss28-29) • taking evidence and production of documents or other articles (s30) • search and seizure (ss39-45) • arrangements for persons to give evidence or assist investigation (ss 33-38) • serving documents (ss46-48) • proceeds of crime actions (ss49-57)
Grounds of refusal:	See s24 MACMA • likely to prejudice sovereignty, security or other public interest of Samoa or would be against the interest of justice • postponed if granting the request is likely to interfere with an ongoing Samoan investigation or proceeding Note: if a request by a foreign State for assistance is refused in whole or in part, the Attorney General shall give to the Competent Authority of the requesting foreign State the notice of refusal, together with the reasons for the refusal (s25 MACMA)
Other:	• assistance may be provided subject to conditions as the Attorney General determines in a particular case or class of case (s26) • restriction on use of evidence (s15) • requests not to be disclosed (s70 privilege for foreign documents)

OUTGOING MA REQUESTS

Assistance can request:	See Part 2 of MACMA and dependent on laws of recipient foreign country • locating or identifying persons (s8) • taking evidence and production of documents or other articles (ss 9, 10, 17) • arrangements for persons in custody to give evidence or assist investigation (s11-13) • serving documents (s16) • proceeds of crime actions (ss18-19)
Admissibility requirements:	Part V (ss59-68) MACMA

SOLOMON ISLANDS

CENTRAL AUTHORITY

Attorney-General. For queries and handling of requests refer to the Director of Public Prosecutions

Attorney-General's Chambers
PO Box G111
Honiara
SOLOMON ISLANDS

P. +AGC +677 28395/28396
F. AGC +677 28397

JMuria@attorneygeneral.gov.sb

Office of the Director of Public Prosecutions
PO Box 1216
Honiara
SOLOMON ISLANDS

P. ODPP +677 28958/28426/7
F. ODPP +677 28431

JMuria@attorneygeneral.gov.sb

LEGISLATION

Mutual Assistance in Criminal Matters Act 2002

INCOMING MA REQUESTS

ag.gov.ws

Basis for MARs:	As specified in MACMA, may include countries that have bilateral or multilateral relationships or MOUs with Solomon Island
Method of receiving MARs:	Email preferred though hardcopy and diplomatic channels also acceptable.
Requirements:	See s7 MACMA
Definition of 'serious offence':	Offence for which maximum penalty is imprisonment or other deprivation of liberty for a period of not less than 12 months, or more severe penalty including an offence against a law relating to taxation
Assistance can provide:	• Voluntary assistance (e.g. voluntary witness statement) • Evidence-gathering or search warrant (s8) • Proceeds of crime actions (ss12-15, 18) • Arrangements for persons to give evidence or assist investigation (ss9-11)
Grounds of refusal:	Discretionary grounds of refusal (s4): • likely to prejudice sovereignty, security or other essential public interest of Solomon Islands • after consulting with requesting agency, postpone if granting the request is likely to interfere with an ongoing Solomon Islands investigation or proceeding
Other:	• Assistance may be provided subject to conditions (s4(2)(a)) • Restriction on use of evidence and materials obtained by MLA (s17) • Requests not to be disclosed/ Privilege for foreign documents (s16)

OUTGOING MA REQUESTS

Assistance can request:	See s6 MACMA and dependent on laws of recipient foreign country • Voluntary taking evidence and production of documents or other articles (s6a) • Search and seizure (s6b) • Proceeds of crime actions (s6c-e) • Arrangements for persons to give evidence or assist investigation (s6f) • Any other form of assistance involving coercive power over person or property (s6g) • Permit presence of nominated persons during execution of request (s6h)

Admissibility requirements:	• Fulfilment of the requirements under the Evidence Act 2009
	  o Documents relating to court process (s106)
	  o Law reports of other countries (s112)
	  o Court discretion to allow a person to give evidence (s148)

TONGA

CENTRAL AUTHORITY

Attorney General
Attorney-General's Office

PO Box 85
Nuku'alofa,
Kingdom of Tonga

P. +676 24 055 / +676 24 007
F. +676 24 005

ag@crownlaw.gov.to

ago.gov.to

LEGISLATION

Mutual Assistance in Criminal Matters Act

INCOMING MA REQUESTS

Basis for MARs:	Reciprocity
Method of receiving MARs:	Email, hardcopy by post or diplomatic channels
Requirements:	See s7 MACMA
Definition of 'serious offence':	• offence for which maximum penalty is imprisonment or other deprivation of liberty for a period of not less than 12 months, or a more severe penalty; and • a law of a foreign State, in relation to acts or omissions which, had they occurred in Tonga, would have constituted an offence for which the maximum penalty is imprisonment or other deprivation of liberty for a period of not less than 12 months, or more severe penalty, including an offence of a purely fiscal character.
Assistance can provide:	• voluntary assistance (e.g. voluntary witness statement) • evidence gathering order or search warrant (s8) • consensual transfer of detained persons (s9) • persons in custody to give evidence or assist in investigation/proceeding (s10) • proceeds of crime actions (ss12-15)
Grounds of refusal:	Discretionary grounds of refusal (s4): • likely to prejudice sovereignty, security of Tonga or would otherwise be against the public interest • after consulting with requesting agency, postpone if granting the request is likely to prejudice the conduct of investigation or proceeding in Tonga Incomplete content of request for assistance (s7[2]): • a request for mutual assistance from a foreign State may be considered but shall not be granted by the Attorney General until the request complies with subsection (1).
Other:	• assistance may be provided subject to conditions (s4(2)(a)) • restriction on use of evidence and materials obtained by MLA (s17) • requests not to be disclosed/ Privilege for foreign documents (s16)

OUTGOING MA REQUESTS

Assistance can request:	See s6 MACMA and dependent on laws of the foreign country • have evidence taken, or documents or other articles produced • search and seizure • proceeds of crime actions • persons in custody to give evidence or assist in investigation/proceeding (s6g and 10) • provide any other form of assistance in any investigation commenced or proceeding instituted in Tonga, that involves or is likely to involve the exercise of a coercive power over a person or property believed to be in the foreign State • permit the presence of nominated persons during the execution of any request made under this Act.
Admissibility requirements:	Evidence Act Foreign Evidence Act Tonga Police Act (Part 4-6) Magistrate Act (Part IV)

TUVALU

CENTRAL AUTHORITY

Attorney-General
Office of the Attorney-General

Government Building
Vaiaku, Funafuti
TUVALU

P. +688 20 123
F. +688 20 817

agoffice@gov.tv

LEGISLATION

Mutual Assistance in Criminal Matters Act 2004

INCOMING MA REQUESTS

Basis for MARs:	Treaty (bilateral or multilateral), letters rogatory or any foreign country on the basis of reciprocity
Method of receiving MARs:	Email, hardcopy or diplomatic channels
Requirements:	See s8 MACMA
Definition of 'serious offence':	Offence for which maximum penalty is imprisonment for 12 months or longer (note same definition as in the Proceeds of Crime Act)
Assistance can provide:	• taking evidence and production of documents or other articles (ss14-19) • search and seizure (ss21-23) • arrangements for persons in custody to give evidence or assist investigation (s24) • proceeds of crime actions (ss41-49)
Grounds of refusal:	Mandatory grounds (s10): • political offence • prosecuting, punishing or otherwise causing prejudice to a person on account of the person's race, sex, religion, nationality or political opinions • providing the assistance would prejudice the sovereignty, security or national interest of Tuvalu • double jeopardy • death penalty, unless the Attorney-General considers that due to special circumstances, the request should be granted (s11) Discretionary grounds for refusal (s12): • Dual criminality • Lapse of time or any other reason • Could prejudice an investigation or proceeding in Tuvalu • Prejudice safety of any person (whether or not outside Tuvalu) • Result in manifest unfairness or a denial of human rights • Impose excessive burden on the resources of the Crown • Appropriate, in all the circumstances, that assistance not be granted
Other:	• assistance may be provided subject to conditions (s9) • the Attorney-General also holds the discretion to refuse requests for assistance if dual criminality is not established.

OUTGOING MA REQUESTS

Assistance can request:	See s7 MACMA and dependent on laws of recipient foreign country • taking evidence and production of documents or other articles (s13) • search and seizure (s20) • arrangements for persons in custody to give evidence or assist investigation (ss25-35) • proceeds of crime actions i.e. forfeiture, pecuniary penalty or restraining orders (ss39, 40)
Admissibility requirements:	See Part 9 (ss52-60) MACMA

VANUATU

CENTRAL AUTHORITY

Public Prosecutor
Office of the Public Prosecutor

PMB 9035
Port Vila
VANUATU

P. +678 22 271

oppvila@vanuatu.gov.vu

opp.gov.vu

LEGISLATION

Mutual Assistance in Criminal Matters Act 2002 [Ch. 285]

INCOMING MA REQUESTS

Basis for MARs:	Treaty (bilateral or multilateral), letters rogatory or any foreign country on the basis of reciprocity
Method of receiving MARs:	Email, hardcopy or by diplomatic channels
Requirements:	See s6 MACMA
Definition of 'serious offence':	Offence for which maximum penalty is imprisonment for at least 12 months
Assistance can provide:	• voluntary assistance (e.g. voluntary witness statement) • taking evidence and production of documents or other articles (ss12-17) • search and seizure (ss19-22) • arrangements for persons in custody to give evidence or assist investigation (ss31-34) • proceeds of crime actions (ss40-48)
Grounds of refusal:	Mandatory grounds (s8): • political offence • prosecuting, punishing or otherwise causing prejudice to a person on account of the person's race, sex, religion, nationality or political opinions • request would prejudice the sovereignty, security or national interest of Vanuatu • double jeopardy • death penalty, unless the Attorney-General considers that due to special circumstances, the request should be granted (s9) Discretionary grounds (s10): • dual criminality • lapse of time or any other reason • prejudice investigation or proceeding for criminal matter in Vanuatu • prejudice safety of any person (whether or not outside Vanuatu) • result in manifest unfairness or a denial of human rights • impose excessive burden on the resources of Vanuatu • appropriate, in all the circumstances, that assistance not be granted
Other:	• assistance may be provided subject to conditions (s7) • limits for the use of information obtained under the Act and provides safeguards against inappropriate or unofficial use (s62) • offence to intentionally disclose the contents or existence of an incoming request, unless necessary to do so in the performance of duties or with the approval of the Public Prosecutor (s63)

OUTGOING MA REQUESTS

Assistance can request:	See s7 MACMA and dependent on laws of recipient foreign country • taking evidence and production of documents or other articles (s11) • search and seizure (s18) • arrangements for persons in custody to give evidence or assist investigation (ss23-30) • proceeds of crime actions (ss38,39)
Admissibility requirements:	See Part 9 (ss51-60) MACMA

6.2 – Other Country Profiles

CANADA

CENTRAL AUTHORITY

International Assistance Group
Department of Justice

284 Wellington Street
Ottawa Ontario
K1A 0H8 CANADA

P. +613 957 4832
After hours: +613 851 7891
F. Fax +613 957 8412

cdncentralausthority@justice.gc.ca

justice.gc.ca

Language:
English or French

LEGISLATION

Mutual Legal Assistance in Criminal Matters Act

INCOMING MA REQUESTS

Basis for MARs:	• treaty and convention requests • letters rogatory • possibility of entering into a time-limited case specific administrative arrangement in the absence of a treaty • to the extent possible, Canada will also execute non-treaty requests (e.g. taking voluntary statements from persons; obtaining publicly available documents; or serving documents) for assistance made by foreign police and prosecutors where the assistance needed may be provided on a voluntary basis.
Method of receiving MARs:	By email (unless hardcopy required to be registered or served)
Requirements:	A step-by-step guide for Canada's requirements for incoming requests can be found at https://www.justice.gc.ca/eng/cj-jp/emla-eej/mlaguide-guideej.pdf
Definition of 'serious offence':	Offences as specified within the relevant treaty, convention or other international agreement that is in force, to which Canada is a party and that contains a provision respecting mutual legal assistance in criminal matters.

Assistance can provide:	• For treaty and convention requests:
	• search and seizure;
	• gathering physical or documentary materials;
	• compelling witnesses to attend before authorities in order to give statements or testimony (statements and testimony of suspects can only be given voluntarily), including by video or audio link;
	  o transferring sentenced persons to the requesting country to give evidence or to assist in an investigation;
	  o lending court exhibits;
	  o examining a place or site in Canada;
	  o enforcing foreign restraint, seizure and forfeiture orders; and
	  o enforcing criminal fines.
	• More limited assistance is available by letters rogatory (i.e. if there is no treaty or convention relationship):
	  o orders compelling witnesses to give evidence (including by video-link) and to produce records provided following conditions are met:
	  1. request made by a judge, court or tribunal in the requesting country; and
	  2. the criminal matter for which the assistance is sought must be pending before the foreign judge, court or tribunal.
	• to the extent possible, Canada will also execute non-treaty requests for assistance made by foreign police and prosecutors where the assistance needed may be provided on a voluntary basis (e.g. taking voluntary statements from persons; obtaining publicly available documents; or serving documents).
	• Canada may enter into a time-limited case specific administrative arrangement with a non-treaty country to respond to a request for court-ordered assistance (s6).
	• Dual criminality is generally not required, except for requests for search warrants and restraint/seizure and forfeiture orders.

Grounds of refusal:	• Generally under s 8 of MLACMA, but specifically according to the terms of each section (ex. refusal of a request for an order of forfeiture under s 9.4(2) of MLACMA). See also terms of the applicable treaty or convention.
Other:	• Limits for the use of information obtained and safeguards against inappropriate or unofficial use • Requests not to be disclosed • Advise of any media attention that the case has received • Advise whether request is urgent and provide justification • Advise of any previous contacts with Canadian law enforcement and provide relevant contact information

OUTGOING MA REQUESTS

Assistance can request:	Where "business records" are sought to be introduced as evidence in Canadian proceedings under the Canada Evidence Act, they must be accompanied by an affidavit or certification, which will be specified in Canada's MLA request. If video-link testimony is being sought, Canada may require an oath to be administered and/or that Canadian authorities be permitted to directly pose the questions to witnesses.

UNITED KINGDOM

CENTRAL AUTHORITY

The UK has three Central Authorities: Home Office: UK Central Authority (UKCA), Crown Office and Her Majesty's Revenue and Customs (HMRC)

UKCA for MLA requests for England, Wales & Northern Ireland:

UK Central Authority International Directorate Home Office,
2nd Floor, Peel Building
2 Marsham Street, London SW1P 4DF

Tel: +44 207 035 4040
Fax: +44 (0)207 035 6986

UKCAILOR@homeoffice.gov.uk

Crown Office for MLA requests for Scotland:

International Co-operation Unit
Crown Office ,25 Chambers Street, Edinburgh EH1 1LA

Tel: +44 (0)131 243 8152
Fax: +44 (0)131 243 8153

Email: coicu@copfs.gov.uk

HMRC for MLA requests for tax and fiscal matters in England, Wales & Northern Ireland:

Criminal Law and Benefits and Credits Advisory Team HM Revenue and Customs - Solicitor's Office, 1st Floor (South),
Bush House S/W Wing ,The Strand,
London ,WC2B 4RD

Fax: +44 (0)3000 586324

Email: mla@hmrc.gov.uk

gov.uk/guidance/mutual-legal-assistance-mla-requests
UK MLA guidelines

LEGISLATION

Crime (International Co-operation) Act 2003

INCOMING MA REQUESTS

Basis for MARs:	Treaty (bilateral or multilateral), letters rogatory or any foreign country on the basis of reciprocity
Method of receiving MARs:	UKCA: via post, courier, fax or email HMRC: via post or email Crown Office in Scotland: via post, email, courier or fax
Requirements:	Requests must be in writing and can be sent electronically. Further information on requirements for authorities outside of the UK in making requests can be found at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/415038/MLA_Guidelines_2015.pdf
Definition of 'serious offence':	Serious offence is not defined for the purpose of considered requests. However there is a de minimis policy, meaning the UK will not consider trivial requests and will not usually accept any requests were a value of loss of less than £1,000 is involved. If coercive measures are sought by court order (e.g. search warrant), UK authorities would need to be satisfied that if the conduct constituting the offence were to occur in a part of the UK it would constitute an offence in that part. If an offence in the foreign country, which is not an offence in the UK, assistance may be provided on non coercive measures (eg obtaining voluntary witness statements). Any such request will be considered on a case by case basis. Please note the legal system in Scotland is distinctly different from the system in England, Wales and Northern Ireland and the nature of, and basis for, criminal offences can be different.
Assistance can provide:	• service of process • statements and interviews • hearings via video or telephone conference • request for evidence (testimony) to be taken before a court • production orders (used to obtain 'special procedure material' e.g. communications content, banking evidence etc) • search and seizure • communications data (non-content) • live interception of communications • restraint (freezing), confiscation and forfeiture • temporary transfer of a prisoner for purposes of investigation • the UK is not a signatory to the European Convention on the Transfer of Proceedings in Criminal Matters and has a reservation under Article 21 of the Convention on Mutual Assistance in Criminal Matters. Requests for transfer of proceedings will be considered on a case-by-case basis. Further information can be found in the MLA guidelines.

UNITED KINGDOM

INCOMING MA REQUESTS

Grounds of refusal:	• politically motivated • prejudice the sovereignty, security or other essential interests of the UK • prejudice the ordre public of the UK (this includes the risk that the death penalty will be imposed for the crime under investigation) • De minimis requests (trivial or disproportionate): financial loss or gain or damage of less than £1,000, or the alleged offence was committed more than 10 years ago (and there is no or insufficient explanation for the delay in investigation or prosecution) (Note: This does not apply to Scotland or HMRC) • double jeopardy • relates to an offence that the UK regards as an offence under military law, which is not also an offence under ordinary criminal law • substantial grounds for believing that the request has been made for the purpose of investigating, prosecuting or punishing a person on account of his/her race, gender, sexual orientation, religion, nationality, ethnic origin or political opinions or that person's position may be prejudiced for any of those reasons • request is for a coercive or intrusive measure for which the UK requires dual criminality and in respect of which there is no equivalent UK offence
Other:	• dual criminality is required for search and seizure, production orders and restraint and confiscation. • limits for the use of information obtained under the Act and provides safeguards against inappropriate or unofficial use (s9(2) Crime (International Co-operation) Act 2003) • the UK has relatively strict data protection laws and procedures (e.g. Data Protection Act 2018) and the ability of UK authorities to provide information and/or evidence will be determined in line with the provisions of this legislation

OUTGOING MA REQUESTS

Assistance can request:	Chapter 2 Crime (International Co-operation) Act 2003

UNITED STATES OF AMERICA

CENTRAL AUTHORITY

Office of International Affairs Criminal Division
United States Department of Justice

1301 New York Avenue, N.W.
Washington DC 20005

P. +1 202 514 0000
F. +1 202 514 0080

oia.mla@usdoj.gov
(for receipt of incoming MLA only)

justice.gov/criminal-oia

LEGISLATION

18 U.S.C. § 3512 is the primary domestic procedural statute for executing MLA requests that foreign authorities send to the US involving criminal matters.
Other laws governing production of evidence in domestic cases also may apply. 28 U.S.C. § 1782 is primarily used to assist international tribunals.
When making MLA requests the US invokes bilateral treaties and multilateral conventions as the principal mechanisms for assistance. 28 U.S.C. § 1781 also permits the US to send letters rogatory.

INCOMING MA REQUESTS

Basis for MARs:	The U.S. can receive requests pursuant to MLATs or multilateral conventions that provide for MLA in criminal matters; letters of request; and letters rogatory. The U.S. executes letters of request and letters rogatory on the basis of comity and reciprocity.
Method of receiving MARs:	Email is the preferred method of receipt; however, requests may also be sent by regular mail or fax. Diplomatic channels are also available but not necessary.
Requirements:	The legal requirements that must be satisfied to obtain assistance depend on the nature of the assistance requested. Generally, the information provided must meet the same U.S. legal standards (see below) for production of evidence in U.S. domestic cases. MLA requests generally should contain: • Identification of the requesting authority; • Sufficient facts describing the offense and the investigation, specifically, stating what happened and demonstrating how the conduct described satisfies the elements of the offense; • A description of the assistance sought; • A statement explaining the purpose for which the evidence, information, or other assistance is sought, establishing a clear nexus between the assistance sought and the offense; • The legal provisions establishing the offense; • A description of any procedures the foreign authority needs the U.S. to follow when executing the request; and • Any other information helpful to the execution of the request.
Definition of 'serious offence':	Under U.S. law, offenses are categorized as either misdemeanors or felonies, which are distinguishable, inter alia, by the term of imprisonment that they carry. A misdemeanor is punishable by up to one year of imprisonment. A felony carries a term of imprisonment of more than one year. The United States does not apply a standard definition for "serious offense" in the MLA context, except as required by treaty or convention.
Assistance can provide:	• Taking statements or testimony from a witness, including by video, and compelling such statements, if necessary; • Providing and authenticating documents, records and articles of evidence; • Compelling production of electronic evidence from an ISP or web hosting service; • Locating or identifying persons or items; • Serving legal process; • Conducting searches and seizures; • Identifying, tracing, restraining and confiscating (forfeiting) proceeds or instrumentalities of crime; • Transferring persons in custody for testimony or other assistance; and • Other assistance not prohibited by U.S. law.
Grounds of refusal:	• Security or other essential interests of the U.S., especially constitutional concerns such as those implicating the First Amendment to the U.S. Constitution, which protects freedom of speech (see explanation below in Section designated "Other"); • Failure to satisfy dual criminality regarding certain types of assistance; • Failure to satisfy treaty requirements; • Request relates to a political offense (discretionary); or

UNITED STATES OF AMERICA

INCOMING MA REQUESTS

Grounds of refusal:	• Request relates to an offense under military law that would not be an offense under ordinary, criminal law; or • The effort necessary to provide the assistance is not proportional to the seriousness of the offense (previously referred to as "de minimis").
Other:	• **Legal Standard for Most Non-electronic evidence: Relevance** The legal standard for the production of most non-electronic evidence (e.g., witness statements; records, documents, or other items held by third parties) is relevance. The evidence requested must be relevant to the investigation. • **Legal Standard for Searches and Seizures: Probable cause** For the search of a person, place, or thing, and seizure of evidence, the legal standard is "probable cause." Probable cause is satisfied with sufficient facts leading a reasonable person to believe that a crime has been committed and that there is evidence of that crime on the person or in the place or thing to be searched. In order for a search warrant to issue, 18 U.S.C. § 3512 requires that the conduct alleged, if it had been committed in the United States, would be punishable by a term of imprisonment of more than one year, i.e., there must be dual criminality. • **Legal Standard for Internet Content Data: Probable cause** Data consisting of internet content, including the content of communications, may be produced only pursuant to search warrants, after establishing probable cause. If the content of an account is sought, foreign authorities must provide sufficient facts to show that: the account/profile is/was used at a time relevant to the offense; and investigators have reason to believe that the account has information relating to the offense. It is not enough to merely show that the person has an internet account/profile. • **Legal Standard for Subscriber and Transactional data (non-content): Relevance and Materiality** For production of non-content data, foreign authorities must provide specific and articulable facts showing that the requested data is relevant and material to an ongoing criminal investigation (18 U.S.C. § 2703(d)). • **Confidentiality** The United States provides confidentiality when requested by the foreign authority. The request for confidentiality must be express and must provide a justification (e.g., release of information about the foreign investigation will damage the investigation). Please note that, unless confidentiality is requested and granted, all applications seeking legal process that are filed with a U.S. court are public and are searchable by anyone on the internet. U.S. courts may authorize the execution of requests under conditions of confidentiality when justified. • **Speech Protected under the U.S. Constitution** The First Amendment to the U.S. Constitution protects freedom of speech, including the freedom to publish political speech, criticism, and the expression of opinions. When foreign authorities seek internet records for social media posts or emails expressing opinions that may be deemed unlawful in the requesting country, U.S. authorities must determine whether the conduct alleged falls under a category of protected speech in the United States. Speech is not protected if it constitutes a true threat or incitement to violence.

OUTGOING MA REQUESTS

Assistance can request:	The United States has a very comprehensive code for the admissibility of evidence (the Federal Rules of Evidence). In addition, individual U.S. states have their own evidence rules, which sometimes differ from the federal rules. Generally, to be admissible in U.S. courts, evidence must be relevant and must possess indicia of reliability. To establish the reliability of the evidence, prosecutors must authenticate the evidence. Consequently, the United States often requests certificates of authenticity from records custodians for evidence produced in foreign countries. Such certificates of authenticity can take the place of authentication through the use of live witness testimony at trial.

CHAPTER 7 – Service Provider Profiles

As discussed in Chapter 2, cooperation with service providers is essential. With this in mind, the table below provides high-level summaries of some service providers PILON members may seek information from, either directly or through MLA. Information relating to other service providers may be found at Search-ISP list or internet search.

Most service providers have developed and published law enforcement guidelines. It is highly recommended that officers read the relevant guidelines for the service provider they wish to seek information from in the first instance. These guidelines usually include information about the providers preferred way of being contacted by law enforcement with most larger companies having a dedicated 'portal' or 'law enforcement system' that must be used for making requests (preservation, emergency and in some circumstances non-content data). These portals enable law enforcement officers seeking data for investigations that relate to a particular service provider to quickly and securely request this data. The portals can only be used by law enforcement personnel and often require an acknowledgment that by accessing the portal and submitting a request you are authorised to represent a law enforcement agency.

For service providers that do not have a dedicated portal or specific forms, a generic preservation request template and generic emergency request template is available for download on the PILON website.

The information in this chapter was current at the time of finalising this Handbook, but contact information and procedures are subject to change and should be verified on the relevant webpage every time before being relied upon.

Tip: Keep in mind that communications with service providers should be sent by the relevant law enforcement agency from an official email address or using an official government or law enforcement agency letterhead.

Service provider	Contact	Law enforcement information/guidelines
Airbnb Airbnb is an online marketplace and hospitality service for people to lease or rent short-term lodging including holiday cottages, apartments, homestays, hostel beds or hotel rooms.	Airbnb Ireland UC Law Enforcement Liaison, 8 Hanover Quay Dublin 2, IRELAND Airbnb, 1 Infinite Loop Cupertino CA 95014 USA Portal: Airbnb Law Enforcement Portal Email: leainfo@airbnb.com	• LEA seeking data from the Airbnb platform can be found here and need to register with the Airbnb Law Enforcement Portal . • Requests not from US law enforcement should generally be directed to Airbnb Ireland except for requests involving Japan or China. • Requests from US law enforcement should be addressed to Airbnb Inc. located in San Francisco, California. • Airbnb Ireland, Airbnb GSL, and Airbnb China have a policy of using reasonable efforts to notify affected users when they receive a valid Law Enforcement Request seeking user data. • If the concerned user is a non-United States resident, law enforcement officers should serve the request on Airbnb Ireland. • Emergencies: Use 'emergency request' button on portal.
Amazon (Amazon.com and Amazon Web Services). Amazon is an electronic commerce and cloud computing company.	Amazon.com Inc. Corporation Service Company, MC-CSC1, 300 Deschutes Way SW Suite 208, Tumwater WA 98501 USA Attn: Legal Department – Subpoena Portal: Amazon Law Enforcement System Email: subpoena-criminal@amazon.com	• Amazon Law Enforcement Guidelines. • Amazon only accepts service of subpoenas, search warrants and other legal process through the Amazon Law Enforcement System (portal). • Non-US LEA requests must go through legal and diplomatic channels in its jurisdiction, including through MLA or letters rogatory processes. • Preservation: upon receipt of lawful and binding request, will preserve requested information for up to 90 days. • Emergencies: Use 'Submit Emergency Request' button on homepage of portal.

Service provider	Contact	Law enforcement information/guidelines
Apple Apple is an American multinational technology company that designs, develops and sells consumer electronics, computer software and online services.	Apple Inc. Attention: Privacy and Law Enforcement Compliance, 1 Infinite Loop, Cupertino CA 95014 USA Email: lawenforcement@apple.com; or for emergency requests exigent@apple.com	• Apple Legal Process Guidelines for Government and Law Enforcement outside the US and for Government and Law Enforcement within the US . • Government and law enforcement personnel outside of the United States transmitting an information request to Apple should complete a Government & Law Enforcement Information Request template. • When making a requested require law enforcement to include the following information with the legal request so the request can be verified: Law Enforcement Agency Law Enforcement Agent Name and Badge/ID number Agency issued email address Law Enforcement Phone number (with extension if applicable) Verifiable physical return address Law Enforcement Fax number. • Preservation: 90 days. Must include the relevant Apple ID/account email address, or full name and phone number, and/or full name and physical address of the subject Apple account. • Emergencies: Complete Emergency Government & Law Enforcement Information Request form and send to exigent@apple.com.
BlackBerry Blackberry is an enterprise software multi-national company specializing in enterprise software	BlackBerry Limited, BlackBerry Legal Department, 2200 University Avenue East, Waterloo, Ontario, Canada N2K 0A7 Email: lawfulaccess@blackberry.com; or for enquiries contact pso.au@blackberry.com	• Use PINs and/or IMEIs as identifiers for accounts. • Preservation: 90 days, contact lawfulaccess@blackberry.com.

Service provider	Contact	Law enforcement information/guidelines
Booking.com Booking.com is a travel metasearch engine for lodging reservations. It is owned and operated by and is the primary revenue source of United States-based Booking Holdings and is headquartered in Amsterdam	Booking.com B.V. Herengracht 597 1017 CE, Amsterdam Netherlands Portal: Booking.com Law enforcement request portal (only for emergency requests and for use by Dutch authorities)	• Booking.com Law Enforcement Guidelines. • Booking.com B.V. is the data controller for any personal data collected through the Booking.com online reservation services. • All data disclosure requests must be addressed to Booking.com B.V. • Only accepts requests through the formal mutual assistance process through Dutch authorities. • Preservation: Will not provide preservation in advance of a MAR. • Emergencies: Will accept emergency disclosure requests if fulfil requirements in Guidelines.
Dropbox DropBox is a file hosting service that offers cloud storage, file synchronization, personal cloud and client software.	Dropbox, 333 Brannan Street, San Francisco, CA 94107 Email: legalcompliance@dropbox.com	• Dropbox law enforcement guidelines are available by request (email legalcompliance@dropbox.com).
eBay eBay, Inc. is an American multinational e-commerce corporation that facilitates consumer-to-consumer and business-to-consumer sales through its website. The company manages the eBay website, an online auction and shopping website in which people and businesses buy and sell a wide variety of goods and services worldwide.	eBay, Attn: Law Enforcement eRequest System, 2211 North First Street San Jose CA 95131 Portal: Law Enforcement eRequest System Email: LawEnforcement@ebay.com (for general information)	• eBay Law Enforcement Guide. • eBay's online Law Enforcement eRequest System (LERS) are handled manually and are processed in approximately 10 days. • eBay's Global Asset Protection (GAP) Team promotes the safe use of its platforms and to collaborate with local, federal and international law enforcement in apprehending and prosecuting criminals.

Service provider	Contact	Law enforcement information/guidelines
Facebook Facebook is an online social media and social networking service. The 'Facebook Family of Apps' includes Facebook, Instagram, WhatsApp and Messenger.	Facebook Inc. Facebook Security, LE Response Team, 1 601 Willow Road Menlo Park CA 94025 Portal: Facebook Law Enforcement Online Request System	• Online Law Enforcement Response System ("The Portal"). • Facebook's Safety Centre set outs Information for law enforcement authorities that provide guidance for LEA seeking records from Facebook and Instagram. • Facebook owns what it refers to as the 'Facebook Family of Apps' which includes Facebook, Instagram, WhatsApp and Messenger. • Facebook users can access a history of their own activity on Facebook and/or download their own information using the 'Download your information' feature from their account settings. More information on someone accessing their own data can be found at facebook.com/help/accessyourdata. • Information on hacking of a Facebook account can be found at facebook.com/hacked. • Information about online safety can be found at facebook.com/safety. • Abusive content on Facebook can be reported at facebook.com/report. • Preservation: 90 days; Submit request through Portal noting Facebook automatically deletes records once the preservation expires. If the Facebook Portal does not allow preservation, this means there is no account for the user. • Emergencies: Submit a request through Portal.
Google Google is a multinational technology company specializing in Internet-related services and products. This includes Gmail, YouTube, Google Voice and Blogger to name a few.	Google LLC. Google Legal, Investigations Support, 1600 Amphitheatre Parkway, Mountain View CA 94043 Portal: Google Law Enforcement Request System Email: USLawEnforcement@google.com	• Legal requests for user data should be submitted through the Google Law Enforcement Request System (LERS). • LERS requires each user to register for a unique account to submit legal requests. • Further information on Google treats requests for user information can be found on the Transparency Report Help Centre page. • Users can use Google Takeout to create an archived file of their own content from most Google services, and can then choose to share that content as they wish. • Preservation: 1 year (with possibility of extension) if MAR is underway. Otherwise 90 days. • Emergencies: Submit a request through LERS.

Service provider	Contact	Law enforcement information/guidelines
Instagram Instagram is a photo and video sharing social networking service. The application allows users to upload media, editable by filters and organised with tags and location information as well as like photos and follow other users to add their content to a feed. Posts can be shared publicly or with pre-approved followed.	Facebook, Inc., Law Enforcement Response Team, 1601 Willow Road, Menlo Park, CA 94025 Portal: Facebook Law Enforcement Online Request System	• Information for Law Enforcement on seeking Instagram account records. • As Instagram part of the 'Facebook Family of Apps' see Facebook entry above.
KIK Kik Messenger is a freeware instant messaging mobile application that sends and receives messages, photos, videos, sketches, mobile webpages and other content after users register a username. Kik is known for its features preserving users' anonymity, such as allowing users to register without providing a telephone number. The application logs user IP addresses which the company can use to determine location.	KIK, MediaLab.AI Inc., Santa Monica, CA 90401 Email: lawenforcement@kik.com	• KIK Law Enforcement Resource Center for Information for Law Enforcement and Kik's Law Enforcement FAQs. • Kik is known for its features preserving users' anonymity, and uses usernames as the unique identifier (instead of a phone number). • The application logs user IP addresses which Kik can use to determine location. • Preservation: 90 days; Complete Preservation Request form and send to lawenforcement@kik.com with "PRESERVATION REQUEST" in the subject line. Note that Kik will not be able to identify the username of a subject user without a valid US legal order. Extensions for an additional 90 days should be made by submitting a new, completed and valid preservation request at least one week before original request expires (there is an 'extension' box in the form) and include the original preservation request Kik ticket number for reference. • Emergencies: See Emergency Disclosure Request page where can download an Emergency Disclosure Request form and send to lawenforcement@kik.com with "EMERGENCY DISCLOSURE REQUEST" in the subject line.

Service provider	Contact	Law enforcement information/guidelines
Microsoft Microsoft is a multinational technology company specialising in computer software, consumer electronics, personal computers, and related services.	Microsoft Corporation One Microsoft Way Redmond, WA 98052 Portal: Microsoft Law Enforcement Request Portal (LE Portal) Email: msndcc@microsoft.com (for general enquiries only) or lealert@microsoft.com (for emergency requests	• Microsoft Law Enforcement Request Portal (LE Portal). • Microsoft's best known software products are Microsoft Windows line of operating systems, the Microsoft Office suite, and the Internet Explorer and Edge web browsers. Its flagship hardware products are the Xbox video game consoles and the Microsoft Surface personal computers. • Further information about Microsoft's data practices in handling of government requests can be found here. • Preservation: 90 days. • Emergencies: lealert@microsoft.com or +1 425-722-1299 (option 1) for 24/7 emergency response.
PayPal PayPal Holdings, Inc. operates a worldwide online payments system that supports online money transfers and serves as an electronic alternative to traditional paper methods like checks and money orders.	PayPal Holdings Portal: Safety Hub – PayPal Law Enforcement Tool Email: lawenforcement@paypal.com	• PayPal law enforcement center has information for LEA to work with and contact the Global Investigations Team including the PayPal Law Enforcement Guide. • LEA and government agencies can submit PayPal data requests through Safety Hub - PayPal Law Enforcement Tool. • *Emergencies*: Send request to lawenforcement@paypal.com with 'Urgent Life Safety' in the subject line. • For asset freeze orders or emergency disclosure orders that require immediate attention, email relevant order to lawenforcement@paypal.com marked with high importance and 'Immediate Attention' and nature of request in the subject line.
Skype Skype specializes in providing video chat and voice calls between computers, tablets, mobile devices, the Xbox One console and smartwatches via the Internet and to regular telephones.	Skype Communications SARL, 23-29 Rives de Clausen, L-2165 Luxembourg, Company, No: R.C.S. Luxembourge B100.468, VAT: LU 20981643 See Microsoft entry Portal: Microsoft Law Enforcement Request Portal	• Skype is headquartered in Luxembourg and is a division of Microsoft Corporation. • Law enforcement must make specific enquiries to determine the location of the required data. • Video chat content, where recorded by a user, may be available and this content is held by Microsoft in the US. • Requests must be submitted in English, French or German, or must also include a translation into one of these languages.

Service provider	Contact	Law enforcement information/guidelines
Snapchat Snapchat is an imaging and multimedia application. One of the principal features of Snapchat is that pictures and messages are usually only available for a short time before they become inaccessible to their recipients.	Snap, Custodian of Records, 2772 Donald Douglas Loop North, Santa Monica, CA 90405 Portal: Snap Inc. Law enforcement online service (Snapchat emergency disclosure requests only) Email: lawenforcement@snapchat.com (queries and legal process requests)	• Snap Safety Centre – Information for Law Enforcement for law enforcement has information possible availability of Snapchat user records, information or content and process required to obtain it. • Snap Inc. Law Enforcement Guide including some sample language to include in requests. • Snapchat does not retain data for very long and is unlikely to retain content once at least one receiver has accessed the 'Snap' (photo or video taken using the Snapchat app's camera on a mobile device and may be shared with user's friends, in a Story or Chat). • Non-US government and LEA must use MLA processes to seek user information from Snap. • Snap retains logs for the last 31 days of Snaps sent and received, for 24 hours of posted stories, and for any unopened chats or those saved by a sender or recipient. The content is removed once all recipients have viewed it or 30 days after it was sent when unopened. • *Preservation*: Will respond to properly submitted preservation requests wile MLA processes are undertaken. 90 days and will extend one additional 90-day period with formal extension request. • *Emergencies*: Complete and submit the Law Enforcement Emergency Response Form at the dedicated emergency disclosure request service lawenforcement.snapchat.com/emergency.

Service provider	Contact	Law enforcement information/guidelines
Twitter Twitter is an online news and social networking service where users post and interact with messages called "tweets".	Twitter, Inc., c/o Trust & Safety - Legal Policy, 1355 Market Street, Suite 900, San Francisco, CA 94103 Portal: Twitter's online legal request submission site	• Twitter Law Enforcement Guidelines. • Legal Requests can be submitted on a dedicated Legal Request Submission site. • A Twitter account profile often contains a profile photo, header photo, background image, and status updates, called Tweets. In addition, the account holder has the option to fill out a location (e.g., San Francisco), a URL (e.g., twitter.com), and a short "bio" section about the account for display on their public profile. • *Preservation*: 90 days. Preservation requests should be signed by requesting official, have valid return official email address, be sent on law enforcement letterhead in non-editable format, and include the @username and URL of the subject Twitter profile (e.g. https://twitter.com/twittersafety (@twittersafety), and/or the Twitter account's unique, public user identification number (UID) or a Periscope username and URL (e.g., @twittersafety and https://periscope.tv/twittersafety). • *Emergencies*: law enforcement officers can submit an emergency disclosure request through the Legal Request Submissions site (the quickest and most efficient method).
WhatsApp WhatsApp is a freeware and cross-platform instant messaging and voice over IP (VoIP) service	Law Enforcement Response Team, 1601 Willow Road, Menlo Park, CA 94025 Portal: WhatsApp Law Enforcement Online Request System	• WhatsApp Information for Law Enforcement including Law Enforcement Guidelines. • Users seeking information on their own accounts can access WhatsApp's Request Account Info feature. • Note that WhatsApp encrypts all data. • *Preservation*: 90 days. Submit request via WhatsApp Law Enforcement Online Request System. • *Emergencies*: Submit request via WhatsApp Law Enforcement Online Request System and include the word "EMERGENCY" in the subject line of your message.

Further contacts & resources

APEC

Requesting Mutual Legal Assistance in criminal matters from APEC Economies: A Step-by-Step Guide (February 2015)

Council of Europe

The Convention on Cybercrime of the Council of Europe (CETS No. 185 or commonly referred to as the Budapest Convention)

Council of Europe Electronic Evidence Guide: A basic guide for police officers, prosecutors and judges (Version 2.1, March 2020)

Council of Europe Electronic Evidence Guide: A basic guide for police officers, prosecutors and judges (Version 2.1, March 2020).

Other resources available at https://www.coe.int/en/web/cybercrime/resources including specific information on international cooperation.

International Institute for Justice and the Rule of Law

The Good Practices for Central Authorities sets out the institutional, legal and practical considerations needed to create and support durable legal institutions.

INTERPOL

INTERPOL runs three Global Programmes to fight crime (counter-terrorism, cybercrime and organised and emerging crime) and developed the i-24/7 global police communications system, enabling law enforcement direct access to databases in real-time. Authorities making or actioning MARs may use INTERPOL's global network and data to source the evidence sought and INTERPOL officers may help facilitate international informal 'police-to-police' requests for information. INTERPOL has a significant presence in the Pacific region, including NCB in Fiji, Kiribati, Marshall Islands, Papua New Guinea, Samoa, Solomon Islands, Tonga and Vanuatu.

Pacific Transnational Crime Network (PTCN)

The Pacific Transnational Crime Network (PTCN) provides a Police-led proactive criminal intelligence and investigative capability to combat transnational crime in the Pacific through a multi-agency and regional approach.

UNODC

The Mutual Legal Assistance Request Writer Tool was developed by UNODC to assist criminal justice practitioners in drafting MARs.

The UNODC Online Directory of Central Authorities is available to central authorities and government agencies with a user account.

UNODC Practical Guide for Requesting Electronic Evidence Across Borders was published in January 2019 and is available for member states' criminal justice officials through the UNODC Sherloc Portal

Glossary

APNIC	Asia Pacific Network Information Centre (www.apnic.net) Regional internet registry for the Asia Pacific region administering IP addresses for the Asia Pacific.
Bit	Portmanteau of 'binary digit' The basic unit of information in computing and digital communications.
Bluetooth	A wireless technology standard used for exchanging data between devices (fixed or mobile) over short distances using a short-range wireless connection.
Blu-ray disc	Often referred to as 'Blu-ray' is a digital optical disc data storage medium designed to supersede the DVD format. It is mainly used for video and video games.
browser web browser	A software application for accessing information on the internet. Browsers are used on a range of devices. It is not the same thing as a search engine, which is just a website that provides links to other websites. E.g. Google Chrome, Safari, Firefox, Microsoft Edge.
CCTV	Closed Circuit Television
CD	Compact Disc
Central Authority	An agency or organisation designated to facilitate the implementation and operation of an international treaty in public and private international law. In international cooperation for transnational criminal law matters, it is the national body responsible for making, receiving and executing requests for mutual legal assistance and extradition, or transmitting such requests to another Central Authority for execution.
Cloud Cloud storage Cloud computing	Cloud storage is a model of computer data storage where the digital data is stored in pools (a pool is a collection of resources kept ready to use) and said to be 'on the cloud'. Physical storage can be across multiple servers, which are typically owned and managed by a hosting company. Cloud storage providers are responsible for keeping the data available and accessible, and the physical environment secure. Cloud computing is the on-demand availability of computer system resources (i.e. cloud storage and computing power) without direct active management by the user.
computer network	A group of computers that use a set of common communication protocols (such as IP) over digital interconnections for the purpose of sharing resources located on, or provided by, network notes. The nodes can be classified by many means and are identified by hostnames and network addresses. Computer networks can support many applications and services such as access to the world wide web, digital video and audio, shared use of application and storage servers and use of email and instant messaging applications.
cookie	Small files stored on a user's computer by a web browser while browsing a website. Cookies were designed for websites to remember useful information such as items chosen in an online store, or previously entered names, passwords and payment card numbers.
CSAM	Child Sexual Abuse Material
CSP	Communication Service Provider A type of service provider that transports information electronically and encompasses public and private companies in the telecommunications, internet, cable, satellite and managed services businesses.
cybercrime	Refers to any crime that involves a computer and a network. The computer may have been used in the commission of the crime, or it may be the target of the crime.
data	Any sequence of one or more symbols and requires interpretation to become information. Can be singular, plural or a mass noun.
data storage device storage device	Any device for storing information or data (e.g. CD, DVD, USB).
database	An organised collection of data that be accessed in many ways, but generally stored and accessed electronically.

digital forensics	A branch of forensic science related to the recovery and investigation of material found in computer systems, digital devices and other storage media with the aim of admissibility in court. Originally referred to as 'computer forensics' it has expanded to encompass investigation of all devices capable of storing digital data.
domain name DNS	A domain name is an identification string that defines an area within the internet and serve to identify internet resources (i.e. computers, networks, services) with a text label that is easier to memorise than the numbers used in internet protocols. Domain names are formed by the rules and procedures of the Domain Name System (DNS). The Domain Name System (DNS) is a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. It is sometimes compared to being a type of phonebook for the internet.
dongle	A small piece of computer hardware that connects to a port on another device to provide additional functionality. Originally 'dongle' referred to software protection dongles, but now is used more broadly to mean any small hardware that plugs into a computer.
DoS DDoS	A Denial of Service (DoS) attack is a cyber-attack where perpetrator seeks to make a machine or network resource unavailable to intended users by disrupting services of a host connected to the Internet A Distributed Denial of Service (DDoS) attack is a large-scale DoS attack where the perpetrator uses more than one unique IP address or machines and incoming traffic floods the victim from many different sources.
DVD	Digital Video Disc
electronic evidence	Is any information generated, stored or transmitted using electronic devices that may be relied upon in court. To guarantee that the evidence is accepted in court, it is necessary to obtain the information following processes using specialised personnel and operating within an adequate legal framework.
encryption	The process of encoding information.
GPS	Global Positioning System
hard drive	A device used for storing large amounts of data
hardware	Physical components making up a computer system (e.g. keyboard, monitor, mouse)
host hosting provider	A hosting provider or internet/web hosting service is a service that allows individuals or organisations to make (or host) their website available via the world wide web. Hosts are companies that provide space on a server owned for use by clients as well as providing internet connectivity.
HTML	Hypertext Markup Language HTML is used for writing documents for web servers.
HTTP	Hypertext Transfer Protocol (or HTTPs is Secure HTTP) HTTP is a protocol with the necessary agility and velocity to distribute and handle multimedia information systems over the Internet.
IANA	Internet Assigned Numbers Authority Entity that oversees global IP address allocation, autonomous system number allocation etc. IANA is part of the Internet Corporation for Assigned Names and Numbers (ICANN).
INTERPOL	International Criminal Police Organization
IP address	Internet Protocol address IP Addresses are the fundamental type of source of information available on the internet showing where data packages are to be delivered. IP addresses are expressed as a chain of numbers separated by decimal points and are used to represent and identify a computer on the internet. IPv4: e.g. 192.168.1.252 IPv6: e.g. 2001:0db8:85a3:0042:0000:8a2e:0372:4688
ISP	Internet Service Provider Is an organisation that provides access to the internet, can be community or privately owned, and non-profit or for profit. E.g. Solomon Telekom, Vodafone, Digicel, TPG.
LAN	Local Area Network

letters rogatory	A formal letter of request from a court to a foreign court for some type of judicial assistance (e.g. collecting evidence, interviewing witnesses).
log	Register of determined events generated by the operating system or application for a period of time
MA MLA	mutual assistance or mutual legal assistance The process countries use to obtain government-to-government assistance in criminal investigations and prosecutions..
MAC address	Media Access Control address A unique identifier specific to the network card inside a computer XX-XX-XX-XX-XX-XX (X represents digits or letters A to F). Also referred to as the hardware address or Ethernet address.
MACMA	Mutual Assistance Criminal Matters Act
malware	Portmanteau of malicious software. A program with the objective to cause damage to computers, systems or networks and users.
MAR	mutual assistance request
memory card	Devices used to store digital information, often used in digital cameras, mobile phones, laptop computers etc
metadata	Information about data. There are many types of metadata which can be used to summarise basic information about data which can make it easier to track or work with specific data. E.g. metadata can provide information about how and when a file was created, received, accessed and modified and by whom. E.g. digital image can include metadata that describes how large picture is, colour depth, image resolution, when image created
MLAT	mutual legal assistance treaty An agreement between two or more countries for the purpose of gathering and exchanging information to enforce public or criminal laws.
modem	Portmanteau of modulator demodulator Hardware device that allows a computer or another device (i.e. router, switch) to connect to the internet. It 'modulates; an analogue signal from a telephone or cable wire to a digital data that a computer can recognise, and vice versa. Modems are often classified by the maximum amount of data they can send in a given unit of time (e.g. bit/s). The first modems were 'dial-up' meaning they have to dial a phone number to connect to an ISP. Modern modems are typically DSL (digital subscriber line) or cable modems, considered to be broadband devices.
NCMEC	National Centre for Missing and Exploited Children
P2P Peer-to-Peer	Peer-to-Peer (P2P) computing or networking is a distributed application that partitions tasks between peers where peers are equal. P2P protocol uses the internet for the interchange and download of files. Clients using P2P networks do not have fixed IP addresses and servers will only have a listing of clients and file searches.
pharming	Is a type of cyberattack where a 'pharmer' redirects a website's traffic to another site that is under their control. Pharming ca be done by changing the hosts file on a victim's computer, or by exploiting a vulnerability in DNS server software.
phishing	Is the fraudulent attempt to obtain sensitive information or data (i.e. username, password, credit card details). Phishing techniques often involve fake emails (email spoofing), text or instant messaging that direct users to enter personal information on a fake website that looks legitimate.
PILON	Pacific Island Law Offices' Network
proxy	In computer networking, a proxy server is a server that acts as an intermediary for requests from clients seeking resources from other servers.
PTCN	Pacific Transnational Crime Network
router	Is a networking device that determines the next network point that a packet should be forwarded towards its destination. Routers essentially direct internet traffic.

server	A piece of computer hardware or software that provides functionality for other programs or devices (referred to as 'clients').
service provider	Broad term to encompass a provider of services that transports information electronically. For example, internet service provider, email provider, news provider (press), entertainment provider (music, movies), search, online shopping site.
social media	Are interactive computer-mediated technologies or tools that allow people or companies to create, share or exchange information, ideas, pictures, and/or videos in virtual communities and networks.E.g. Facebook, TikTok, YouTube
software	Computer software or software is a program designed to perform specific tasks (e.g. word processing, accounting, network management, website development etc). It is essentially instructions that tell the computer how to work.
UNODC	United Nations Office on Drugs and Crime
URL	Uniform Resource Locator A chain of characters which is assigned a unique address to each of the documents of the World Wide Web.
USB	Universal Serial Bus A standard that defines the protocols for communication, connection and power supply for devices that are connected to computers.
virus	A computer virus is a type of computer program what replicates itself by modifying other computer programs and inserting its own code. When it replicates those areas are said to be 'infected'.
VoIP	Voice over Internet Protocol A method and group of technologies for the delivery of voice communications and multimedia sessions over IP networks. It is also called IP telephony.
VPN	Virtual private network Extends a private network across a public network and enables users to send and receive data across other networks as if their computing devices were directly connected to the private network. Encryption is common to a VPN connection.
WLAN networks	Wireless Local Area Network Links two or more devices using some wireless distribution method and usually providing a connection to access the wider internet.
WWW	World Wide Web Is the universe of network-accessible information (ie. all resources and users on the internet that are using HTTP).

PACIFIC ISLANDS
LAW OFFICERS' NETWORK

Level 6, Tatte Building

Sogi, Apia

SAMOA

www.pilonsec.org