



Frequently Asked Questions: Cyber Sanctions and Ransomware Payments

These FAQs are intended to support the Guidance Note on Cyber Sanctions, available at: <https://www.dfat.gov.au/international-relations/guidance-note-cyber-sanctions>

This document only provides a summary of relevant sanctions laws. It should not be relied upon as a substitute for legal advice or for consulting the full text of sanctions laws at legislation.gov.au. It is your responsibility to ensure you do not contravene Australian sanctions laws, including by obtaining your own legal advice.

More information on Sanctions is available through the Australian Sanctions Office on DFAT's website ([Australia and sanctions | Australian Government Department of Foreign Affairs and Trade \(dfat.gov.au\)](http://Australia and sanctions | Australian Government Department of Foreign Affairs and Trade (dfat.gov.au)))

Frequently Asked Questions

1. What are cyber sanctions?
2. What is a significant cyber incident?
3. I conduct cyber-related activities for legitimate educational, network defence, or research purposes only. Am I vulnerable to the application of sanctions under Australian law for these activities?
4. Will sanctions be effective in combatting cybercrime?
5. How do I know if I am dealing with a designated person or entity?
6. What are my responsibilities in relation to Australian autonomous cyber sanctions laws?
7. How can I mitigate my risk of violating Australian autonomous cyber sanctions laws?
8. What happens if I have made a ransomware payment to a designated person and/or entity?
9. Will I be prosecuted for making a ransomware payment to a designated person and/or entity?
10. What if I think I've made a mistake and not complied with Australian autonomous cyber sanctions laws?
11. What if I have information on activity that is possibly illegal under Australian autonomous sanctions laws?
12. What are my obligations if I hold, or think I may hold a controlled asset of a designated person and/or entity?
13. Do I have to comply with the sanctions laws of other countries?
14. If I applied for a permit, on what basis would the Minister for Foreign Affairs (or the Minister's delegate) issue a permit to undertake an activity that would otherwise contravene Australian autonomous sanctions law?
15. Will a permit be granted to make a ransomware payment to a designated person or entity?
16. Does the Australian Government plan to ban the payment of ransoms for cyber-related extortion?
17. Does the imposition of sanctions under Australian autonomous cyber sanctions laws for ransomware incidents amount to the banning of ransomware payments by stealth?
18. What measures will the 2023-2030 Australian Cyber Security Strategy take to address the threat of ransomware?

Q1. What are cyber sanctions?

Australian autonomous cyber sanctions are a tool of foreign policy referenced in the *2023-2030 Australian Cyber Security Strategy* as part of Australia's commitment to promote a rules-based cyberspace, grounded in international law and norms of responsible state behaviour, and to hold accountable those who do not comply with the rules. Cyber sanctions may be imposed under Australia's autonomous thematic sanctions criteria in the *Autonomous Sanctions Act 2011* and the *Autonomous Sanctions Regulations 2011* (Cyber Sanctions Framework).

The intent of the cyber sanctions framework is to disrupt and frustrate the perpetrators of malicious cyber activity, such as ransomware, and not to pursue or punish victims of crime.

The Minister for Foreign Affairs may impose a sanction under this Cyber Sanctions Framework, (i.e. a cyber sanction) if satisfied that a person or entity has caused, assisted with causing, or been complicit in, a cyber incident or an attempted cyber incident that is significant or which, had it occurred, would have been significant.

Once sanctioned, a person or entity is referred to as a 'designated person' or 'designated entity'.

The sanction can be in the form of targeted financial sanctions and/or a travel ban.

If a targeted financial sanction has been imposed:

- All Australians and Australian businesses are prohibited from 'dealing with' designated persons or entities.
- 'Dealing with' designated persons or entities includes: making any asset, including money, available to a designated person or entity.
 - Assets cannot be made available directly or indirectly to a designated person or entity;
 - Assets cannot be provided to, or for the benefit of, a designated person or entity.
- All Australians and Australian businesses holding an asset that is owned or controlled by a designated person or entity, i.e. a 'controlled asset' are prohibited from:
 - using or dealing with a controlled asset;
 - allowing a controlled asset to be used or dealt with; or
 - facilitating the use of, or dealing with, a controlled asset.

Travel bans prohibit the entry into or transit through Australia of designated persons. A person subject to a travel ban may be a citizen or resident of any country.

Q2. What is a 'significant cyber incident'?

The Minister for Foreign Affairs may impose a sanction under the Cyber Sanctions Framework if satisfied that a person or entity has caused, assisted with causing, or been complicit in, a cyber incident or an attempted cyber incident that is significant or which, had it occurred, would have been significant.

A 'cyber incident' may include events that result in harm to individuals, businesses, economies or governments. The conduct amounting to a significant cyber incident or attempted significant cyber incident could have occurred anywhere in the world outside of Australia.

What constitutes a 'significant cyber incident' will be determined on a case-by-case basis. Regulation 6A of the *Autonomous Sanctions Regulations 2011* sets out the matters the Minister for Foreign Affairs may have regard to in deciding whether a cyber incident was, or would have been, significant.

Considerations to determine whether a cyber incident is 'significant' may include:

- Whether the conduct of the person or entity was malicious;
- Whether the cyber incident involved, or could have involved if it was attempted but did not occur, any of the following:
 - actions that destroyed, degraded or rendered unavailable an essential service or critical infrastructure;
 - actions that resulted in the loss of a person's life, or caused serious risk of loss of a person's life;
 - theft of intellectual property, trade secrets or confidential business information for the purposes of gaining a competitive advantage for an entity or a commercial sector;
 - interference with a political or governmental process, the exercise of a political right or duty, or the functions or operations of a parliament; and/or

- Any other matters the Minister considers relevant, such as the: (i) breadth of the damage; (ii) seriousness of the damage; and (iii) the number of people impacted by the damage.

Q3. I conduct cyber-related activities for legitimate educational, network defence, or research purposes only. Am I vulnerable to the application of sanctions under Australian law for these activities?

Cyber Sanctions are not intended to prevent or interfere with legitimate cyber-enabled academic, government, business, or non-profit activities.

The Australian Government may consider imposing sanctions on those who carry out or facilitate significant cyber incidents – when there is sufficient evidence, it is in Australia’s national interest, and it is appropriate to do so.

Our autonomous sanctions framework aims to deter cybercrime by:

- (i) disrupting criminal activity where prosecution may, or may not, be a viable option;
- (ii) exposing cybercriminals’ activities and their identities, placing them at further risk of detection by law enforcement agencies; and
- (iii) imposing costs and consequences on cybercriminals, hackers and threat actors who target Australia and other countries.

Q4. Will sanctions be effective in combatting cybercrime?

Sanctions are part of a suite of possible measures the Australian Government considers in responding to significant cyber incidents.

Sanctions are one of the strongest ways Australia can signal our objection to, and impose costs for, conduct that is contrary to international norms of responsible cyber behaviour. They may be considered in conjunction with other policy and operational considerations to effect positive change and to deter and respond to significant cyber incidents.

When it is in our national interest to do so, Australia will cooperate with likeminded partners as coordinated efforts can amplify the effect of sanctions.

Q5. How do I know if I am dealing with a designated person or entity?

A designated person or entity is an individual, organisation, group or business who or which has been sanctioned by Australia and is subject to targeted financial sanctions and/or a travel ban under Australian autonomous sanctions laws. Those designated persons may be Australian citizens, residents or Australian or foreign nationals or entities.

You are responsible for conducting the necessary due diligence to properly inform yourself about persons or entities connected with your proposed activity or operation to ensure they are not a designated person or entity.

As part of your due diligence checks, you can search the [Consolidated List](#). The Consolidated List is a list of all persons and entities who are subject to targeted financial sanctions under Australian sanctions laws. Listed persons may also be subject to travel bans.

If your proposed activity in any way involves a designated person or entity listed on the Consolidated List, you should consider seeking legal advice before taking further action.

The Australian Sanctions Office (ASO) provides a [checklist on what you can do](#) to comply with, and reduce your risk of contravening, Australian autonomous sanctions laws (including cyber sanctions). We recommend you also review the ASO’s website for further information ([Australia and sanctions | Australian Government Department of Foreign Affairs and Trade \(dfat.gov.au\)](#)).

Q6. What are my responsibilities in relation to Australian autonomous cyber sanctions laws?

It is your responsibility to ensure you (and/or your business) do not contravene Australian autonomous cyber sanctions laws. You should consider getting your own legal advice and conduct your own due diligence to ensure you are fully informed about who you are dealing with.

As part of your due diligence checks, it is important that you inform yourself about persons or entities connected with your proposed activity to ensure you do not contravene Australian cyber sanctions laws. To do this, you can search the [Consolidated List](#). The Consolidated List is a list of all persons and entities who are subject to targeted financial sanctions under Australian sanctions laws. Designated persons on the Consolidated List may also be subject to travel bans.

The Australian Sanctions Office (ASO) is here to assist you to understand your responsibilities and will work with you to prevent and address breaches of Australian autonomous cyber sanctions laws. The ASO cannot provide legal advice or advice on the sanctions laws of other countries.

The ASO provides a [checklist on what you can do](#) to comply with, and reduce your risk of contravening, Australian autonomous sanctions laws. We recommend you also review the ASO's website for further information ([Australia and sanctions | Australian Government Department of Foreign Affairs and Trade \(dfat.gov.au\)](#)).

Q7. How can I mitigate my risk of violating Australian autonomous sanctions laws?

It is your responsibility to ensure you (and/or your business) do not contravene Australian autonomous cyber sanctions laws. You should consider getting your own legal advice and conduct your own due diligence to ensure you are fully informed about who you are dealing with.

The Australian Sanctions Office (ASO) is here to assist you to understand your responsibilities and will work with you to prevent and address breaches of Australian autonomous cyber sanctions laws. The ASO cannot provide legal advice or advise on the sanctions laws of other countries.

If you intend to engage in activity with a person or entity who may be connected to a cybercrime it is incumbent on you to familiarise yourself with the applicable Australian sanctions law (see [What You Need To Know](#) and [Sanctions Regimes](#)), ensure that you know who you are dealing with and, if applicable, understand how the goods/services you are providing or procuring will ultimately be used. This includes understanding your customer's business and organisational structure.

The level of due diligence required will vary depending on the nature of the activity you propose to engage in and the risk of non-compliance with Australian autonomous cyber sanctions laws. At a minimum the ASO expects you to:

- conduct your own checks on the person or entity involved in your activity;
- understand the company structure (if applicable) and any links to designated persons and/or entities;
- check DFAT's [Consolidated List](#) to ascertain if you would be dealing with a designated person or entity (directly or indirectly); and
- keep records of the due diligence that is conducted.

The ASO provides a [checklist on what you can do](#) to comply with, and reduce your risk of contravening, Australian autonomous cyber sanctions laws. We recommend you review the ASO's website for further information ([Australia and sanctions | Australian Government Department of Foreign Affairs and Trade \(dfat.gov.au\)](#)).

Q8. What happens if I have made a ransomware payment to a designated person and/or entity?

It is strongly recommended not to pay a ransom.

- Making a ransomware payment does not guarantee sensitive data will be recovered, nor prevent it from being sold or leaked online. You may also be targeted by another attack. It also makes Australia a more attractive target for criminal groups.
- Making or facilitating a ransomware payment may breach Australian sanctions laws and result in criminal penalties where such payments are made to persons or entities subject to Australian autonomous sanctions laws.
- Making or facilitating a ransomware payment may also breach other Commonwealth or state criminal laws.

Ransomware and cyber extortion incidents pose some of the most significant and destructive cybercrime threats to Australian individuals and organisations. Ransomware uses malicious software to cripple digital infrastructure by encrypting devices, folders and files, rendering essential computer systems inaccessible unless a ransom is paid. Cybercriminals may also demand a ransom to prevent data and intellectual property from being leaked or sold online. Cyber extortion occurs where cybercriminals exfiltrate commercially sensitive or personal data from victims, threatening sale or release if extortion demands are not met.

The ransomware business model is fuelled by payments made to cybercriminals, with cryptocurrency transactions enabling malicious actors to anonymously profit from extortion claims.

If you identify that you have undertaken an activity in contravention of an Australian sanctions law (including making a ransomware payment to a designated person or entity) without a permit to do so, please **notify the Australian Sanctions Office (ASO) immediately** via the [Contact Us form on Pax](#) or by email at sanctions@dfat.gov.au.

The ASO wants to work with you to ensure everyone understands their responsibilities to comply with Australia's autonomous sanctions laws. The ASO will work with you to prevent and address breaches.

If you are asked to pay, or have paid, a ransom you should also:

- Call the Australian Cyber Security Hotline on 1300 CYBER1 (1300 292 371) for cyber security assistance; and
- Report the cybercrime, incident or vulnerability to ASD <https://www.cyber.gov.au/report-and-recover/report>
- Inform the ASO via the [Contact Us form on Pax](#) or by email at sanctions@dfat.gov.au if you think you have made a payment to a designated person or entity.

Q9. Will I be prosecuted for making a ransomware payment to a designated person and/or entity?

It is strongly recommended not to pay a ransom.

The Government's focus is on pursuing and deterring perpetrators of malicious activity and the sanctions are directed towards that end.

The Government's priority is to assist Australians who find themselves victims of such attacks.

The Government encourages victims of ransomware attacks to:

- Call the Australian Cyber Security Hotline on 1300 CYBER1 (1300 292 371) for cyber security assistance; and
- Report the cybercrime, incident or vulnerability to ASD <https://www.cyber.gov.au/report-and-recover/report>
- Inform the ASO via the [Contact Us form on Pax](#) or by email at sanctions@dfat.gov.au if you think you have made a payment to a designated person or entity.

While the Government strongly discourages the payment of ransoms, the focus of the cyber sanctions framework is to disrupt and frustrate the perpetrators of malicious cyber activity, such as ransomware attacks, and not to punish victims of crime.

That a victim had engaged with the Government concerning the ransomware attack and/or voluntarily disclosed the fact of the ransom payment would be taken into account in any decision to pursue any enforcement or compliance action.

OFFICIAL

The Australian Sanctions Office (ASO) considers on a case-by-case basis whether to refer a suspected sanctions breach to the Australian Federal Police (AFP) for enforcement action. Where a ransomware payment has been made to a designated person and/or entity, the ASO may generally consider as mitigating factors against referral to the AFP:

- (i) the ransomware incident being reported to the relevant cyber authorities, including the AFP;
- (ii) a prompt and voluntary disclosure to the ASO, as soon as possible; and
- (iii) any other relevant information.

Q10. What if I think I've made a mistake and not complied with Australian autonomous sanctions law?

Notify the Australian Sanctions Office (ASO). If you identify that you have undertaken an activity in contravention of an Australian sanctions law, without a permit to do so, please notify the ASO immediately by using the [Contact Us form on Pax](#).

The ASO wants to work with you to ensure everyone understands their responsibilities to comply with Australia's autonomous sanctions laws. The ASO will work with you to prevent and address breaches.

Q11. What if I have information on activity that is possibly illegal under Australian autonomous sanctions laws?

If you have any information in relation to a possible contravention of an Australian sanctions law, please notify the Australian Sanctions Office (ASO) by using the [Contact Us form on Pax](#) or notify the Australian Federal Police (AFP) or Australian Border Force (ABF).

Information on how to contact the AFP and report a crime is provided on the [AFP's website](#). Suspicious or illegal immigration, customs and/or border-related activity can be reported through the ABF's [Borderwatch](#) program.

If you have information relating to cybercrime activities, you should also:

- Call the Australian Cyber Security Hotline on 1300 CYBER1 (1300 292 371) for cyber security assistance; and
- Report the cybercrime, incident or vulnerability to ASD <https://www.cyber.gov.au/report-and-recover/report>.
- Inform the ASO via the [Contact Us form on Pax](#) or by email at sanctions@dfat.gov.au.

Q12. What are my obligations if I hold, or think I may hold a controlled asset of a designated person and/or entity?

Under Australian autonomous sanctions laws the responsibility to freeze an asset subject to targeted financial sanctions rests with the person or entity that holds the asset – for example, the financial institution that holds the funds of a designated person and/or entity.

If you are, or think you may be, using or dealing with an asset that is owned or controlled by a designated person or entity (that is, you are holding a freezable or controlled asset), you must hold (or 'freeze') the asset and inform the Australian Federal Police (AFP) as soon as possible.

Asset holders are required by law to provide the AFP with specific information about freezable or controlled assets. Information on how to contact the AFP is available on the [AFP's website](#).

We also recommend you inform the Australian Sanctions Office (ASO) via the [Contact Us form on Pax](#) or by email at sanctions@dfat.gov.au if you are, or think you may be, holding a freezable or controlled asset.

Q13. Do I have to comply with the sanctions laws of other countries?

The sanctions laws of other countries may apply to the activities of Australian citizens or Australian-registered bodies corporate, whether undertaken in Australia or overseas. It is your responsibility to ensure you do not contravene sanctions laws.

OFFICIAL

You should consider the wider legal and commercial context of your trade and investments and seek your own legal advice on whether you might be affected by the sanctions laws of another country.

The ASO cannot provide you with legal advice, including on the laws of another country.

Q14. If I applied for a permit, on what basis, would the Minister for Foreign Affairs (or the Minister's delegate) issue a permit to undertake an activity that would otherwise contravene Australian autonomous sanctions laws?

It is strongly recommended not to pay a ransom.

The Minister for Foreign Affairs (or the Minister's delegate) may, at the request of an applicant, consider granting a sanctions permit to allow an activity that would otherwise be prohibited under the Cyber Sanctions Framework provided **both** of the following two conditions are met:

- It would be in the 'national interest' to grant a permit, which will depend on the particular circumstances of the case.
 - The Minister or delegate will consider all relevant considerations in making an assessment of whether the granting of a permit is in the national interest.
- The application is for an activity that is a:
 - basic expense dealing; or
 - legally required dealing; or
 - contractual dealing.

You should consider getting your own legal advice if you think your proposed activity is affected by sanctions and may meet the criteria for a permit.

Go to [Sanctions Permits](#) for information on permits, including how to apply.

Q15. Will a permit be granted to make a ransomware payment to a designated person or entity?

It is strongly recommended not to pay a ransom.

- Paying a ransom does not guarantee sensitive data will be recovered, nor prevent it from being sold or leaked online. You may also be targeted by another attack. It also makes Australia a more attractive target for criminal groups.
- Making or facilitating a ransomware payment may breach Australian sanctions laws and result in criminal penalties where such payments are made to persons or entities subject to targeted financial sanctions.

If you are asked to pay a ransom you should:

- Call the Australian Cyber Security Hotline on 1300 CYBER1 (1300 292 371) for cyber security assistance; and
- Report the cybercrime, incident or vulnerability to ASD <https://www.cyber.gov.au/report-and-recover/report>.
- <https://www.cyber.gov.au/report-and-recover/report>.
- Inform the ASO via the [Contact Us form on Pax](#) or by email at sanctions@dfat.gov.au if you think will be making a payment to a designated person or entity.

Sanctions permit applications are considered on a case-by-case basis. A sanctions permit may be provided on application if the Minister for Foreign Affairs (or the Minister's delegate) is satisfied that it would be in the national interest to grant a permit and the application is in relation to an activity that is a basic expense dealing, a legally required dealing or a contractual dealing. The Minister may also grant a permit on their own initiative.

If you believe your proposed activity is affected by sanctions and that you meet the criteria for a permit, you should consider getting your own legal advice and, if appropriate, submit an application for a sanctions permit through [Pax](#), ensuring you provide all relevant information.

Further information on permits and how to apply is available at [Sanctions Permits](#).

Q16. Does the Australian Government plan to ban the payment of ransoms for cyber-related extortion?

It is strongly recommended not to pay a ransom.

- Paying a ransom does not guarantee sensitive data will be recovered, nor prevent it from being sold or leaked online. You may also be targeted by another attack. It also makes Australia a more attractive target for criminal groups.
- Making or facilitating a ransomware payment may breach Australian sanctions laws and result in criminal penalties where such payments are made to persons or entities subject to targeted financial sanctions.

If you are asked to pay, or have paid, a ransom you should:

- Call the Australian Cyber Security Hotline on 1300 CYBER1 (1300 292 371) for cyber security assistance; and
- Report the cybercrime, incident or vulnerability to ASD <https://www.cyber.gov.au/report-and-recover/report>.
- Inform the ASO via the [Contact Us form on Pax](#) or by email at sanctions@dfat.gov.au if you think you will be making a payment to a designated person or entity.

The Government will seek to co-design a ransomware reporting obligation for businesses to report any ransomware incident or extortion claim and/or payment.

It is important that businesses and individuals undertake their own due diligence to ensure the payment of a ransom does not contravene Australian autonomous sanctions law.

It is recommended that you inform yourself about persons or entities that may be connected with the ransomware demand to ensure you do not contravene Australian autonomous sanctions law. It is recommended you get your own legal advice to ensure you are fully informed.

The recently released [2023-2030 Australian Cyber Security Strategy](#) outlines new measures that assist organisations in securing their data and systems, and accessing support from government and other service providers.

Q17. Does the imposition of sanctions under Australian autonomous cyber sanctions laws for ransomware incidents amount to the banning of ransomware payments by stealth?

It is strongly recommended not to pay a ransom.

- Paying a ransom does not guarantee sensitive data will be recovered, nor prevent it from being sold or leaked online. You may also be targeted by another attack. It also makes Australia a more attractive target for criminal groups.
- Making or facilitating a ransomware payment may breach Australian sanctions laws and result in criminal penalties where such payments are made to persons or entities subject to targeted financial sanctions.

If you are asked to pay a ransom you should:

- Call the Australian Cyber Security Hotline on 1300 CYBER1 (1300 292 371) for cyber security assistance; and
- Report the cybercrime, incident or vulnerability to ASD <https://www.cyber.gov.au/report-and-recover/report>.
- Inform the ASO via the [Contact Us form on Pax](#) or by email at sanctions@dfat.gov.au if you think you will be making a payment to a designated person or entity.

Q18. What measures will the *2023-2030 Australian Cyber Security Strategy* take to address the threat of ransomware?

Ransomware and cyber-related extortion, espionage and fraud have become significant threats to Australians and Australian organisations, large and small. Data breaches have demonstrated that more needs to be done to make sure the right legal and policy settings are in place to break the food chain when it comes to ransomware and cyber-related extortion demands from, and payments to, cybercriminals.

The *2023-2030 Australian Cyber Security Strategy* (Strategy) has a strong focus on lifting our collective cyber resilience, to minimise the likelihood of a ransomware attack.

As part of this, under the Strategy, the Australian Government will seek to co-design a ransomware reporting obligation for businesses to report any ransomware incident or extortion claim and/or payment. Timely reporting of ransomware and cyber extortion incidents is needed to enhance whole-of-economy risk mitigation and preparedness and help tailor victim support services. This will ultimately bolster our collective security and strengthen our defences against future cyber attacks.

Under the Strategy, the Australian Government is amplifying domestic law enforcement and offensive capability to disrupt cybercrime activities both nationally and internationally, including through Joint Standing Operation Aquila, led by the Australian Federal Police (AFP) and the Australian Signals Directorate (ASD).

Operation Aquila focusses on investigating, targeting and disrupting the highest-priority cybercrime threats and syndicates impacting Australia, both nationally and internationally, with a priority on ransomware threat groups. Through Operation Aquila, the AFP and ASD, use offensive cyber capability as a criminal investigation tool towards prosecution and disruption, including proactively identifying and disrupting top tier cybercriminals and cybercrime syndicates, and shaping the online environment to deter cybercriminals from targeting Australia.

Australia is also an active participant in the United States-led Counter Ransomware Initiative, including by chairing and coordinating the International Counter Ransomware Task Force.