Financial institutions
Energy
Infrastructure, mining and commodities
Transport
Technology and innovation
Life sciences and healthcare

NORTON ROSE FULBRIGHT

Asia Pacific insights

Business ethics and anti-corruption

Issue 13 / November 2017

In this issue:

From the editor

Many thanks for picking up a copy of Issue 13 of our *Asia Pacific Insights* into Business ethics and anti-corruption matters. We hope our articles will be useful to your work.

Rapid technological advancements pose profound challenges to the cyber-security landscape and personal data protection. As many countries take steps to address these critical issues, Singapore is seeking to introduce new laws through its Cybersecurity Bill and make amendments to the Personal Data Protection Act in a bid to keep pace with the changing digital landscape and take the lead in becoming a Smart Nation. Stella Cramer, Magdalene Lie, Jeremy Lua and I review these upcoming legal changes.

In another sign of convergence between Australia and the UK, the Australian Government has announced that it will introduce legislation to tackle modern slavery. Abigail McGregor, JP Wood and Greg Vickery examine the similarities and differences between the UK Modern Slavery Act and the upcoming Australian regime, and consider the steps that Australian businesses can take to prepare for the new law.

Sanctions continue to be a hot topic under the new US Trump Administration. My US-based colleagues Steve McNabb and Kim Caine take a look at the stiff sanctions imposed on Russia, Iran and North Korea. The broad reach of US sanctions laws has extended to Asia, including Singapore. Steve, Kim and Vijay Rao team up with Singapore-based US counsel Paul Sumilas to review the case of a Singapore company that got entangled in the web of US sanctions on Iran.

If you would like to discuss the matters raised in any of these articles or on other business ethics issues, please feel free to contact us.

Wilson Ang
Partner
Tel +65 6309 5392
wilson.ang@nortonrosefulbright.com

Contents

Singapore proposes changes to cybersecurity and data protection regimes

In a bid to keep pace with advancements in the technological landscape, the Singapore Government has embarked on public consultations on its draft Cybersecurity Bill (the Cyber Bill) and its proposed amendments to Singapore's Personal Data Protection Act (PDPA) to update the country's data protection regime. These changes will have a significant impact on how companies manage personal data and secure their information systems.

This article seeks to summarize the proposed changes to the Singapore cybersecurity and data protection regulatory framework and provide some brief thoughts on how this may impact organizations operating in Singapore.

Draft Cyber Bill

The draft Cyber Bill was unveiled on July 10, 2017. On the same day, the Cyber Security Agency (CSA) and the Ministry of Communications and Information (MCI) launched a public consultation to seek views and comments from the industry and members of public on the Cyber Bill. Originally scheduled to end on August 3, 2017, the public consultation period was extended due to widespread interest in the legislation. The Cyber Bill comes on the back of various moves by the Singapore Government to strengthen its approach to cybersecurity, starting with the setting up of the CSA in April 2015, the launch of Singapore's Cybersecurity Strategy in October 2016, and more recently, the amendments to the Computer Misuse and Cybersecurity Act earlier this year.

Who is covered – Critical Information Infrastructure

A key thrust of the Cyber Bill is the identification of 11 critical sectors as providing "essential services" and the ability of the CSA to designate as Critical Information Infrastructure (CII) any computer or computer system necessary for the continuous delivery of essential services. Such provision apply to both the public and the private sector.

The 11 critical sectors identified are

- Energy
- Info-communications
- Water
- Healthcare
- Banking and finance
- Security and emergency services
- Aviation
- Land transport
- Maritime
- Government
- Media

As mentioned, computers and computer systems that are necessary during times of national emergency may be designated as CIIs – and so such designation could potentially cover any industry.

The CSA may also designate a person as the owner of a CII, which the Cyber Bill proposes to define as a person who has effective control over the operations of the CII and has the ability and right to carry out changes to, or is responsible for, the continuous functioning of the CII. The CSA may require certain information in advance from the owner to determine if a system is a CII. The designation of systems as CII will be treated as an "official secret" under the Official Secrets Act, and will not be divulged to the public.

Duties of CII owners

CII owners are subject to the following statutory duties to

- Provide information.
- Comply with codes and directions.
- Report incidents – i.e. breach notification to the CSA.

- Conduct audits by an auditor approved by the Commissioner of Cybersecurity (the Commissioner).
- Conduct risk assessments.
- Participate in exercises.

In addition, CII owners are required to comply with any code of practice or relevant standard issued under the Cyber Bill. Failure to comply with these duties would be a criminal offence due to the national security implications of non-compliance.

CSA is the central cybersecurity authority

The Cyber Bill proposes to vest the extensive supervisory and regulatory powers on a Commissioner of Cybersecurity (the Cyber Commissioner), which is a position that will be held by the Chief Executive of the CSA.

CSA – extensive enforcement powers

Apart from its supervisory powers over CIIs, the Cyber Bill also confers on the Cyber Commissioner significant powers to respond to, and prevent, cybersecurity incidents. These powers include the power to examine persons, produce evidence, and where satisfied that the cybersecurity threat meets a certain specified severity threshold, impose measures requiring a person to carry out remedial measures or to cease certain activities, take steps to assist in the investigation and perform a scan of a computer or computer system to detect cybersecurity vulnerabilities. Property may also be seized. These powers apply to all computer or computer systems in Singapore, and are not limited to CIIs.

The Minister has the power to impose extraordinary emergency cybersecurity measures and requirements if the Minister is satisfied that it is necessary for the purposes of preventing, detecting or countering any threat to the essential services or national security, defence, foreign relations, economy, public health, public safety or public order of Singapore. This includes the power to authorize a specified person to direct another person to provide information "relating to the design, configuration or operation of any computer, computer program or computer [service][system]" if it is necessary to identify, detect or counter any such threat.

Companies and institutions should therefore be prepared for such actions, and have the necessary protocols in place to facilitate and respond to these investigations and regulatory actions.

Assistant Cyber Commissioners – from Sector Leads

The Cyber Bill grants the Minister the power to appoint as Assistant Commissioner public officers from other Ministries or from other regulators. This is an unusual feature as certain public officials would be double-hatting as an Assistant Commissioner of Cybersecurity (Assistant Cyber Commissioner) while being an official from another Ministry or statutory body performing a similar regulatory/supervisory function.

Assistant Cyber Commissioners are, in most cases, "Sector Leads" in the respective sectors, i.e. the lead government agency in charge of each sector. Therefore, CII owners should already know the Assistant Cyber Commissioners from existing regulatory relationships. For example, the Assistant Cyber Commissioner for financial institutions would likely be an officer from the Monetary Authority of Singapore (MAS). Hopefully, this will help cut down the bureaucratic burden on CII owners when dealing with a new regulator for cybersecurity issues by allowing continuity and consistency of established relationships with existing regulators.

Regulating cybersecurity service providers

There is a proposal to license and regulate cybersecurity service providers. It is recognized that since cybersecurity service providers are given access to customer systems and networks, they gain a deep understanding of system vulnerabilities, and that there should be some assurance concerning ethics and standards these providers should meet. The Cyber Bill proposes a licensing framework for cybersecurity service providers for two types of licences – investigative cybersecurity services (penetration testing) and non-investigative cybersecurity services (managed security operations). The list of licensable services is set out in the Second Schedule.

Licensed providers will need to meet certain basic requirements: key executive officers are to be fit and proper; retention of service records for 5 years; compliance with a code of ethics; and ensuring that employees performing the services are fit and proper. These requirements will also apply to overseas providers.

At this stage, it is not clear how the CSA would evaluate applicants for licensing, and the CSA will have a further consultation with industry on detailed requirements before it is implemented.

Comment

Singapore's strategy of being a smart nation and financial centre has at its core a resilient and strong foundation in cybersecurity. The Cyber Bill helps ensure that this objective is achieved by focusing on the continuity of essential services in Singapore. It also comes at a time when the business world is reeling from the impact of the WannaCry and NotPetya attacks.

The Cyber Bill takes a holistic approach to the regulation of cybersecurity by giving the CSA oversight of the regime and enforcement powers to police the regime; providing a framework for regulation of critical information infrastructure systems, including mandatory breach notification; and establishing a licensing framework for cybersecurity service providers.

The consultation paper notes that the regulatory framework will be flexible to take account of the unique circumstances of each sector. It will also require a proactive approach to enhance cybersecurity before threats and incidents happen – based on the risk profile of the sector. Offences and penalties are to ensure compliance with the Cyber Bill rather than punish those that suffer from cyberattacks.

Proposed changes to the PDPA

Hot on the heels of CSA and MCI's public consultation on the draft Cyber Bill, the Personal Data Protection Commission (PDPC) announced a public consultation on proposed changes to the PDPA on July 27, 2017.

In summary, the PDPC proposes to make two significant changes to Singapore's data protection regime

- To relax the requirement for organizations to obtain consent before processing personal data, making it easier for online businesses to collect and share data and encouraging the growth of new technologies such as Internet of Things devices and artificial intelligence.
- To introduce a mandatory breach notification requirement, in response to the increasing frequency of cyberattacks and personal data theft.

The proposed changes reflect the twin challenges Singapore faces in its push to transition to the digital economy.

Proposed relaxation of the consent requirement

Under the current data protection regime, organizations must obtain consent from individuals before collecting, using or disclosing their personal data. Consent is not required in limited circumstances, for example, where consent is deemed, or where it is necessary for any investigation or proceedings.

The PDPC proposes to allow organizations to process personal data without consent

- Where it has notified the individual of the purpose for which his personal data was processed. The organization must meet two conditions to rely on this exception
  - It is impractical for the organization to obtain consent.
  - The collection, use or disclosure of personal data is not expected to have any adverse impact on the individuals.
- Where the processing is necessary for legal or business purposes. An organization relying on this exception need not notify the individual that his personal data has been processed, if it can meet two conditions
  - It is not desirable or appropriate to obtain consent from the individual.
  - The benefits to the public (or a section thereof) clearly outweigh any adverse impact or risks to the individual.

While consent is not required in these two exceptions, the organization still has to conduct a risk and impact assessment of the consequences of processing the data without consent.

Proposed mandatory breach notification

Under the current data-protection regime, organizations are not required to notify any party following a data breach. Instead organizations are encouraged to voluntarily notify the PDPC in the event of a data breach that may cause public concern or where there is a risk of harm to a group of affected individuals. This has led to uneven notification practices across organizations.

In light of Singapore's smart nation initiative and its push towards a digital economy, the PDPC proposes to introduce a mandatory data breach notification requirement under the amended PDPA. The salient features of the PDPC's mandatory breach notification are set out as follows.

Criteria for notification

- Notification to both affected individuals and PDPC if the data breach poses any risk of impact or harm to affected individuals.

- Notification to the PDPC if the scale of the data breach is significant even if the risk of impact or harm is minimal. In this regard, the PDPC has proposed defining a breach involving 500 or more affected individuals as being of a significant scale so as to require notification to the PDPC.

Concurrent notification

For organizations that are currently required to notify their sectoral regulator or a law enforcement agency in the event of a data breach under other written law, the PDPC proposes to require such organizations to concurrently notify the sectoral regulator / law enforcement agency and the PDPC in accordance with the notification requirements under the other written law. As for organizations required to notify affected individuals under other written law, they will be considered to have fulfilled their breach obligations under the PDPA if the affected individuals have been notified according to the requirements under the other written law.

Obligations of data intermediary

The PDPC proposes to require data intermediaries (DI) to immediately inform the organization that it processes the personal data on behalf of in the event the DI suffers a data breach, regardless of the impact or scale of the breach. The organization will then be responsible for complying the mandatory breach notification requirements under the PDPA.

Exception and exemptions from breach notification

The PDPC proposes that the exclusions under section 4 of the PDPA should apply to the proposed breach notification requirement. In addition, the PDPC also proposes two further exemptions for organizations from the requirement to notify affected individual: where notification to affected individuals is likely to impede law enforcement investigations, and where the breached personal data is encrypted to a reasonable standard. Further, the PDPC may also further exempt organizations from the breach notification requirements in order to cater to exceptional circumstances where notification to affected individuals may not be desirable and the PDPA and the other laws do not provide for such notification.

Time frame for notification

In respect of affected individuals, the PDPC proposes that organizations notify them "as soon as practicable", and does not impose any fixed time cap for such breach notification. In respect of breach notification to the PDPC, the "as soon as practicable" standard similarly applies, subject to a time-cap of no later than 72 hours from the time the organization becomes aware of the data breach.

Comment

In our view, the proposed change to the consent requirement is welcome, albeit somewhat surprising, given the trend of increasing regulation of personal data in recent years. It would give organizations flexibility in deciding whether they wish to obtain consent in any given situation.

However, clarification is needed in respect of several terms used in these exceptions ("impractical", "desirable", "benefits to the public"). For instance, an organization may claim that collecting data is necessary for any "business purpose" (including to lower costs), and to therefore do away with the need to obtain consent. While encouraging for digital businesses, the proposals require refinement by the PDPC in order to avoid tipping the balance against individuals and their ability to control the use of their personal data.

Similarly, refinement by the PDPC is also needed in respect of its proposal to introduce mandatory breach notification.

First, the proposal to require notification to both affected individuals and to the PDPC if the data breach poses any risk of impact or harm to the affected individuals may be too onerous. There are certain situations where the impact or harm of a data breach to affected individuals may be minimal or insignificant, e.g. if the nature of the breach itself is unlikely to result in actual access or use of the data by a third party (e.g. in a ransomware attack) or if the data breach was discovered early and sufficient mitigatory measures had been put in place to minimize such risks. Instead, an approach based on materiality may be more practicable and relevant.

Second, the proposal to designate a breach involving 500 or more individuals as a "significant" breach is arbitrary. The number of individuals affected by a breach may not necessarily be determinative of any systemic issue within any organization.

Third, the proposed concurrent application of PDPA data breach notification requirements together with similar obligations imposed under other written law is onerous and curiously out of sync with the approach adopted proposed by MCI and the CSA in the draft Cyber Bill, i.e. the appointment of Assistant Cyber Commissioners that are "sector leads" (see above). Organizations that are currently subject to breach notification requirements imposed by other regulators, e.g. MAS in respect of financial institutions, would already be subject to supervision on such matters. Concurrent breach notification would only serve to increase the compliance burdens of such organizations, even if

requirements are harmonized. It should be noted that organizations faced with a data breach would be in crisis-resolution mode; resources should be directed at managing and resolving the breach, rather than managing requests for information from multiple regulators. In our view, the PDPC should consider aligning its approach to concurrent data breach notification with that proposed in the draft Cyber Bill, through the appointment of liaisons that are officers from "sector leads". This would prevent the wastage of precious resources in a crisis-environment caused by concurrent reporting to various regulators on overlapping matters.

Conclusion – what these legislative changes may mean for your organization

Organizations operating in a critical sector and potentially owning CIIs should put in place an overarching cybersecurity policy tailored to the organization's needs and the requirements of the regime. This policy should set out the organization's approach to meeting its legal and regulatory obligations, and specify who is accountable for the CII within the organization. Ideally, this person should be at C-suite level.

As a result of the Cyber Commissioner's powers to respond to, and prevent, cybersecurity incidents, and the mandatory breach notification requirement proposed by the PDPC, we recommend that all organizations should have in place a comprehensive cyber-response plan that includes protocols for responding to, and cooperating with, requests from the Cyber Commissioner/PDPC on cybersecurity and cyber breaches. This will minimize disruption to operations and ensure compliance with regulatory obligations.

Cost of compliance will undoubtedly increase – in particular with respect to ensuring compliance with the mandatory breach notification requirement and the new licensing regime for cybersecurity service providers that will likely be passed onto customers. However, given the impact of recent cyberattacks on business such as WannaCry and the NotPetya ransomware, this is likely the new reality and cost of doing business in a technology enabled world.

On the data privacy front, while the relaxation of the consent requirement will be a welcome change for businesses, organizations should still be aware that regulatory risks remain and that significant resources are still required to ensure compliance with the PDPA.

For more information contact:

Stella Cramer
Partner, Singapore
Tel +65 6309 5349
stella.cramer@nortonrosefulbright.com

Wilson Ang
Partner, Singapore
Tel +65 6309 5392
wilson.ang@nortonrosefulbright.com

Magdalene Lie
Associate, Singapore
Tel +65 6309 5321
magdalene.lie@nortonrosefulbright.com

Jeremy Lua
Associate, Singapore
Tel +65 6309 5336
jeremy.lua@nortonrosefulbright.com

ASIFMA, advised by Norton Rose Fulbright, responds to consultation on changes in the Singapore Personal Data Protection Act

The Asia Securities Industry & Financial Markets Association (ASIFMA) was advised by global law firm Norton Rose Fulbright in its response to Singapore's Personal Data Protection Commission Public Consultation on "Approaches to Managing Personal Data in the Digital Economy".

The Consultation Paper was issued on July 27, 2017 and proposed key amendments to the Personal Data Protection Act which include an enhanced framework for collection, use and disclosure of personal data, and mandatory data breach notification.

ASIFMA is an independent regional trade association with over 100 members firms comprising a diverse range of global financial institutions, including banks, asset managers and market infrastructure service providers.

What businesses need to know about the proposed Modern Slavery Act in Australia

The Australian Government's commitment to introduce regulation to tackle modern slavery is now beyond doubt.

On August 16, 2017, the Minister for Justice Michael Keenan announced that the Federal Government proposes to introduce legislation to require large businesses to report annually on their actions to address modern slavery. This announcement reinforces Australia's commitment to having one of the strongest responses to modern slavery in the world.

Following a period of consultation, the Government proposes a targeted regulatory regime under which large businesses will report annually in relation to their actions to address modern slavery against a set of minimum criteria. It also proposes a central repository of the annual statements.

Here, we outline what the reporting requirement is likely to involve and how Australian businesses can prepare for it.

What is modern slavery?

At its broadest, the term "modern slavery" specifically refers to any situations of exploitation where a person cannot refuse or leave work because of threats, violence, coercion, abuse of power or deception.

The Australian Government proposes that for the purpose of the reporting requirement, modern slavery will be defined to incorporate conduct that would constitute a relevant offence under existing human trafficking, slavery and slavery-like offence provisions set out in Divisions 270 and 271 of the Commonwealth Criminal Code.

This will mean modern slavery will encompass slavery, servitude, forced labour, debt bondage, and deceptive recruiting for labour or services.

The Government proposes to exclude practices, such as forced marriage, that they regard as unlikely to be present in business operations and supply chains.

What are the statistics?

As at June 2017, the Walk Free Foundation's Global Slavery Index estimates

- *45.8 million people globally* are subject to some form of modern slavery and collectively approximately US$150 billion per year is generated in the global private economy from forced labour alone.
- *30,435,300 people in Asia-Pacific Region* are "enslaved" (66.4 per cent of all people enslaved).
- *4,300 people in Australia* are enslaved.

Many Australian businesses may be unaware of the risk that they have slavery in their business or supply chains. Statistically, the incidence of modern slavery within Australia appears to be relatively low, but the concern is that the statistics reflect a low level of awareness of the issues, and the actual incidence may be much higher, both domestically and overseas.

Path to an Australian Modern Slavery Act

The Australian Government's proposals have clearly been influenced by international developments, particularly the introduction of the UK's Modern Slavery Act 2015.

The UK Act requires commercial organizations carrying on business in the UK with an annual turnover of £36 million or more to publish an annual statement that sets out the steps if any it has taken in the previous financial year to prevent slavery from occurring within in its operations and supply chains.

Any statement needs to be adopted by the board and signed by a director. As a result, this is an issue that requires board level attention. A number Australian businesses that operate in the UK have published statements under their Act.

Following the UK's implementation of this legislation, on February 15, 2017, the Attorney-General, Senator the Hon George Brandis QC, asked The Foreign Affairs and Aid Subcommittee to inquire into and report on establishing a Modern Slavery Act in Australia.

The announcement follows the Inquiry's initial hearings and, interestingly, pre-empts the Subcommittee's report.

Key Australian Government proposals

Like the UK Act, the Australian Modern Slavery Act will define the types of entities that will be subject to the reporting requirement. These entities may not be limited to corporations, but may include unincorporated associations and other bodies of persons, partnerships, superannuation funds and approved deposit funds.

The Act will likely apply to all businesses that are headquartered in Australia or have part of their operations in Australia and that meet the applicable revenue threshold. The Australian Government has suggested a revenue threshold that will be no lower than A$100 million total annual revenue.

It is proposed that entities report annually within five months after the end of the Australian financial year. Statements will be posted on business websites and a publicly accessible, searchable, central repository will be formed, run by the Australian Government or a third party.

Entities will need to report against a minimum set of criteria in relation to their operations and their supply chains (more on this later). In this way it differs from the UK legislation, which does not prescribe the content of statements (although it does list matters that may be included).

Statements will need to be approved at board level and signed by a director (or equivalent).

The Australian Government has said it will issue detailed guidance and awareness raising materials for businesses to assist in complying with the reporting requirement.

The Australian Government does not propose to apply the reporting requirement to Commonwealth or State and Territory procurement.

No penalty regime will be put in place, but the Australian Government will monitor compliance with the new provisions and will subject the legislation to review three years after its introduction.

What are the key dates?

The Australian Government has announced a consultation period with industry in relation to its proposals.

As the broad proposal to establish a Modern Slavery Act in Australia appears to have cross-party support, we anticipate Australian businesses could well see a Modern Slavery Bill tabled in Parliament by early 2018 and legislation enacted shortly afterwards.

What will a Modern Slavery Act mean for Australian businesses?

All the current indications are that Australia is likely to have a reporting requirement relating to modern slavery that is similar to what is already in operation in the UK. That regime could be in place as early as 2018.

While the Australian Government does not intend to include penalties for non-compliance, Australian businesses ought to expect that there will be significant public criticism of those businesses that do not comply with the legislation and that statements, once published, will be subject to intense public scrutiny, as has been the case in the UK.

The existence of a central repository of statements will facilitate the monitoring and review of statements. It is also likely to assist businesses, consumers and other stakeholders to understand the steps being taken by businesses to eradicate modern slavery in their operations and supply chains and take more effective steps to address the underlying issues.

In his announcement, the Justice Minister Michael Keenan said:

"It will support the business community to respond more effectively to modern slavery, raise business awareness of the issue and create a level playing field for business to share information about what they are doing to eliminate modern slavery."

"Importantly, it will also encourage business to use their market influence to improve workplace standards and practices."

What can Australian businesses do to prepare and respond?

To date, the UK experience is that there have been varying responses from commercial organizations to the UK reporting requirement. Although some organizations have been able to demonstrate that they have taken concrete steps towards tackling the risk of modern slavery in their operations and supply chains, others have only just begun to develop their awareness of the issues and are on a steep learning curve.

Given the Australian Government's announcement and cross-party political support for an Australian Modern Slavery Act, it makes sense for larger Australian businesses to assume an Australian Modern Slavery Act will likely be enacted in the near future and consider how they will prepare for the introduction of a reporting requirement that is likely to be similar in many respects to the UK requirement.

Bearing in mind the current proposed minimum reporting criteria, this approach ought to include consideration of at least the following steps

- Mapping the organization's structure, businesses and supply chains.
- Formulating policies in relation to modern slavery – this will involve collating current policies, identifying gaps, adapting existing policies and formulating new policies, as needed.
- Carrying out a risk assessment – identifying those parts of the business operations and supply chains where there is a risk of modern slavery taking place.
- Assessing and managing identified risks – this may include carrying out further due diligence in the entity's operations and supply chains and reviewing and adapting contract terms and codes of conduct with suppliers.
- Considering and establishing processes and KPIs to monitor the effectiveness of the steps taken to ensure that modern slavery is not taking place in the business or supply chains.
- Carrying out remedial steps where modern slavery is identified.
- Developing training for staff on modern slavery risks and impacts.

Businesses should bear in mind that apart from the introduction of new government regulation, there are many other good reasons for taking these steps, particularly at a time when businesses are facing renewed public pressure to operate sustainably and ethically.

By undertaking these steps, businesses will be well placed to respond effectively to new regulations and show that they are committed to eradicating modern slavery, in Australia and overseas, and taking concrete steps to achieve that objective.

Norton Rose Fulbright made a submission to the Inquiry (No. 72) and participated in the public hearing held in Sydney on June 23, 2017.

For more information, contact Abigail McGregor or JP Wood to discuss how modern slavery legislation may impact on your business and ways to manage your supply chain risks.

For more information contact:

Abigail McGregor
Partner, Sydney
Tel +61 2 9330 8742
abigail.mcgregor@nortonrosefulbright.com

Jehan-Philippe Wood
Partner, Perth
Tel +61 8 6212 3281
jehan-philippe.wood@nortonrosefulbright.com

Greg Vickery
Partner, Perth
Tel +61 7 3414 2857
greg.vickery@nortonrosefulbright.com

US imposes stiff sanctions on Russia, Iran and North Korea

On August 2, 2017 the US President signed into law legislation imposing stiff sanctions on Russia, Iran, and North Korea. The Countering America's Adversaries Through Sanctions Act (the "Act"), codifies and expands existing sanctions on Russia; targets additional sectors of the Russian economy and Russian persons involved in perpetuating human rights abuses, selling weapons to Syria, and other activities deemed to be detrimental to US national interests; limits the President's ability to ease sanctions on Russia; and seeks to punish North Korea for its nuclear program and Iran for its ballistic missile program and sponsorship of terrorism.

Key provisions of the Act are highlighted below.

Russia sanctions

Title II, the Countering Russian Influence in Europe and Eurasia Act of 2017, contains a package of sanctions that relate to, among other things, cybersecurity, crude oil projects, financial institutions, corruption, human rights abuses, evasion of sanctions, transactions with Russian defense or intelligence sectors, export pipelines, privatization of state-owned assets by government officials, and arms transfers to Syria.

Codification of existing sanctions

The statute codifies existing Russia sanctions imposed by the Obama administration under Executive Order (E.O.) Nos. 13660, 13661, 13662, 13685, 13694, and 13757.[1] These sanctions will remain in effect and the President may only terminate them if he submits a notice to the appropriate congressional committees, subjecting the proposed action to congressional review and approval.[2]

Expansion of sectoral sanctions

Sanctions related to the financial and energy sectors

The statute broadens Directives 1 and 2, issued by the U.S. Department of the Treasury, Office of Foreign Assets Control (OFAC) pursuant to E.O. 13662, to make dealings in new debt,[3] which have a US nexus and involve Russian banks and energy companies designated on the Sectoral Sanctions Identifications (SSI) List, more difficult by reducing the maturity period for such new debt.[4] Within 60 days of enactment of the Act, the Treasury Secretary must modify Directive 1 to prohibit the conduct by US persons and within the United States of all dealings in new debt of longer than 14 days (rather than 30 days) maturity or new equity of persons determined to be subject to the directive, as well as their property and interests in property. Directive 2 also must be modified within 60 days to prohibit the conduct by US persons or persons within the United States of all dealings in new debt of longer than 60 days (rather than 90 days) maturity of persons determined to be subject to the directive, as well as their property and interests in property.

1 Executive Order No. 13660 (79 Fed. Reg. 13493; relating to blocking property of certain persons contributing to the situation in Ukraine), Executive Order No. 13661 (79 Fed. Reg. 15535; relating to blocking property of additional persons contributing to the situation in Ukraine), Executive Order No. 13662 (79 Fed. Reg. 16169; relating to blocking property of additional persons contributing to the situation in Ukraine), Executive Order No. 13685 (79 Fed. Reg. 77357; relating to blocking property of certain persons and prohibiting certain transactions with respect to the Crimea region of Ukraine), Executive Order No. 13694 (80 Fed. Reg. 18077; relating to blocking the property of certain persons engaging in significant malicious cyber-enabled activities), and Executive Order No. 13757 (82 Fed. Reg. 1; relating to taking additional steps to address the national emergency with respect to significant malicious cyber-enabled activities).

2 H.R. 3364, sec. 222.

3 "Debt" is defined to include: (1) bonds; (2) loans; (3) extensions of credit; (4) loan guarantees; (5) letters of credit; (6) drafts; (7) bankers acceptances; (8) discount notes; or (9) commercial paper.

4 H.R. 3364, sec. 223(b) and (c).

Accordingly, the statute raises the bar for US persons to engage in debt financing and other extensions of credit involving Russian banks and energy companies designated on the SSI List (and entities owned 50 percent or more by one or more designated persons). We expect that these changes will apply prospectively.

Sanctions related to exports for new projects to produce oil

Directive 4 also is expanded to prohibit the provision, exportation, or reexportation, directly or indirectly, by US persons or persons within the United States, of goods, services (except for financial services), or technology in support of exploration or production for new deepwater, Arctic offshore, or shale projects: (1) that have the potential to produce oil; and (2) that involve any person determined to be subject to the directive or the property or interests in property of such a person who has a controlling interest or a substantial non-controlling ownership interest in such a project defined as not less than a 33 percent interest.[5]

This modification is notable for a couple of reasons. First, Directive 4 previously focused on projects within Russia or Russian waters. As modified, Directive 4 applies to projects anywhere in the world. Second, Directive 4 previously applied to projects involving persons designated under the directive (or any entity 50 percent or more owned by one or more designated persons). As modified, the coverage of Directive 4 would be broadened to include projects in which a person subject to Directive 4 has an ownership interest of 33 percent or greater. Together, these changes make it more difficult for US persons to support projects that have the potential to produce oil involving designated Russian energy companies.

The Treasury Secretary is directed to make these changes within 60 days. It appears that the changes would be made applicable to new projects only, but it is not clear how OFAC will interpret "new."

Sanctions related to the defense or intelligence sectors

The statute requires the President to impose, on and after the date that is 180 days after the enactment of the Act, sanctions on persons that he determines knowingly engage in a "significant" transaction with a person that is part of, or operates for or on behalf of, the defense or intelligence sectors of the Government of the Russian Federation, including the Main Intelligence Agency of the General Staff of the Armed Forces of the Russian Federation or the Federal Security Service of the Russian Federation.[6] The statute also instructs the President to issue, within 60 days of enactment of the Act, "regulations or other guidance to specify the persons that are part of, or operate for or on behalf of, the defense and intelligence sectors of the Government of the Russian Federation."[7]

These sanctions have extraterritorial reach. Any person, whether US or non-US, can be subject to five or more specified sanctions[8] for engaging in significant transactions with designated parties. The menu of sanctions includes, for example, denial of various forms of financial assistance (such as Export-Import Bank assistance and loans from US and international financial institutions), a ban on investments in debt or equity of the entity, restrictions on property transactions, export restrictions, procurement restrictions, and a visa ban and exclusion from the United States of corporate officers. All of these sanctions, furthermore, may be imposed on the "principal executive officer or officers of the sanctioned person, or on persons performing similar functions and with similar authorities as such officer or officers."[9] These sanctions may effectively isolate the designated parties from US and other markets or, at a minimum, significantly impair their ability to conduct business around the world.

The statute also permits the President to delay the imposition of sanctions on persons identified pursuant to these authorities if the President certifies to Congress that such persons are "substantially reducing the number of significant transactions"[10] with the Russian intelligence or defense sectors. This appears to provide companies with a wind-down period so they can terminate existing contracts and other relationships with parties that become designated.[11]

Sanctions related to export pipelines and crude oil projects

The statute authorizes the President to impose sanctions with respect to a person the President determines (1) knowingly makes an "investment" that directly and significantly contributes to enhancing Russia's ability to construct energy export pipelines, or (2) sells, leases, or provides to Russia, for the construction of Russian energy export pipelines, goods, services, technology, information, or support – any of which has a fair market value of US$1 million or more, or that, during a 12-month

5 H.R. 3364, sec. 223(d).

6 H.R. 3364, sec. 231(a).

7 H.R. 3364, sec. 231(d).

8 H.R. 3364, sec. 235. These sanctions include: (1) denial of Export-Import Bank assistance; (2) export restrictions; (3) denial of loans from US financial institutions; (4) denial of loans from international financial institutions; (5) specified prohibitions applicable to financial institutions; (6) denial of government contracts; (7) prohibition of foreign exchange transactions; (8) prohibition of transfers of credit or payments through the United States; (9) prohibition of property transactions; (10) ban on investment in equity or debt; (11) exclusion of corporate officers; and (12) sanctions on principal executive officers.

9 H.R. 3364, sec. 235(12).

10 H.R. 3364, 231(c).

11 The President also may waive the initial application of sanctions provided that the appropriate written determination and certification are provided to Congress. H.R. 3364, 231(b).

period, have an aggregate fair market value of US$5 million or more – that could directly and significantly facilitate the maintenance or expansion of the construction, modernization, or repair of energy pipelines by Russia.[12] The President's decision should be made in coordination with US allies. It remains to be seen how the President will elect to wield this authority and the impact that coordination with US allies will have on the President's decision.

The statute also amends section 4(b)(1) of the Ukraine Freedom Support Act of 2014[13] by requiring (rather than authorizing) the President to impose (unless he determines that it is contrary to the US national interest), on or after the date that is 30 days after enactment of the Act, three or more specified sanctions[14] on non-US persons determined by the President to have knowingly made a significant investment in a special Russian crude oil project.[15]

Secondary sanctions with respect to non-US financial institutions

The statute amends section 5 of the Ukraine Freedom Support Act of 2014[16] by requiring (rather than authorizing) the President to impose secondary sanctions (unless he determines that it is contrary to the US national interest), on or after the date that is 30 days after enactment of the Act, on Russian and other non-US financial institutions that knowingly facilitate: (1) significant defense and energy-related transactions (e.g. transfer of defense articles into Syria or development of special Russian crude oil projects) or (2) significant financial transactions on behalf of Specially Designated Nationals and Blocked Persons (SDNs). Non-US financial institutions determined to be knowingly facilitating any such transactions may be subject to prohibitions or strict conditions on the opening or maintenance in the United States of a correspondent or payable-through account.[17]

Limitation of President's authority to ease or terminate sanctions

Importantly, the statute limits the President's authority to waive or lift sanctions related to Russia. Before granting a waiver, terminating sanctions on a person or entity, or granting a license "that significantly alters United States foreign policy" on Russia, the President would have to submit a report to Congress describing the proposed action and the basis for it. The report would need to address whether the action is intended to change the direction of US policy toward Russia, as well as the anticipated effects on diplomacy and national security. Congress could then block the President's effort to ease or terminate the sanctions.

Iran sanctions

Title I, the Countering Iran's Destabilizing Activities Act of 2017, contains sanctions targeting persons that support terrorism, sell weapons to Iran, support its ballistic missile program, or abuse internationally recognized human rights.

It imposes sanctions on any person who contributes materially to Iran's ballistic missile program or weapons of mass destruction programs,[18] or participates in the sale or transfer of military equipment to Iran. In addition, while the US government previously has taken action against the Iranian Revolutionary Guard Corps (IRGC), the statute for the first time targets the IRGC for its support for terrorism. It requires the President to impose blocking sanctions with respect to the IRGC and non-US persons that are officials, agents, or affiliates of the IRGC.[19] The statute also calls for additional sanctions on any person determined to be responsible for torture and other violations of internationally recognized human rights.[20]

Further, the statute expands enforcement of the US arms embargo against Iran,[21] requires the President to review the applicability of sanctions relating to Iran's support for terrorism and its ballistic missile program to persons on the SDN List and to either impose such sanctions with respect to that person or exercise the prescribed waiver authority,[22] and authorizes the President to temporarily waive the imposition or continuation of sanctions under specified circumstances.[23]

12 H.R. 3364, sec. 232.

13 22 U.S.C. § 8923(b)(1).

14 The sanctions include: (1) denial of Export-Import Bank assistance; (2) procurement sanctions; (3) arms export prohibition; (4) dual-use export prohibition; (5) prohibition on property transactions; (6) prohibition on banking transactions; (7) prohibition on investment in equity or debt of sanctioned person; (8) exclusion from the United States and revocation of visa or other documentation; and (9) sanctions on principal executive officers. 22 U.S.C. § 8923(c).

15 H.R. 3364, sec. 225. Special Russian crude oil projects are projects intended to extract crude oil from (1) the exclusive economic zone of the Russian Federation in waters more than 500 feet deep; (2) Russian Arctic offshore locations; or (3) shale formations located in the Russian Federation. See 22 U.S.C. § 8921.

16 22 U.S.C. § 8923(b)(1).

17 The statute includes a host of other provisions related to Russia, including measures: (1) requiring sanctions on any person that knowingly makes or facilitates a significant investment in Russia's ability to privatize state-owned assets unjustly benefiting Russian government officials or their associates, sec. 233; requiring the President to impose sanctions on a non-US person who knowingly exports, transfers, or otherwise provides to Syria significant financial, material, or technological support, sec. 234; authorizing the Treasury Secretary to determine that state-owned entities operating in the Russian railway or metals and mining sectors may be subject to blocking sanctions pursuant to Executive Order 13662, sec. 223; requiring the President to impose sanctions against any person who knowingly engages in "significant activities undermining cybersecurity," sec. 224; amending section 9 of the Sovereignty, Integrity, Democracy, and Economic Stability of Ukraine Act of 2014, 22 U.S.C. § 8908(a), to require (rather than authorize) the President to impose sanctions with respect to significant corruption in the Russian Federation, sec. 227; and amending the Support for the Sovereignty, Integrity, Democracy, and Economic Stability of Ukraine Act of 2014, 22 U.S.C. § 8901 et seq., by requiring sanctions to be imposed related to transactions with persons that evade Russia sanctions and transactions with persons responsible for human rights abuses, sec. 228.

18 H.R. 3364, sec. 104.

19 H. R. 3364, sec. 105.

20 H.R. 3364, sec. 106.

21 H.R. 3364, sec. 107.

22 H.R. 3364, sec. 108.

23 H.R. 3364, sec. 112.

North Korea sanctions

Title III, the Korean Interdiction and Modernization of Sanctions Act, expands the sanctions related to North Korea in an effort to punish the country for its nuclear and ballistic-missile programs, target human rights abuses by the North Korean government, and limit North Korea's access to the US market.

The statute amends the North Korea Sanctions and Policy Enhancement Act of 2016[24] to increase the President's authority to impose sanctions on persons who violate U.N. Security Council resolutions regarding North Korea. For example, it expands the category of persons subject to mandatory and discretionary designations (and mandatory and discretionary asset blocking).[25] It also mandates that US financial institutions that have or obtain knowledge that a correspondent account is being used by a non-US financial institution to provide significant financial services indirectly to designated persons is no longer used to provide such services.[26]

There is an exception to this prohibition that allows a US financial institution to process transfers of funds to or from North Korea, or for the direct or indirect benefit of any designated person if the transfer arises from and is ordinarily incident and necessary to give effect to an underlying authorized transaction, and does not involve debiting or crediting a North Korean account.

In addition, the State Department is required to submit a determination, within 90 days of enactment of the Act, regarding whether North Korea meets the criteria for designation as a state sponsor of terrorism.[27]

For more information contact:

Stephen M McNabb
Partner, Washington, DC
Tel +1 202 662 4528
stephen.mcnabb@nortonrosefulbright.com

Kimberley Hope Caine
Senior associate, Washington, DC
Tel +1 202 662 0394
kim.caine@nortonrosefulbright.com

24 22 U.S.C. § 9221 et seq.

25 H.R. 3364, sec. 311(a).

26 H.R. 3364, sec. 312.

27 The statute also requires the President to determine whether certain specified Korean entities should be designated, sec. 311(d), prohibits a non-US government that provides to or receives from North Korea a defense article or service from receiving certain types of US assistance, sec. 313, requires enhanced security screening procedures and/or seizure or forfeiture with respect to certain vessels, aircraft, conveyances, or operators of sea ports or airports, sec. 314, requires the President to impose US property-based sanctions on non-US persons that employ North Korean forced laborers, id., creates a rebuttable presumption of denial of US entry with respect to goods made with North Korean labor, sec. 321(b), and adds prohibitions on US entry and operation of certain vessels, sec. 315.

Singapore company fined over US$12 million for alleged US sanctions violations

On July 27, 2017, the US Department of the Treasury's Office of Foreign Assets Control (OFAC) announced a settlement with Singapore-based CSE Global Limited (CSE) and its wholly-owned subsidiary, CSE TransTel Pte. Ltd. (TransTel) for allegedly causing at least six separate financial institutions to engage in the unauthorized exportation or re-exportation of financial services from the United States to Iran. The companies agreed to pay over US$12 million to settle the alleged violations of the International Emergency Economic Powers Act[1] (IEEPA) and the Iranian Transactions and Sanctions Regulations[2] (ITSR). CSE is an international technology group, and TransTel supplies telecommunications systems and services to the oil and gas industry. During the relevant time period, TransTel conducted business in Iran through, and owned a 49 percent stake in, an Iranian entity.

Violations

Between August 25, 2010 and November 5, 2011, TransTel entered into contracts with multiple Iranian companies, at least two of which were on the Specially Designated Nationals and Blocked Persons List (SDN List), to deliver and install telecommunications equipment related to several Iranian energy projects. These contracts included projects for the South Pars Gas Field in the Persian Gulf, the South Pars Power Plant in Assalouyeh, Iran, and the Reshadat Oil Field in the Persian Gulf. TransTel also engaged a number of third-party vendors, including Iranian companies, to provide goods and services in connection with these projects.

During this time, CSE and TransTel maintained separate US and Singaporean dollar bank accounts with an unidentified non-US financial institution located in Singapore. In April 2012, CSE and TransTel provided the bank with a letter stating that they would not route any transactions related to Iran through the bank. Despite this letter, and in connection with the projects in Iran, TransTel originated 104 fund transfers totaling over US$11 million from the Singaporean bank to multiple third-party vendors, including vendors located in Iran. These fund transfers were processed through the United States financial system and made no reference to Iran, allegedly causing multiple US financial institutions to engage in the prohibited exportation or re-exportation of financial services from the United States to Iran. Further, TransTel allegedly had knowledge and reason to know that these fund transfers would be received in Iran.

Penalty

In calculating the penalty, OFAC took into consideration the fact that CSE and TransTel did not voluntarily self-disclose their conduct, and that the alleged conduct constituted an egregious violation. OFAC also considered the following aggravating factors

- TransTel engaged in and obfuscated its involvement in known prohibited conduct, including the misrepresentations to the Singaporean bank.
- TransTel's senior management at the time had actual knowledge of, and played an active role in, the alleged conduct.
- TransTel's alleged violations resulted in significant economic benefit to Iran and/or Iranian people and companies on the SDN List.
- TransTel is a sophisticated enterprise with operations in multiple countries.

Based on the penalty guidelines, the base penalty for CSE's and TransTel's activity was over US$38 million. However, OFAC considered a number

1 50 U.S.C. § 1705(a) ("It shall be unlawful for a person to violate, attempt to violate, conspire to violate, or cause a violation of any license, order, regulation, or prohibition issued under this chapter.")

2 31 C.F.R.§ 560.204 ("...[T]he exportation, reexportation, sale, or supply, directly or indirectly, from the United States, or by a United States person, wherever located, of any goods, technology, or services to Iran or the Government of Iran is prohibited...")

of mitigating factors in calculating the penalty, including the fact that TransTel had not received any penalty notice or finding of violation in the previous five years, that TransTel and CSE both undertook remedial steps to ensure future compliance with US sanctions programs, and that TransTel and CSE both provided substantial cooperation during OFAC's investigation. Based on this, the final penalty imposed was US$12,027,066.

Key takeaways

Non-US companies are targets

The IEEPA makes it unlawful for anyone to violate or to cause a violation of any regulations or prohibitions issued under its authority (including the ITSR). While recent enforcement actions have focused on non-US banks that process US dollar transactions with sanctioned countries and not the non-US customers of those banks, this enforcement action is similar in principle and underscores that non-US companies that conduct sanctioned country business using US dollars can themselves be penalized for causing a violation of the ITSR.

US dollar nexus

While the use of US dollars itself is not sufficient to create OFAC jurisdiction, US dollar transactions are often routed through US financial institutions, which does provide OFAC with jurisdiction over the conduct. Non-US companies should take care when dealing with sanctioned countries or entities on the SDN List. Transactions with those parties which involve the US financial system could result in US sanctions violations.

Parent/subsidiary supervision

The misconduct occurred even though CSE allegedly instructed TransTel to screen third-party vendors for US sanctions compliance before TransTel entered into any of the Iranian contracts. Parent companies should have a compliance program designed to ensure that subsidiaries are also following applicable regulations. Indeed, simply telling a subsidiary to comply is insufficient.

Cooperation

As noted above, CSE and TransTel could have been fined over US$38 million. However, in part because of their substantial cooperation during OFAC's investigation, the settlement resulted in a fine of less than one third of the base penalty. OFAC specifically cited the fact that CSE and TransTel provided detailed information in an organized and timely manner. Once potential misconduct has been uncovered, a company should engage competent counsel to conduct a thorough investigation, so that, if necessary, the company can maximize cooperation credit with the relevant authorities while best protecting the company's interests.

Remediation

Another key reason why CSE and TransTel received a reduced fine was because they promptly took remedial steps to ensure compliance with US sanctions laws. When a compliance program fails and a company has reason to believe that violations of law may have occurred, it should take concrete and actionable steps to identify the root cause of the issue and implement measures to address the compliance shortcomings.

Conduct at the top

One of the aggravating factors here was the fact that senior management was allegedly aware of and helped facilitate the conduct. To have an effective compliance program, a company must ensure that senior executives and the board of directors consider compliance a top priority and that they actively demonstrate this belief through action.

For more information contact:

Stephen M McNabb
Partner, Washington, DC
Tel +1 202 662 4528
stephen.mcnabb@nortonrosefulbright.com

Paul Sumilas
Of Counsel, Singapore
Tel +65 6309 5442
paul.sumilas@nortonrosefulbright.com

Kimberley Hope Caine
Senior associate, Washington, DC
Tel +1 202 662 0394
kim.caine@nortonrosefulbright.com

Vijay Rao
Associate, Washington, DC
Tel +1 202 662 0211
vijay.rao@nortonrosefulbright.com

Contacts

Asia

China
Sun Hong
Tel +86 21 6137 7020
hong.sun@nortonrosefulbright.com

Hong Kong
Alfred Wu
Tel +852 3405 2528
alfred.wu@nortonrosefulbright.com

India
Sherina Petit
Tel +44 20 7444 5573
sherina.petit@nortonrosefulbright.com

Japan
Eiji Kobayashi
Tel +81 3 5218 6810
eiji.kobayashi@nortonrosefulbright.com

Singapore
Wilson Ang
Tel +65 6309 5392
wilson.ang@nortonrosefulbright.com

Paul Sumilas
Tel +65 6309 5442
paul.sumilas@nortonrosefulbright.com

Thailand
Somboon Kitiyansub
Tel +662 205 8509
somboon.kitiyansub@nortonrosefulbright.com

Sarah Chen
Tel +662 205 8518
sarah.chen@nortonrosefulbright.com

Australia
Abigail McGregor
Tel +61 3 8686 6632
abigail.mcgregor@nortonrosefulbright.com

Global

Global head of dispute resolution and litigation
Gerard G. Pecht
Tel +1 713 651 5243
gerard.pecht@nortonrosefulbright.com

Head of business ethics and anti-corruption
Sam Eastwood
Tel +44 20 7444 2694
sam.eastwood@nortonrosefulbright.com

Global resources

Norton Rose Fulbright is a global law firm. We provide the world's preeminent corporations and financial institutions with a full business law service. We employ 4000 lawyers and other legal staff based in more than 50 cities across Europe, the United States, Canada, Latin America, Asia, Australia, Africa, the Middle East and Central Asia.

People worldwide

>7000

Legal staff worldwide

>4000

Offices

59

Key industry strengths

- Financial institutions
- Energy
- Infrastructure, mining and commodities
- Transport
- Technology and innovation
- Life sciences and healthcare

Our office locations

Europe

Amsterdam
Athens
Brussels
Frankfurt
Hamburg
Istanbul
London
Luxembourg
Milan
Monaco
Moscow
Munich
Paris
Piraeus
Warsaw

United States

Austin
Dallas
Denver
Houston
Los Angeles
Minneapolis
New York
St Louis
San Antonio
San Francisco
Washington DC

Canada

Calgary
Montréal
Ottawa
Québec
Toronto
Vancouver

Latin America

Bogotá
Caracas
Mexico City
Rio de Janeiro
São Paulo

Asia Pacific

Bangkok
Beijing
Brisbane
Hong Kong
Jakarta[1]
Melbourne
Port Moresby (Papua New Guinea)
Perth
Shanghai
Singapore
Sydney
Tokyo

Africa

Bujumbura[3]
Cape Town
Casablanca
Dar es Salaam
Durban
Harare[3]
Johannesburg
Kampala[3]
Nairobi[3]

Middle East

Abu Dhabi
Bahrain
Dubai
Riyadh[2]

Central Asia

Almaty

1 TNB & Partners in association with Norton Rose Fulbright Australia
2 Mohammed Al-Ghamdi Law Firm in association with Norton Rose Fulbright US LLP
3 Alliances

NORTON ROSE FULBRIGHT

Norton Rose Fulbright

Norton Rose Fulbright is a global law firm. We provide the world's preeminent corporations and financial institutions with a full business law service. We have more than 4000 lawyers and other legal staff based in more than 50 cities across Europe, the United States, Canada, Latin America, Asia, Australia, Africa, the Middle East and Central Asia.

Recognized for our industry focus, we are strong across all the key industry sectors: financial institutions; energy; infrastructure, mining and commodities; transport; technology and innovation; and life sciences and healthcare. Through our global risk advisory group, we leverage our industry experience with our knowledge of legal, regulatory, compliance and governance issues to provide our clients with practical solutions to the legal and regulatory risks facing their businesses.

Wherever we are, we operate in accordance with our global business principles of quality, unity and integrity. We aim to provide the highest possible standard of legal service in each of our offices and to maintain that level of quality at every point of contact.