Cyber Security Strategy

Government of JERSEY

R.124/2017

Chief Minister's Foreword

Jersey is one of the most stable and successful international financial services centres in the world, raising the bar on good practice globally. Part of that success comes from the fact that we have always been able to reposition ourselves quickly to meet new challenges and opportunities as they appear on the horizon.

A good example of this in action is the Island's commitment to updating its Data Protection legislation to ensure that it remains adequate with the new European regime. In early 2017 the Government published the "Digital Policy Framework"[1], which brings together for the first time Jersey's digital ambitions across Government, industry and society more widely. This framework will provide the strategic direction that Jersey needs to capitalise on the benefits that digital technology will provide in years to come.

Whilst it is important that we look to digital technology as a means of improving our economy and wellbeing, we must also acknowledge that new technology brings new risks. In today's digitally connected world, cyber security has become a prerequisite for a strong society and a thriving economy; especially in the financial services sector and the expanding digital industry.

The 2015 Innovation Review[2], Digital Jersey's 2016 Opportunity Analysis[3] and the aforementioned Digital Policy Framework have all highlighted cyber security as a key building block that underpins Jersey's continued success as a jurisdiction.To ensure that Jersey continues to be seen as a stable and attractive place to live and do business, in both the physical and digital world, the Government has produced the Island's first Cyber Security Strategy.

For Islanders, we envisage a cyber resilient Island where all Islanders are informed about cyber security risks, and the essential services for maintaining life and a modern economy are as secure as possible. Having a well-educated workforce will play a key role in delivering this and will also benefit the broader economy.

For businesses, we aspire to be in a position where all businesses are fully aware of their individual cyber risks and responsibilities, have sufficient information to allow them to take the best decisions for their organisations and where cyber security is a priority for the board room. Commercial organisations have responsibility for managing their own risks, but Government can play a role by facilitating information sharing, providing appropriate minimum cyber security standards and having an effective incident response capability in place.

The Government's role is to build partnerships, raise awareness and engage with the public, whilst also directing Government's own resources to secure the Island's systems. Collaboration is essential, and this strategy brings together stakeholders who might otherwise be in competition. Government, as a critical ally, will encourage and support cyber security initiatives across the Island. This approach will not only keep the Island secure but will enhance the Island's reputation, bringing more business to the Island and contributing towards economic diversification. Government will also work with key international cyber partners such as the UK's National Cyber Security Centre (NCSC).

Strengthening cyber resilience is good for Islanders, good for businesses and good for Jersey.

[1]Link to the Digital Policy Framework: http://digitalpolicy.gov.je/
[2] Link to the Innovation Review: https://www.gov.je/SiteCollectionDocuments/Industry%20and%20finance/R%20Jersey%20Innovation%20Review%2020150911%20GB.pdf
[3] Digital Jersey's Opportunity Analysis: http://www.digital.je/media/Public_Files/DJLKPMGReport2016.pdf

Table of contents

1. The vision

The wider context

This Cyber Security Strategy (the "Strategy") contributes to Jersey's wider strategic aims as a jurisdiction. To ensure this, the Strategy has been prepared in accordance with the **strategic goals** set out in the recent "Shaping our Future" Framework (the "Framework").

The Strategy will contribute towards **four out of the ten** strategic goals, indicating a strong alignment with the Framework's goals, as illustrated below:

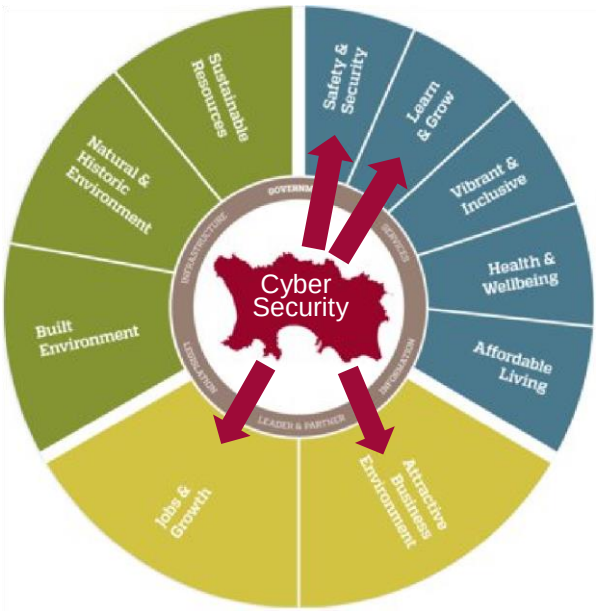


Figure 1: the ten strategic goals of Jersey's "Shaping our Future" Framework

The vision

The Internet has become an integral part of our daily lives. It allows us to communicate, socialise and do business in new and exciting ways. It enables better freedom of expression, it acts as a catalyst for innovation and is now a cornerstone of our social and economic lives. Helping all Islanders and all local businesses to be safe online will underpin our success as a jurisdiction well into the 21st century.

The cyber security vision for 2020 is to **'make Jersey a safer place to live and to do business in'** - making the Island more attractive for new and existing businesses, underpinning new growth areas such as the digital sector and enhancing Jersey's potential and brand as a jurisdiction.

Strategically, Government's role is to:

- act in a proportionate way to balance cyber security with privacy and civil liberties
- act as an enabler, partner and supportive (although sometimes critical) friend
- collaborate with, and facilitate collaboration across, business and jurisdictions
- be guided by our values of liberty, transparency and rule of law

The Strategy's vision is underpinned by five pillars. The Government is committed to fulfilling the objectives of each pillar:

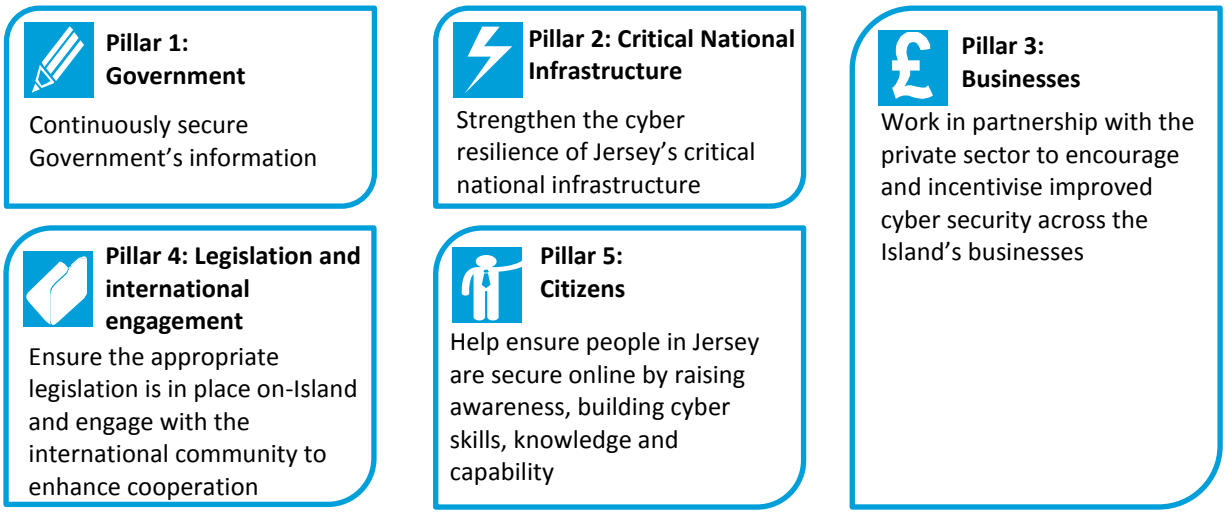


Figure 2: the Cyber Security Strategy five pillars

In order to fulfil the objectives of these five pillars, the Government has identified **eight strategic goals**:

1. Establish an information sharing, reporting and incident response capability
2. Plan for the future cyber landscape
3. Educate for the future
4. Establish a framework to continuously assess Island-wide risks
5. Create strong cyber governance across the Island
6. Foster partnership and collaboration
7. Set minimum security requirements
8. Support law enforcement

The eight strategic goals are summarised in "Chapter 2 - Executive summary" and explained fully in "Chapter 3 – Jersey's Cyber Security Strategy".

2. Executive summary

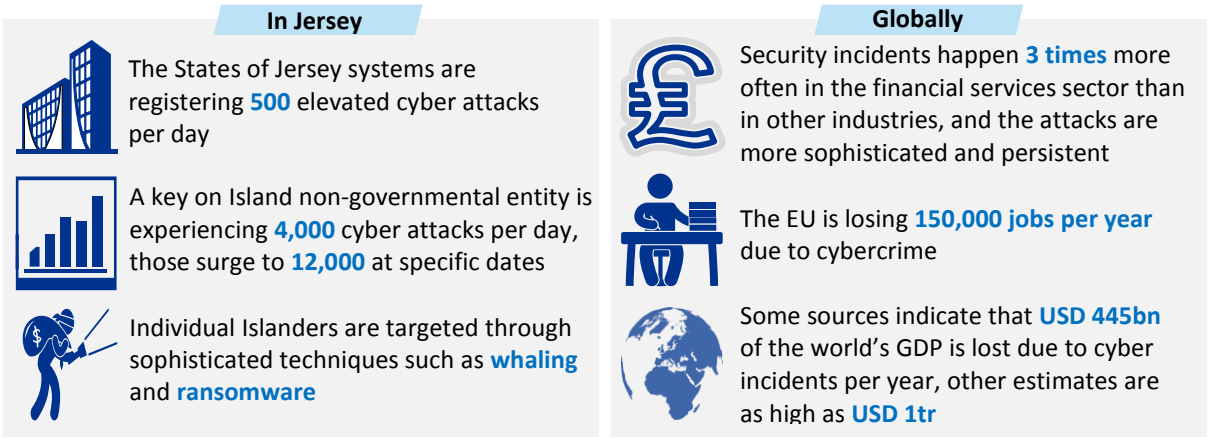
Introduction

Achieving a high standard of cyber security resilience will enable Jersey to continue to operate with confidence in the digital era. Successful implementation of this Cyber Security Strategy will underpin Jersey's continued success as an international finance centre and act as a catalyst for our digital aspirations, whilst also benefiting all Islanders.

Why does it matter?

Jersey faces similar cyber security threats to those faced by most advanced economies and the frequency and sophistication of cyber attacks is increasing. Given this context, like other jurisdictions, we need to continue to strengthen our defensive capabilities and cyber resilience.

Figure 3: Threat landscape in Jersey and globally[4]



The five pillars

There are five critical pillars to the strategy; achieving the desired level of cyber maturity in each of these five pillars will result in the entire Island being more cyber resilient. These five pillars are:

1. **Government**: Continuously secure Government's information
2. **Critical national infrastructure**: Strengthen the critical national infrastructure's cyber resilience
3. **Business**: Work in partnership with the private sector to encourage and incentivise improved cyber security across the Island's businesses
4. **Legislation and international engagement**: Ensure the appropriate legislation is in place on-Island and engage with the international community to enhance cooperation
5. **Citizens**: Help ensure people in Jersey are secure online by raising awareness, building cyber skills, knowledge and capability

[4] Jersey figures from the States of Jersey and the Cyber Security Task Force.
Global figures from: "2015 Industry Drill-Down Report: Financial Services", Websense: https://www.websense.com/assets/reports/report-2015-industry-drill-down-finance-en.pdf, Net Losses Estimating the Global Cost of Cybercrime", Mcafee and the Centre for Strategic and International Studies (CSIS): http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf

The strategic goals

Delivery of the pillars rely on eight strategic goals. The key actions relating to each of the eight goals are summarised below:

1. **Establish an information sharing, reporting and incident response capability:** We will determine ways in which an incident response capability can be made available for the Island. Establishing such a capability is key to delivering the strategy's vision. It is impossible to prevent all cyber incidents, but, when a cyber incident does happen, we must be prepared to respond swiftly and appropriately. This response will at times involve multiple entities, who must be prepared when confronted with national security incidents to set aside commercial interests and work together. Any incident response capability must also be supported by a cyber information-sharing and incident reporting mechanism.
2. **Plan for the future cyber landscape:** We will develop and conduct regular training exercises that simulate cyber attacks, using them to identify vulnerabilities and prepare for real incidents. All planning for disaster recovery will also include cyber security as a priority. These exercises will ensure that the Island is prepared to face a range of potential threats, and keeps pace with the cyber threats of tomorrow.
3. **Educate for the future:** We will strive to ensure that Jersey has a sufficient pipeline of cyber security professionals. We are exploring options to deliver appropriate educational programmes that will create and develop local specialists in cyber security. Successful delivery of this goal will require joint working with the Education Department, Highlands College, Jersey International Business School, Digital Jersey and local experts and businesses. Potential actions include updating primary and secondary educational curricula (to include up-to-date cyber security information and ensuring that support (including financial support) is in place for students planning to study cyber security for further education.
4. **Establish a framework to continuously assess Island-wide risks:** We will regularly assess the Island's cyber security risks and maturity by conducting comprehensive reviews, such as the 2015 Atkins review. Regular assessments will be used to focus our efforts, ensure flexibility in an ever changing cyber landscape, measure progress, justify spending and manage performance.
5. **Create strong cyber governance across the Island:** We will ensure that Government's internal cyber security governance structure is fit for purpose, work with our critical national infrastructure operators to confirm that they are prioritising cyber security and encourage businesses to give cyber security the appropriate attention at board level.
6. **Foster partnership and collaboration:** We will forge partnerships on and off-Island that will enhance Jersey's cyber security resilience. The fact that no one is actually risk free in the cyber space must be turned into a strength and be used to encourage collaboration and solidarity. The existing relationships with the United Kingdom (UK), the States of Guernsey and other Island nations involved in the SINCERE[5] project are the current international priorities, however we will continue to explore other potentially beneficial relationships. Potential areas for collaboration include: cooperation on cyber crime investigation, partnerships in terms of incident reporting, response capabilities and information sharing mechanisms. The Government will ask the UK to extend to Jersey its ratification of the Council of Europe Convention on Cybercrime ("the Budapest Convention"), in 2017.
7. **Set minimum security requirements:** In conjunction with critical national infrastructure partners and the business community, we will consider what baseline level of cyber security is appropriate for different types of organisations to achieve a reasonable level of security. Encouraging on-Island

[5] The "Small Island Nations Centre of Excellence for Research and Education" (or "SINCERE") project goal is to create a centre of excellence for research and education with the aim of combating cyber crime and promoting cyber crime investigation training, research and education. This project is fully funded by external sources (the European Union's budget) and involves cross-Island partnership and coordination with relevant European Union partners. The project's main partners are the police forces of Jersey, Guernsey, Isle of Man, , and Gibraltar on the islands side, Canterbury Christ Church University on the academic side and Lithuania as the project's leader.

organisations to attain baseline security requirements, where appropriate and proportionate to the risks faced, will become an effective way to protect the Island from many cyber threats. The Government is mindful of differences in security needs, the Cyber Essentials standard is proven to help some organisations achieve a minimum level of cyber security in a cost effective manner and is particularly useful for smaller organisations. We will explore how to encourage appropriate minimum cyber security requirements such as Cyber Essentials and more advanced security standards within a reasonable timeframe.

8. **Support law enforcement:** We will ensure that Jersey's legislation is fit for purpose and that the States of Jersey Police is appropriately empowered to effectively address cyber crime. Actions include forging the right partnerships (such as with EUROPOL, the FBI, etc.) and working on cross-border programs (including the SINCERE project).

Link between the vision, the strategic goals, and objectives

The overall vision of this strategy will be fulfilled by achieving the eight strategic goals presented in the previous section. In order to facilitate delivery, each of the goals has been broken down further into clear objectives, fully detailed in chapter 3 and summarised below:

Vision	Strategic goals	Strategic objectives
The cyber security vision for 2020 is to 'make Jersey a safer place to live and to do business in' - making the Island more attractive for new and existing businesses, underpinning new growth areas such as the digital sector and enhancing Jersey's potential and brand as a jurisdiction	1. Establish an information sharing, reporting and incident response capability	■ Establish trusted information sharing mechanisms ■ Establish incident reporting mechanism ■ Establish incident response capability
	2. Plan for the future cyber landscape	■ Develop Island-wide cyber attack scenarios ■ Organise Island-wide cyber security exercises ■ Develop Island-wide contingency plans
	3. Educate for the future	■ Strengthen training and educational programs
	4. Establish a framework to continuously assess Island-wide risks	■ Conduct regular national risk assessments
	5. Create strong cyber governance across the Island	■ Encourage strong cyber security governance ■ Identify and engage all relevant stakeholders
	6. Foster partnership and collaboration	■ Continue international cooperation and establish relevant on-Island partnerships
	7. Set minimum security requirements	■ Explore and set minimum security requirements
	8. Support law enforcement	■ Support law enforcement ■ Take stock of existing policies and regulations

3. Jersey's Cyber Security Strategy

3.1 Establish an information sharing, reporting and incident response capability

Strategic objective	What does good look like?
1. Establish trusted information sharing mechanisms	Government, critical national infrastructure partners, private businesses and citizens know about and are confident using information sharing mechanisms to receive timely cyber security information.
2. Establish incident reporting mechanisms	Government, critical national infrastructure partners, private businesses and citizens are confident in reporting cyber incidents using incident reporting mechanisms, enabling greater protection for all parties involved.
3. Establish incident response capability	An entity is set up to provide adequate response in case of major cyber security incidents. This entity must support the Government, critical national infrastructure and potentially business to handle major cyber security incidents whilst also promoting cyber security situational awareness across the Island. This entity will also be able to draw on the best practice available from the UK's NCSC and, for major incidents, technical support and handling guidance from the NCSC.

Background:

Jersey needs to continuously improve its ability to quickly recover from any serious attempts to compromise essential services via a cyber attack. In other jurisdictions, this is typically achieved through an incident response entity such as a computer emergency response team (CERT).

It is also important to establish an effective cyber security information sharing and incident reporting mechanism, allowing stakeholders to understand the range of threats currently faced by the Island, and to feel comfortable to report cyber incidents through this mechanism. Having appropriate intelligence is essential, evidence shows that 80%[6] of successful cyber attacks would have been prevented (or at least the consequences would have been minimised) given proper threat intelligence.

Progress made:

In the absence of a central cyber security information sharing body, some channels have been made available:

a) *Creation of the Fraud Prevention Forum (www.fraudprevention.je)*

The Jersey Fraud Prevention Forum has developed a coordinated approach to protecting the general public from online fraud. The incidents reported through the Forum are raised with the States of Jersey Police.

b) *Creation of a single point of contact within the States of Jersey Police (SOJP) for online scams (scams500@police.je)*

The SOJP has made a single point of contact available for receiving and dealing with online scams.

c) *Encourage use of Action Fraud (www.actionfraud.police.uk)*

Action Fraud is the UK's national reporting centre for fraud and cyber crime where incidents can be reported if an individual is subject to a fraud, scam or has experienced cyber crime.

[6] Ponemon Institute Research Report on Threat Intelligence: https://www.webroot.com/shared/pdf/CyberThreatIntelligenceReport2015.pdf

Proposed next steps:

- Establish trusted information sharing mechanisms; this will allow local entities to be alerted in real time about vulnerabilities
- Establish incident reporting mechanisms; this will allow the reporting of cyber incidents in a secure and private environment

The Government will introduce appropriate mechanisms for information sharing and incident reporting both for businesses and individuals.

For businesses, the Government will seek to enable access to the already established UK information sharing mechanism through the creation of a Channel Islands node on the UK CISP. This will allow participating organisations to simultaneously share information locally whilst retaining access to national and global information.

For Islanders we aim to inform the wider public on relevant cyber threats including how to protect and report them. This will be achieved by regular awareness campaigns delivered in a public-friendly way. As an initial success story we have secured a partnership with Get Safe Online[7] (GSO) to support our cyber security awareness outreach efforts.[8]

- Establish incident response capability

The Government will create a single point of contact for all on-Island organisations to request assistance in case of any cyber security incident. In most mature jurisdictions, this function is performed by a nationwide CERT or a CERT like entity. The Government has already established a link with the NCSC's incident management team, which has committed to assisting Jersey with major incidents.

It is important that any Jersey incident response capability is designed to meet the Island's needs in a proportionate manner. To understand the most appropriate model for Jersey, the Government will conduct a feasibility study. Part of this study will consider the benefits of adopting a pan-island approach in conjunction with Guernsey. The outcomes of this study will inform next steps in establishing an incident response capability.

[7] Get Safe Online is a public / private sector partnership supported by HM Government and leading organisations in banking, retail, internet security and other sectors with the objective of promoting internet security to the general public (www.getsafeonline.org).

[8] A partnership between Get Safe Online, SoJP, Prison Me No Way and a private sponsor is underway for 1 year, with the possibility of extension. It includes a customised webpage, full access to GSO's online resources, a pop-up shop and business event in both Jersey and Guernsey.

3.2 Plan for the future cyber landscape

Strategic objectives	What does good look like?
1. Develop Island-wide cyber attack scenarios	High-risk organisations have developed sufficient cyber attack scenarios and taken all reasonable precautions to either prevent attacks or minimise their impact.
2. Organise Island-wide cyber security exercises	Governmental organisations and critical national infrastructure providers regularly organise cyber security exercises. They share lessons learned with relevant parties and address discovered vulnerabilities. Members of the business community are also actively encouraged to take a similar approach.
3. Develop Island-wide contingency plans	Island-wide contingency plans for dealing with successful cyber attacks are developed, regularly exercised and updated.

Background:

Cyber security exercises that prepare for various cyber security scenarios enable the testing of emergency plans, detect specific weaknesses, increase cooperation between different sectors, identify interdependencies, stimulate improvements in business continuity planning, and help generate a culture of cooperative effort to boost resilience.

Progress made:

Cyber security exercises, wider CNI engagement and coordination with the UK

The team responsible for Government's IT systems, Information Services Department (ISD), organised its first cyber security exercise in 2015. The lessons learned were documented and followed-up. Similar exercises were also conducted by the Island's financial services regulator and the States of Jersey Police. In addition to this, the Cyber Security Task Force[9] has engaged with the CNI operators who have indicated their willingness to take part in future cyber security exercises. The CSTF has met with the UK National Cyber Security Centre's (NCSC) representatives to discuss the option of joint cyber security exercises with Jersey and the UK.

Proposed next steps:

- Develop Island-wide cyber attack scenarios

Key governmental departments, led by the ISD will develop cyber attacks scenarios against key governmental informational assets. Those scenarios will enable each department to better understand their risks from an attacker's perspective, and thus help them focus future cyber defence efforts.

Government will encourage the CNI operators and high-risk businesses (especially those within the financial sector) to follow a similar approach to test their arrangements against relevant cyber attack scenarios.

[9] The CSTF was established in December 2015 and is a joint task force bringing together the enforcement and high-tech crime unit of the States of Jersey Police, the Government's representatives (including experts managing the Government's IT systems), the Jersey Financial Services Commission, Digital Jersey Limited and the Office of the Information Commissioner. The task force's initial remit is to guide the development of the Jersey's Cyber Security Strategy and to support its implementation.

Scenarios involving cyber attacks on Islanders (such as ransomware) will be developed by appropriate governmental bodies and appropriate plans (including a communications plan) will be established to protect Islanders' interests.

- Organise Island-wide cyber security exercises

The CSTF in coordination with Jersey's Emergency Planning Officer will set-up an Island-wide "cyber security exercise team" to plan cyber security exercises for governmental organisations. This could be extended to include critical national infrastructure operators. The Government will also encourage private businesses to organise similar exercises. The planning team will identify potential synergies between organisations, coordinate joint exercises and facilitate information sharing, where appropriate. The planning team will report to the CSTF in the short to medium term although it is likely that an incident response entity would take over this role in the longer term.

- Develop Island-wide contingency plans

Governmental bodies will develop contingency plans for the event of a successful cyber attack against its systems, Government will also encourage CNI operators and high-risk businesses to follow a similar approach.

Working in partnership and facilitating collaboration, the contingency plans must coordinate across all relevant organisations and follow the key informational assets, as opposed to the traditional approach of being focused on one individual organisation only. Furthermore, cyber security must be viewed as an integral part of any organisation's business continuity planning or disaster recovery planning, as opposed to a 'bolt on' approach.

3.3 Educate for the future

Strategic objective	What does good look like?
1. Strengthen training and educational programs	Individuals can study cyber security related topics to world class standards and earn professional qualifications in Jersey. Training is available at all levels including: academic education (primary, secondary, tertiary and further education) and professional education (bespoke training courses, professional qualifications, continuous professional development).

Background:

One of the most critical elements of any comprehensive and effective Cyber Security Strategy, is the human element. Research indicates that in 2014, 95%[10] of information security incidents worldwide involved human error. Therefore, the focus of Jersey's Cyber Security Strategy is not just on systems and technology but on people and processes.

Education and skills development are essential, and cyber security training should be available at all levels from primary education (even if only as optional awareness raising) all the way to tertiary education (where it may be most appropriate to offer degrees in partnership with other educational providers from abroad) and continued professional development. The digital sector moves extremely quickly, as does the world of cyber security. It is important to ensure that Jersey has the skills required not just for today but for tomorrow and delivering this will require strong partnership and collaboration with business and with off-Island educational establishments.

Progress made:

Various initiatives organised by Digital Jersey Limited

Digital Jersey Limited is organising / hosting a a range of courses and events relevant to the cyber security industry including information security forums and cyber crime forums.

Other Initiatives

The Channel Islands Information Security Forum (CISF), a pan-Channel Islands organisation, is independently organising local events and is providing training relevant for the cyber security profession, such as the "Certified Information Systems Security Professional" certification.

Jersey International Business School ran a series of courses in 2016 to raise awareness of modern cyber threats.

[10]According to IBM's "2014 Cyber Security Intelligence Index"

Proposed next steps:

- Strengthen training and educational programs

Our ambition is that ultimately every person working in Jersey and interacting with a digital system has appropriate cyber security training.

As a flexible and well regulated jurisdiction, with a relatively small workforce, we can leverage our size advantage and train our workforce in basic cyber security skills (relevant for day to day workplace activities). This will become an integral part of Jersey's future value proposition. The training level and frequency will be proportional to the risks each employee faces.

Relevant to academic education:

The Government will encourage engagement between course providers, potential students and potential employers. Such engagement can be formalised through work experience, mentorship programs, internship opportunities, etc. and can help attract individuals to a potential career in cyber security. Furthermore, Government, in partnership with students, education providers and employees will understand how to best support individuals seeking to pursue cyber security skills and qualifications.

For tertiary education, partnerships with off-Island universities recognised for their excellence in cyber security will be established. This will support Government's wider ambitions as set out in the objectives of Jersey's Digital Policy Framework.[11]

Relevant to professional education:

The Government will work with public and private education providers to ensure Jersey is producing an appropriate level cyber security skills and expertise. This will include the ability to study for and sit professional qualifications on-Island and access continuous professional development courses.

Relevant to general public awareness:
The Government will support a range of initiatives to increase the public's understanding of cyber security and the basic steps that individuals can take to protect themselves from cyber crime. This will be achieved in partnership with organisations such as Get Safe Online, SoJP, Barclay's Digital Eagles lab, Digital Jersey and relevant charities

[11] Links to objectives 1 and 2 of Jersey's Digital Policy Framework: http://digitalpolicy.gov.je/

3.4 Establish a framework to continuously assess Island-wide risks

Strategic objectives	What does good look like?
1. Conduct national risk assessments	Island-wide risk assessments, with a specific focus on critical informational infrastructures are conducted regularly. The assessments measure the cyber resilience of the Island and aim to: focus our efforts, ensure flexibility in an ever changing cyber landscape, measure progress, justify spending and manage performance.

Background:
A number of comprehensive and sophisticated cyber security reviews have been conducted over the last two years. Continuing to perform regular reviews, always in tune with the latest developments (i.e. encompassing cloud security, zero day vulnerabilities or ransomware, etc.), is critical to keeping the Island secure.

Progress made:
"Jersey Cyber Security Review"- June 2015:
The Government commissioned Atkins Ltd to undertake an Island-wide cyber security review. This review covered critical national infrastructure, private sector companies and governmental organisations across Jersey. Findings from the Jersey Cyber Security Review are classified.

Multiple reviews of Government's own information security:
These include: the "SoJ Information Security Review" in June 2015 conducted by the Comptroller and Auditor General (C&AG), the "Information Services Department (ISD) security review" during 2015 and the "Current State Assessment" in 2014.

Proposed next steps:

- Conduct national risk assessments

The Government, in partnership with the critical national infrastructure (CNI) operators and private businesses should conduct / participate in regular Island-wide cyber security reviews (such as the recent "Atkins review"). This will help highlight existing and new vulnerabilities, will place Jersey in a good position to address them, will focus Government's cyber security efforts and will help quantify progress and measure performance.

The recommendations from all other cyber security reviews must be considered and built upon. Sufficient resource needs to be allocated (by the Government, the CNI operators and individual businesses) to implement the agreed recommendations.

3.5 Create strong cyber governance across the Island

Strategic objectives	What does good look like?
1. Encourage strong cyber security governance structures across the Island	Government has a mature governance structure in place covering cyber security. Similar structures exists across all critical national infrastructure operators and high-risk businesses[12] consider cyber security at the board level. Those governance structures address both technology and people aspects around cyber security.
2. Identify and engage all relevant stakeholders	All relevant stakeholders are identified and properly engaged with. The Jersey Cyber Security Strategy is being implemented in an inclusive, transparent manner. Jersey's core beliefs and civil liberties are being upheld and the appropriate balance between privacy and security is being struck.

Background:

To operate confidently and effectively in the modern digital environment organisations need to take a proactive approach towards cyber security. Clear governance structures help ensure cyber related issues are identified and addressed in a strategic manner and avoid the common pitfall of just "patching" issues and being reactive to cyber threats or incidents.

Progress made:

The States of Jersey Information Security Roadmap (the "roadmap") – issued in September 2015

The States of Jersey has already started to reform its internal governance processes. An Information Security Roadmap has been approved by the Council of Ministers and is being implemented. This roadmap outlines how Government's departments should approach information security. It covers key topics such as: codes of practice, departmental roles and responsibilities, security training and awareness, technical and physical security and the establishment of an information assurance function. Finally, it outlines the need to establish a cross-departmental cyber security governance board to drive and oversee the implementation of the listed recommendations.

The States of Jersey Information Security Governance Board (the "ISGB") – established in December 2015

This Board stands at the heart of the roadmap and represents Government's main governance structure on cyber security with responsibility for delivering the roadmap. The Board is chaired by the Chief Executive of the States of Jersey and is an example of how cyber security can be elevated to the board level. It accounts for all governmental informational assets and had received adequate training to fulfil its duties.

Proposed next steps:

- Encourage strong cyber security governance structures across the Island

Within Government the ISGB will continue as the core governance board responsible for cyber security across all governmental informational assets. It will oversee the delivery of the internal roadmap. Government will

[12] We have defined high-risk businesses as businesses with particular importance for Jersey's overall security, economy and international reputation.

also appoint a Jersey Information Security Officer (JISO), with an Island-wide remit, covering all five pillars of the Cyber Security Strategy.

Each organisation's board is responsible for protecting their own organisation but board members do not always treat cyber security as a priority or even as a topic for the boardroom. The Government will work with our critical national infrastructure operators to ensure they are considering cyber security as a priority and in partnership with relevant organisations (e.g. JFSC, Digital Jersey, Jersey Business, etc.), will actively encourage cyber security as a topic for the boardrooms of on-Island businesses.

- Identify and engage stakeholders

Partnership, collaboration, enhanced information sharing and buy-in are essential for the successful implementation of the strategy. The CSTF has engaged with stakeholders and this continued engagement is essential for effective implementation of the Cyber Security Strategy. Key stakeholders include governmental organisations, critical national infrastructure operators, the Island's businesses, the regulators, other non-governmental organisations (including industry representatives) and Islanders. The CSTF will continue to use existing lines of communication (the governmental website, governmental social media accounts, various professional networks, the mass media, etc.) until new ones are implemented (such as an information sharing mechanism, as described in goal 1, objective 1).

3.6 Foster partnership and collaboration

Strategic objectives	What does good look like?
1. Continued international cooperation and establish relevant partnerships	Government and its agencies (such as the States of Jersey Police) are successfully cooperating with international partners and getting access to global good practice and resources. This cooperation is increasing the Island's cyber resilience and enabling the prosecution of cyber criminals.

Background:

Government and its agencies will establish and maintain international partnership and engage in cooperation so that Jersey is better placed to address cyber security threats. On-Island, effort will be made to foster closer working between the Government, CNI operators, businesses and Islanders to present a common front and to protect against the fallout of a successful cyber attack.

Progress made:

Wider CNI engagement

Since the Atkins review in June 2015, the Government and CNI operators have continued to engage and work in partnership achieving tangible results. Government welcomes the fact that some CNI operators are addressing identified vulnerabilities and are voluntarily adopting international standards on cyber security.

Proposed next steps:

- Continued international cooperation and establish relevant partnerships

Government and its agencies will continue to lead Jersey's efforts in maintaining international cooperation and will strive to reach jointly beneficial agreements with relevant jurisdictions. The following relationships are a priority to securing Jersey's cyber space:

a. collaborating with Guernsey (where appropriate) on joint initiatives promoting cyber security
b. conducting a feasibility study of a cyber security incident response entity that will consider the benefits of a pan-island approach (see also goal 1, objective 3)
c. partnering with the UK on appropriate initiatives (including areas such as information sharing, incident reporting and incident response)
d. continuing and building upon the cooperation already established through the SINCERE project

3.7 Set minimum security requirements

Strategic objective	What does good look like?
1. Explore and set minimum security requirements	A consensus is reached regarding what appropriate minimum cyber security requirements are. Those minimum requirements are adhered to by relevant entities. Most, if not all, requirements are principle based, allowing for flexibility of implementation.

Background:

All relevant public and private organisations need to take necessary measures to protect their information infrastructure from threats, risks and vulnerabilities. One way to demonstrate a baseline level of cyber security is to achieve adequacy with internationally recognised security standards, frameworks or good practices. Standards include ISO/IEC 27001:2013, NIST SP 800-53 Rev4, ISA 62443-2-1:2009 and COBIT 5. For small and medium enterprises, depending on their risk profile, Cyber Essentials (CE) and Cyber Essential Plus (CE+) may be appropriate. This standards list is not exhaustive and is for guidance purposes only.

Defining a minimum set of security requirements is a complex exercise that must take into account the different levels of maturity, operational capacity and existing standards within each individual organisation.

Progress made:

Discussions between the CSTF and CNI operators regarding the adherence to minimum cyber security standards have been conducted and in some cases the CNI operators are already compliant or are aspiring to be compliant in most of their business areas.

Proposed next steps:

- Explore and set minimum security requirements

Government will work with CNI operators to achieve adequacy with an appropriate cyber security standard relevant to their individual risk profile. At this stage Government is not proposing to impose specific standards however it will regularly evaluate the progress made to judge whether the steps taken provide adequate protection for Jersey as a whole and, if not, reserves the right to take further action including introducing new legislation and regulatory standards.

For high-risk businesses, in particular those within the financial services and supporting sectors, the Government together with other relevant organisations (such as the JFSC, JB, DJL, JFL etc.) will provide support and guidance as set out in this strategy. Even if no cyber security standard will be imposed, the Government expects businesses to manage their cyber security risks properly. Here the JFSC, as an independent regulator, has already played an important role in raising awareness on cyber security by issuing the “Dear CEO” letter. The JFSC has stated its intent to focus on cyber security aspects for their registered members, in the coming period.

For small and medium enterprises:

a) The CSTF has decided that the Cyber Essentials[13] standard is a cost effective way to improve organisational cyber security levels. This standard is straightforward to implement and includes a free option as well, making it especially appropriate for small and medium enterprises.

b) Government will encourage adoption, especially where businesses do not have a more stringent standard. This will be done collaboratively with appropriate organisations such as Jersey Business or Jersey Finance to ensure that all actions are beneficial for Jersey's small and medium enterprises.

Adoption of Cyber Essentials will be voluntary. To encourage adoption, the Government will amend its procurement strategy to require minimum levels of cyber security for organisations to be eligible to bid for specific public contracts. Further include conducting awareness campaigns to ensure local businesses are aware of Cyber Essentials and understand its benefits.

[13] The Cyber Essentials standard identifies some fundamental technical security controls that an organisation needs to have in place to help defend against Internet-borne threats. Adherence to the standard is free of charge and certification costs are minimal, and include the advantage of granting cyber insurance upon certification.

3.8 Support law enforcement

Strategic objectives	What does good looks like?
1. Support law enforcement	Jersey law enforcement agencies have an appropriate legal framework, relevant partnerships and sufficient expertise to successfully investigate and prosecute the perpetrators of cyber crime.
2. Take stock of existing policies and regulations	All Jersey's laws and regulations touching on cyber security have been assessed for potential gaps and overlaps and are amended to ensure they are fit for purposes

Background:

The fight against cyber crime requires the collaboration of many organisations and different communities to be successful. It is important to address and counter the rise of cyber crime and to prepare a response, coordinated with all relevant stakeholders. Ensuring legislation is kept fit for purpose is key to this endeavour.

Progress made:

The States of Jersey Police "Cyber Policing Strategy" and the High Tech Crime Unit

The SoJP has developed its own Cyber Policing Strategy, focussed, as in the UK, on developing capability under four key headings of Pursue, Prevent, Protect and Prepare[14]. The SoJP has also established its High Tech Crime Unit (the "HTCU"). This unit is continuingly developing its investigative capabilities in the high tech domain (including smartphones, CCTV, computers, hardware and online presence).

SINCERE project
The project's goal is to create a centre of excellence for research and education with the aim of fighting cyber crime and promoting cyber crime investigation training, research and education. The project started in 2016, is expected to last for two years, is fully funded through the EU budget, and involves pan-Island partnership as explained in the executive summary of this document.

SoJP partnerships
The SoJP continues to develop meaningful partnerships (both on and off-Island) that will further support all aspects of cyber crime investigation. Successful collaborations include those with the South West Regional Cyber Crime Unit and Guernsey Police Force.

Proposed next steps:

- Support law enforcement

The SoJP will continue to establish relevant partnerships that will support the potential investigation of all aspects of cyber crime. The SoJP has and will continue to develop its cyber investigative capabilities so that it may successfully support the planned incident response capability with investigative skills.

- Take stock of existing policies and regulations

[14]The Police will PURSUE – as in prosecute and disrupt – criminals engaged in cyber crime; PREVENT people from engaging in cyber crime; PROTECT Islanders and businesses against cyber criminals and PREPARE to reduce the impact of cyber crime when it occurs. This approach is referred to as the "four Ps" of policing.

The Government has already conducted a review of legislation and will continue to take legal stock of the existing laws, regulations and applicable standards to ensure:

a) no legislative gap exists that will make it legally impossible to either enact cyber security policies or address cyber crime;
b) no regulation gaps exists that leaves organisations unaccountable for their cyber security (especially in the high-risk sectors).

The Government will extend the Council of Europe's "Convention on Cyber Crime" to Jersey in 2018.

4. Evaluate and adjust

In order to ensure the current Island-wide Cyber Security Strategy achieves its vision by 2020, it should be subject to updates every two years to maintain its ongoing adequacy. Amendments to the current strategy resulting from those future reviews will be treated with the same level of authority as the current strategy. In 2020, a full and thorough review of the current Island-wide Cyber Security Strategy should be scheduled.

A clear set of indicators have been developed to ensure that the Cyber Security Strategy delivers results in the intended way, progress is being measured and performance is being managed. Future reviews of the Cyber Security Strategy will show whether those Key Performance Indicators (KPIs) are being met.

The KPIs below will evolve as detailed action plans are introduced to achieve each of the strategic goals.

Strategic goals		Strategic objectives	Key performance indicators
1	Establish an information sharing, reporting and incident response capability	Establish an information sharing mechanism	■ awareness campaigns are informing businesses of the benefits of tapping into an information-sharing mechanism. The first campaign will take place by June 2018 ■ all local CNIs have tapped into an information-sharing mechanism by December 2018 ■ Government negotiate access to the UK CISP by December 2017
		Establish incident reporting mechanism	■ awareness campaigns are informing businesses of the benefits of incident reporting, the first campaign is launched by June 2018 ■ all local CNIs have committed to an incident reporting scheme by December 2018
		Establish incident response capability	By December 2018: ■ at least one workshop was performed involving appropriate members (such as CIISF, DJL, CNIs, etc.) to discuss what an incident response mechanism might look like ■ a feasibility study was performed or is under way regarding a future incident response mechanism ■ a date to have a decision on the future incident response mechanism is scheduled
2	Plan for the future cyber landscape	Develop Island-wide cyber attack scenarios	■ governmental bodies, led by ISD, and all CNIs will develop appropriate cyber attack scenarios and are adequately prepared for them by December 2019. All high risk business are actively encouraged to prepare in a similar way, on a continuous basis
		Organise Island-wide cyber security exercises	■ From 2019 the Government is organising or is a partner in (at least once per year) Island-wide cyber security exercises. Active effort is undertaken to involve CNIs and businesses in the exercises all non-classified information generated by the Island-wide cyber security exercises is shared with relevant Jersey based organisations
		Develop Island-wide contingency plans	By December 2018: ■ the Government has embedded plans for dealing with cyber incidents into its business continuity planning / disaster recovery planning ■ all CNIs have a clear strategy for dealing with cyber incidents all high-risk businesses have been encouraged to develop a strategy for dealing with cyber incidents

Strategic goals		Strategic objectives	Key performance indicators
3	Educate for the future	Strengthen training and educational programs	**1. Train Jersey's workforce in basic cyber security skills** Jersey's workforce should be educated at least in basic cyber security skills, tailored for each individual's, profession's or industry's risk. The specific ways in which this can be achieved and the related up-take targets per years should be agreed within a year from the strategy's approval. This approach is being pursued due to the size and importance of the task but also due to the negotiation process that needs to take place. **2. Relevant for academic education (primary, secondary education and tertiary education)** The Education Department and Digital Jersey to agree an engagement plan by September 2018 with the aim of connecting students and the digital industry and improving the learning experience for ICT related subjects. The Education Department, supported by the wider government, should explore the possibility of introducing cyber awareness courses weaved into the curricula, within two years of the strategy's approval. Government / partner agencies will to establish partnerships with universities recognised for their excellency in cyber security by December 2018. Government will explore the possibility of making education grants available for students seeking to pursue tertiary education in cyber security, within one year of the strategy's approval. **3. Relevant for professional education** Although the Government will engage with all types of education providers (including non-governmental ones) to ensure professional education is available for Islanders, no formal KPIs will be established, since there is a high dependency on actual market demand for cyber security skills and the decisions taken by private businesses.
4	Establish a framework to continuously assess Island-wide risks	Conduct national risk assessments	■ at least one Island-wide review is completed every three years ■ most, if not all, of the critical vulnerabilities identified in the Island-wide reviews are addressed (or reasonably mitigated) within one year ■ the majority of non-critical vulnerabilities identified in the Island-wide review are addressed (or reasonably mitigated) within two years
5	Create strong cyber governance	Encourage strong cyber security governance	■ the progress and effectiveness of the ISGB is monitored yearly and if gaps are identified suggestions for addressing them are made ■ all CNIs treat cyber security as a topic for the board room by June 2018

Strategic goals		Strategic objectives	Key performance indicators
		structures across the Island	■ in 2018, assess the number of high-risk businesses that treat cyber security as a topic for the board room within one year of the strategy's approval. If the number is deemed to be low, appropriate actions should be identified to increase awareness at the board level ■ by September 2018 the role of the JISO is filled
		Identify and engage stakeholders	■ all stakeholders are identified (CNIs, high-risk entities, governmental organisations, forums, Islanders, etc.) and documented through appropriate means such a stakeholder map by December 2017 ■ all identified stakeholders are engaged when relevant and communicated in an appropriate and timely manner
6	Foster partnership and collaboration	Engage in international cooperation and establish relevant partnerships	■ have the Council of Europe Convention on Cyber Crime extended to Jersey in 2018 ■ have a written commitment regarding collaboration with the States of Guernsey on cyber security by December 2017. Subject to the States of Guernsey's desire to collaborate ■ continuously explore ways of working with the UK, especially with the NCSC ■ continue inter-Island collaboration with the SINCERE project
7	Set minimum security requirements	Explore and set minimum security requirements	■ all CNIs have been engaged in a discussion about minimum cyber security standards applicable to their specific business, in 2018 ■ a voluntary minimum standard is defined and communicated to the wider business community by December 2017 ■ all CNIs adhere to, or are working towards, appropriate minimum cyber security standards by December 2018. The standard needs to be internationally recognised and potentially certifiable. Specific CNIs may choose not to have all of their business certified but only their most important informational assets ■ the business community is engaged and aware of the benefits of adopting a minimum cyber security standard by June 2019
8	Support law enforcement	Support law enforcement	No key performance indicator formally established here as addressing cyber crime is closely linked to the SoJP. We will formally ask the SoJP to propose and track specific key performance indicators referring to this objective.
		Take stock of existing policies and regulations	In 2018: ■ a legal stocktake of the existing policies, regulations and standards touching on cyber security has been conducted ■ all identified gaps and overlaps have a proposed solution and an agreed timeline for implementation

Correlation between strategic objectives and pillars

1. Establish an information sharing, reporting and incident response capability

Strategic objectives	Pillar 1 Government	Pillar 2 CNI	Pillar 3 Business	Pillar 4 Legislation	Pillar 5 Citizens
1. Establish trusted information-sharing mechanisms	✔	✔	✔	✔	✔
2. Establish incident reporting mechanisms	✔	✔	✔	✔	✔
3. Establish incident response capability	✔	✔	✔	✔	✔

2. Plan for the future cyber landscape

Strategic objectives	Pillar 1 Government	Pillar 2 CNI	Pillar 3 Business	Pillar 4 Legislation	Pillar 5 Citizens
1. Develop Island-wide cyber attack scenarios	✔	✔	✔	✔	✔
2. Organise Island-wide cyber security exercises	✔	✔	✔	✔	
3. Develop Island-wide contingency plans	✔	✔	✔	✔	

3. Educate for the future

Strategic objectives	Pillar 1 Government	Pillar 2 CNI	Pillar 3 Business	Pillar 4 Legislation	Pillar 5 Citizens
1. Strengthen training and educational programs	✔		✔		✔

4. Establish a framework to continuously assess Island-wide risks

Strategic objectives	Pillar 1 Government	Pillar 2 CNI	Pillar 3 Business	Pillar 4 Legislation	Pillar 5 Citizens
1. Conduct national risk assessments	✔	✔	✔		✔

5. Create strong cyber governance across the Island

Strategic objectives	Pillar 1 Government	Pillar 2 CNI	Pillar 3 Business	Pillar 4 Legislation	Pillar 5 Citizens
1. Encourage strong cyber security governance structures across the Island	✔	✔	✔	✔	
2. Identify and engage stakeholders	✔	✔	✔	✔	✔

6. Foster partnership and collaboration

Strategic objectives	Pillar 1 Government	Pillar 2 CNI	Pillar 3 Business	Pillar 4 Legislation	Pillar 5 Citizens
1. Continued international cooperation and establish relevant partnerships	✔	✔		✔	

7. Set minimum security requirements

Strategic objectives	Pillar 1 Government	Pillar 2 CNI	Pillar 3 Business	Pillar 4 Legislation	Pillar 5 Citizens
1. Explore and set minimum security requirements	✔	✔	✔	✔	

8. Support law enforcement

Strategic objectives	Pillar 1 Government	Pillar 2 CNI	Pillar 3 Business	Pillar 4 Legislation	Pillar 5 Citizens
1. Support law enforcement	✔			✔	
2. Take stock of existing policies and regulations				✔	

5. Appendix 1 - Glossary

Acronyms:

C&AG: Comptroller and Auditor General
CCTV: Closed circuit television (known also as video surveillance)
CE: Cyber Essentials
CERT: Computer emergency response team
CIISF: Channel Islands Information Security Forum
CISO: Chief Information Security Officer
CISP: Cyber security information sharing partnership
CSIRT: Computer security incident response team
CSTF: Cyber security task force (Jersey Government's task forces dealing with cyber security topics)
CNI: Critical national infrastructure
DJL: Digital Jersey Limited
EU GDPR: European Union General Data Protection Regulation
GSO: Get Safe Online (UK non-profit organisation)
HTCU: High Tech Crime Unit
ICT: Information and communications technology
IM: Information management
IoM: Isle of Man
IoT: Internet of things
ISD: Information services department
ISGB: Information security governance board
ISO: International organization for standardisation
IT: Information technology
IT&C: Information technology and communications
JB: Jersey Business
JFSC: Jersey Financial Services Commission
JISO: Jersey Information Security Officer
Key informational asset: represents the main informational asset that a cyber attacker might target
KPI: Key Performance Indicator
NCSC: National Cyber Security Centre (UK entity)
PMNW: Prison Me No Way
R&D: Research and development
SOC: Security operations centre
SoJP: States of Jersey Police
UK: United Kingdom

The Government: referring to the States' of Jersey / the Government of Jersey. **Please note that when there is a reference to "we" in this document the reference implies the Government, unless otherwise stated.**

6. Appendix 2 - Acknowledgements

"Thank you"

The CSTF team held discussions starting in January 2016 with a number of governmental agencies, critical national infrastructure operators, businesses and other stakeholders. **We would like to thank all of those that met with us and contributed with their expertise, ideas and thoughts for the strategy.**

Critical National Infrastructure operators:

- Electricity
- Gas
- Telecoms
- Transport (including Ports and Airport)

Governmental departments, agencies, bodies and committees:

- Chief Minister's Department
- Corporate Procurement
- Cyber Security Task Force
- Education Department
- eGovernment
- Hi-Tech Crime Unit
- Information Services Department
- States of Jersey Police
- Treasury and Resources Department

Industry representatives and the financial services regulator:

- Channel Islands Information Security Forum
- Digital Jersey Limited
- Jersey Financial Services Commission
- Jersey Finance Limited
- Jersey Business
- Office of the Information Commissioner

Industry representatives and the financial services regulator:

- Channel Islands Information Security Forum
- Digital Jersey Limited

International organisations

- UK National Cyber Security Centre
- Members of the SINCERE Project