Deputy Chief Minister |
Minister for Economic Development,
Tourism, Sport and Culture

Government of JERSEY

19-21 Broad Street | St Helier
Jersey | JE2 4WE

By email

1st March

Dear Chair,

Thank you for your letter dated 10th February in which you provide a number of questions following your briefing with officers on the role of the Cyber Emergency Response Team and the proposed Cyber Defence legislation. I have set out below answers to each of these in turn:

Can you confirm the various platforms used in which CERT.JE receives data?

CERT.JE receives threat intelligence data from third party providers and other CERTs, both directly and via common threat intelligence sharing platforms such as MiSP (also used by UK NCSC). Additionally, CERT.JE receives information on incidents and vulnerabilities directly from local residents and organisations, as well as referrals from other bodies such as States of Jersey Police. These reports are usually via email or phone, but can also be via walk-in or social media.

How secure are these platforms and what assurance do you have that they are reliable?

CERT.JE needs to meet a higher standard of cyber security than would apply to most other networks, given the nature of the systems operated and the data processed. The platforms used are often specialist cyber security applications commonly used by other national security and law enforcement agencies, and are capable of operating to a high standard of security and resilience.

CERT.JE is also part of UK NCSC's Active Cyber Defence service. Additionally, CERT.JE will undertake Cyber Essentials Plus (CE+) certification. The CE+ standard is a recognised minimum baseline suitable for all smaller organisations, and is recommended by the UK Government and the Government of Jersey.

What engagement, if any, has been undertaken with other sectors (finance, retail, tourism etc)?

The Department for the Economy released a consultation document[1] on the proposal for a draft Cyber Defence Law in Jersey in December 2022. Key stakeholders covering a range of sectors were then invited to public briefings held during January 2023. In total 14 public consultation sessions were held with participants which included representatives from Institute of Directors, Chamber of Commerce, Critical National Infrastructure, Operators of Essential Services (including hospitality and retail), cyber security professionals and cyber security service providers and relevant voluntary organisations including the Channel Islands Information Security Forum.

The set-up of CERT.JE has been strongly supported and welcomed across all sectors including businesses, the finance sector, and Critical National Infrastructure providers. The Cyber Security

[1] Government of Jersey, Consultation on proposed Cyber Defence legislation, available at Consultation on proposed cyber defence legislation (gov.je)

Task Force (a managerial level working group with representatives across Modernisation & Digital, Skills Jersey, States of Jersey Police, Jersey Office of the Information Commissioner, Jersey Financial Services Commission, Jersey Finance, and Digital Jersey) has also been engaged throughout the development of CERT.JE, led by the Digital Economy Team in the Department for the Economy.

Is CERT.JE limited to Emergency Response? On its website, CERT.JE is advertised as "The Cyber Security Centre for Jersey" but their title suggests they are an 'Computer Emergency Response Team'. Can you confirm which is correct?

Since June 2021, the Cyber Emergency Response Team for Jersey (CERT.JE) has operated within the Department for the Economy. Whilst 'CERT' is a well recognised global term, countries have increasingly recognised that effective cyber security requires proactive engagement and education as well as responsive services. The remit of CERT.JE is therefore broader than just providing a response in a cyber emergency, and following consultation with stakeholders it has been agreed that the most appropriate name is the Jersey Cyber Security Centre. It is intended to adopt this name in line with the legislative process for the proposed Cyber Defence (Jersey) Law.

What is CERT.JE doing with the information it seeks to collect?

Information is received from various intelligence sources and analysed by cyber security specialists to identify issues of concern to Jersey. This information is then used to help protect individuals and organisations, as well as to inform island wide response to cyber risks. Trust is essential to encourage open information sharing, and CERT.JE does not share confidential information on organisations or individuals with Government, law enforcement or regulators, except with the permission of the organisation concerned or where required by law.

What is CERT.JE's interaction with JT and other broadband providers?

JT and other broadband providers are deemed to be part of Critical National Infrastructure (CNI). CERT.JE has constant and regular engagement with them. Broadband providers also participate in groups operated by CERT.JE including the C-TAC (Cyber Technical Advice Cell), Cyber Security Suppliers Forum, and other key groups.

Can you provide the Panel with a concise, Kings English Problem Statement of less than 200 words of the problem CERT is intended to solve?

Jersey's Island Wide Risk Assessment confirms that cyber security is one of the most critical threats to the island. In addition to increasing risks from cyber crime, other cyber security threats include advanced nation state capabilities from unfriendly regimes such as North Korea and Russia. Many nation state level cyber attacks have a global impact, and following Russia's invasion of Ukraine countries including the UK and the USA have warned of a heightened risk of cyber attacks. Jersey's inclusion on Russia's list of unfriendly jurisdictions has further raised the risk to the island. In the most severe instances, such as attacks on critical services or healthcare, cyber attacks can present a threat to life.

Locally, recent attacks have included schools, law firms, charities and financial services companies. Several of these attacks have been carried out by nation state aligned cyber crime groups such as Lockbit, who were also responsible for the ransomware attack on Royal Mail in January 2021.

Jersey's reputation as a responsible, well-regulated jurisdiction is a critical part of its financial services and digital propositions, and the Island must take steps to actively reduce cyber security risks and ensure that when a cyber incident occurs, the response is timely and effective in order to minimise the damage caused.

If such a problem statement exists, has this been reviewed by others who know this subject and how can you be certain that the problem statement makes the most sense in the circumstance?

The mission of CERT.JE is to "prepare, protect, and defend the Island against cyber threats".

CERT.JE's vision statement is "for Jersey to be internationally recognised as a safe place to live and do business online".

The vision and mission of CERT.JE have been reviewed with Government, Ministers, and external stakeholders including UK NCSC and extensively socialised with industry, the cyber security profession, and other local stakeholders.

The functions of CERT.JE that deliver against these are aligned to the globally recognised FIRST framework and documented in an 'RFC2350' – the recognised global standard for communicating the remit and functions of CERTs. CERT.JE intends to undertake an accreditation process with industry bodies FIRST and TF-CSIRT which will validate CERT.JE's readiness to deliver against this mandate.

Can you give an overview of what exactly CERT.JE is protecting and the size of the problem?

CERT.JE has a defined constituency to protect, documented in their RFC2350. This is the jurisdiction of Jersey, including:

a. all organisations established within the jurisdiction, including the States of Jersey, public sector organisations, private companies, charities and third sector organisations,
b. critical national infrastructure providers operating services in Jersey (regardless of domicile),
c. individuals resident in Jersey
d. the .JE top level domain name (gTLD), and
e. services using telephone and IP ranges allocated to Jersey telecoms providers or for use in Jersey.

Effectively, this reflects where cyber incidents would lead to reputational, political, economic or wellbeing risks to the Island or Islanders. It is anticipated that the planned Cyber Defence legislation will provide the necessary remit and authority to deliver to this scope.

According to the World Economic Forum, with an expected global cost of USD $8trillon in 2023, the cyber crime economy would be the third largest country in the world after the USA and China. The UK Government reported that 39% of organisations fell victim to a cyber attack in 2021.

What is CERT.JE's 'Definition of Winning" and how is success of CERT.JE measured?

CERT.JE will be successful if it delivers the agreed functions and achieves its vision for Jersey to be internationally recognised as a safe place to live and do business online. Success is measured through metrics agreed with the Government of Jersey, and delivery of the business plan. Following transition out of the Department for the Economy, CERT.JE will be measured by performance against the Partnership Agreement. Progress will be routinely monitored through partnership meetings with the sponsoring Department.

What has CERT.je done since June 2021 and how have they measured it (including emergencies resolved and help with special email systems and improvements for Jersey Businesses)?

Over the last 18 months CERT.JE has worked to define the strategy and approach alongside the Digital Economy Team; to undertake island wide incident readiness workshops, to develop relationships locally and internationally, to undertake organisational development including hiring, governance and IT, to deliver an event every 48 hours during Cyber Security Awareness Month in October 2022, acted as a trusted advisor to Government and industry on cyber security matters, and supported local organisations and residents to respond to and recover from cyber attacks. CERT.JE has also partnered with UK NCSC to deploy NCSC's Active Cyber Defence services in Jersey, and led the local cyber response to Russia's war against Ukraine.

Can you provide examples of proactive action that has been taken by CERT.je to prevent a serious breach or attack in Jersey? Could private sector services have been used instead?

For confidentiality reasons CERT.JE cannot identify the specific organisations supported.

One example would be a co-ordinated attack on a Jersey professional services sector. Following two reports by local firms of similar attacks, CERT.JE was able to proactively notify all similar firms of the attack resulting in several additional instances being identified and one attack being stopped in progress. CERT.JE was able to review the pattern behind the each of the attacks and provide appropriate advice where needed. None of the attacks were successful.

A second example is a recent attack on a local public service provider. CERT.JE had a technical team on site within 2 hours and was able to work with the organisation to prevent data leakage and minimise the impact on the network, allowing the organisation to substantially recover in a timely manner. CERT.JE also worked with UK NCSC to pass intelligence about the attack and a related vulnerability to a commercial service provider in the United States, allowing them to take action to reduce the risk posed by their service for other organisations.

It would not be possible to deliver this type of activity though the private sector. However, the private sector does have an important role to play and CERT.JE works closely with cyber security providers in this regard, for example by coordinating local delivery of Cyber Essentials Certifying Body Training to allow local businesses to deliver Cyber Essentials assessments.

To what extent might CERT.JE be regarded as competing with local business providers or overlapping with States of Jersey police activities in educating local organisations on cybersecurity?

As outlined above, CERT.JE works closely with private sector service providers. This is highly collaborative and has been well received. CERT.JE will not use taxpayer funds to deliver services that would otherwise be delivered by the private sector, but will play a role alongside Digital Jersey in supporting the development of local private sector capabilities.

The roles of CERT.JE and law enforcement are complementary. CERT.JE is not a law enforcement body. CERT.JE works closely with States of Jersey Police, handling a number of cyber security incidents referred by the Police, and providing support and advice on cyber security matters, for example providing open source intelligence to support investigations. CERT.JE also collaborates with the Police through the Jersey Frand Prevention Forum.

Does CERT.je have SMART objectives? If so, can you list them?

Current objectives and performance measures are outlined below.

Benefit	Performance Measure (Monitoring)	Proposed Metric	2021 baseline	2022 outturn	2023 target
Raises citizens' and businesses' cyber security	Strategy sets out the steps to strengthen the cyber security of the Government, citizens, businesses and critical national infrastructure. Resourcing of engagement and communication workstream, cyber advisory workstream. Capability to support high risk areas - Gov, CNI and ALBs/ALOs, financial services, telecoms, SMEs.	Total number of individuals and organisations directly engaged though cyber security awareness activity, advice and support. *(primary metric)*	0	1,589	1,500
Government Technical Advisor	Provides the Government with a technical advisor in the management of major island-wide incidents that can recommend appropriate triage. Ability to effectively engage with and support ALB/ALO community where it is not cost justified to duplicate cyber expertise. Provision of tooling and investigate shared cyber services.	Number of public service providers directly engaged or supported	N/A	15	20
CERT Network	Ensures the Government and local community is connected to the latest developments across the EU and international CERT network	Number of established relationships or MOUs with other national CERTs	1	3	10
	Accredit to FIRST and TF-CSIRT, and establish MOUs – requires service maturity including legal and governance, data controllership and ability to contract as legal body.	Maturity against SIM3 model (at year end) for functions provided Application and accreditation status at year end to FIRST and TF-CSIRT	0.0 N/A	0.8 N/A	2.0 Applied
Supports Organisations	Supports organisations to manage incidents and accelerates the process of recovery.	Number organisations supported to manage or recover from cyber incidents	N/A	21	No target*

Has CERT.je ensured that all customer data on databases of all Jersey businesses are strongly encrypted?

Whilst organisations are responsible for their own internal control environment and therefore CERT.JE cannot mandate that specific controls are implemented, CERT.JE provides guidance on controls including encryption. CERT.JE recommends that all non-public data is strongly encrypted both when stored ('data at rest') and when transmitted ('data in in transit'). This issue is becoming increasingly topical with the emergence of quantum computing as this may render current encryption methods invalid.

What action is CERT.JE taking to drive and measure change including promotion of the "Zero Trust" concept?

Efforts to drive change include delivery of October Cyber Security Awareness Month as well as direct and social media outreach, newspaper, radio and television coverage of cyber security issues and the actions that can be taken to address them. Measuring change in cyber security is difficult as the threat continues to increase alongside improvements in our defences. In addition to CERT.JE's metrics and deliverables, the Government of Jersey undertakes a periodic cyber resilient risk assessments to support development and measurement of progress against the 2017 Cyber Security Strategy.

CERT.JE has chosen not to actively promote concepts such as "zero trust" as given the prevalence of small and medium sized organisations in Jersey, practical hands-on guidance on basic security measures has been found to be more helpful. However, CERT.JE does endorse zero trust as a goal and provides advice on this where appropriate.

What "email specific security" measures are provided by CERT.JE?

CERT.JE provides advice on email security, but generally does not operate technical security controls on behalf of individual organisations as that would be undertaken by the private sector. However, CERT.JE has worked closely with UK NCSC to make available and promote NSCS's Active Cyber Defence services across the Channel Islands. Organisations can use these free services to check the configuration of their mail servers and to monitor their network, including mail servers, for known vulnerabilities. Additional tools are available for specified public bodies including local schools and charities.

What training plans have CERT.JE put in place to ensure that security systems are operated by fully trained staff in organisations?

Individual organisations are responsible for their own control environment including implementing appropriate security measures and undertaking appropriate training. CERT.JE provides advice and assistance to support them to do so. In the last 12 months, this has included advisory posts on social media, articles in local print and digital media, and a series of events in Cyber Security Awareness Month.

CERT.JE is working closely with Digital Jersey to develop a cyber security training programme for Jersey residents, and works with the voluntary sector to deliver technical training sessions for local cyber security professionals.

Internally, CERT.JE team members will be trained to a common standard in incident response recognised by CERTs across the EU, with the first two team members due to undertake training in

April 2023. CERT.JE is also working collaboratively with the Government of Jersey's apprenticeship programme, with a cyber apprentice joining CERT.JE in September 2022.

How many people have CERT.JE trained to be secure?

In 2021 direct engagement activity reached 1,589 individuals and organisations, including:

- 581 though attending physical and online events
- 851 through social media engagement
- 136 through online newsletters
- 21 through incident response and direct support

Additionally, CERT.JE attended and presented at a range of external events run by organisations including the IoD, Jersey Business, Jersey Finance, Jersey Funds Association, the Office of the Information Commissioner, Digital Jersey, the Government of Jersey, and others. These are not included in the above statistics.

Security awareness is a cultural as well as educational challenge and it will require ongoing engagement to drive continuous improvement over time, as well as strong support from Government and industry.

Could you please provide us with any training materials used by CERT?

Training materials are constantly updated and tailored to individual industries and events run, however we are happy to provide links to CERT.JE's website and social media where further advice and materials are available.

Can you confirm if use of all USB data drives are disabled in Jersey companies and if and how CERT.JE are ensuring all Jersey organisations adopt this basic security measure is adopted including users of government systems?

Individual organisations are responsible for their own control environment including implementing appropriate security measures, and do not have any visibility into private networks or any statistics on the use of USB drives locally. Whilst there are legitimate uses for USB drives, CERT.JE recommends that USB drives should be disabled where possible.

Can you describe CERT.JE's zero-day prevention techniques?

A 'zero day' is an unknown vulnerability and therefore it is not possible to prevent these. It it possible to reduce the risk associated with zero day vulnerabilities by operating a consistently strong control environment and CERT.JE provides advice and support in this regard.

How much does CERT.JE cost to run?

The budget for the 2023 financial year is £850,000. Of this £500,000 is funded through base budget, £200,000 through the Government Plan, and £150,000 through efficiencies in the Department for the Economy. This covers the full costs of delivering CERT.JE including threat intelligence, resourcing, training, security vetting, the CERT.JE Operations Centre, technology and network equipment, software and support, delivery of education and awareness activity, and international engagement with other cyber defence organisations.

How much value does it generate and/or has contributed to the Island? To what extent might it charge users for its services in the future?

CERT.JE engages and communicate with industry, public bodies and the third sector to develop clear standards, expectations and support for cyber security risk management, control, and assurance, whilst having the ability to monitor threats and respond to major incidents. This will provide the island with a balanced approach that enables the cyber risk profile of the island to be reduced over time, whilst providing a proactive service to reduce the significant cyber security risks the island faces. It is not possible to prevent all security incidents, as the cyber threats to the Island change and develop over time. However maintaining effective cyber defences will allow the island to manage these risks and reduce the frequency and impact of incidents, and thereby protect the wellbeing of residents, the success of the economy, and the reputation of the island.

The ability to for CERT.JE to raise fees and charges should be within the context of providing value added services in support of the main functions and objectives of the CERT.JE and not for commercial gain. For example, this could include facilitating shared delivery or collaborative procurement which supports Government's strategy and maximise return on investment; operating certification schemes, providing training, raising sponsorship to support the delivery of conferences and events.

CERT.JE will not raise fees and charges for services and functions that would challenge the independence of the CERT.JE or see the facility becoming a competitor to private industry.

Fees and charges should be proportionate to the value added services being provided. Any surplus generated by the CERT.JE via fees and charges should be clearly declared within financial reports for that financial year and where the annual surplus is 10% or more of the annual grant received within that accounting period, this should be returned to the Government and used to support developing cyber security policy for the Island.

CERT.JE will not charge or require for organisations to pay a registration fee. CERT.JE will consult Government and follow the necessary public consultation process should such charges become appropriate at a future date.

How is return on taxpayer investment and performance measured by the Department?

Once CERT.JE has transitioned out of the Department for the Economy, financial governance through the grant funding mechanism will ensure proper accountability for public financial resources and continual assessment against the four essential standards of regularity, propriety, value for money and feasibility as per the Public Finance Manual.

Please provide a copy of any Memorandum of Understanding between the Department and CERT.JE.

There is no MoU between CERT.JE and the Department for the Economy. However, it is recognised that an MOU is required to govern the relationship of CERT.JE with Government departments including the Department for the Economy, and Modernisation and Digital. These will be established during 2023 alongside the preparation for transition out of the Department for the Economy.

What risk/cost analysis has been done for the implementation of CERT.JE?

The Council of Ministers approved the creation and funding of the Cyber Emergency Response Team as part of the Government Plan in late 2019, as a key recommendation of Jersey's Cyber Security Strategy[1]. This recommendation was based on a feasibility study conducted by expert

consultants (originally with Guernsey) which incorporated significant stakeholder engagement to evaluate and identify the core functions that would be required by an operational Emergency Response Team.

[1] Government of Jersey, Cyber Security Strategy, 2017, available at: https://www.gov.je/Government/Pages/StatesReports.aspx?reportid=3208

What is the current capability of the sector CERT.JE is protecting and are mature defences in place?

CERT.JE has an island-wide mandate rather than being sector specific. The last island wide cyber resilience assessment completed in 2020 indicated the level of cyber resilience is maturing, with a strong correlation between both organisational size and business turnover with cyber security maturity. Individual businesses are responsible for their own cyber security stance, with the role of CERT.JE to provide guidance and support to all.

In the event of a cyber event, what can CERT.JE do to add to the solution/mitigation and how much will CERT.JE be able to reduce impact?

CERT.JE can provide incident support and resolution in an advisory capacity. CERT.JE also offers advice to prevent incidents. In some cases CERT.JE may provide direct incident support with the agreement of the organisation concerned and where it is in the interest of the Island to do so, for example CERT.JE has recently helped a local organisation mitigate the impact of a significant ransomware attack against its systems. CERT.JE may also work with UK NCSC to provide this support for the most severe incidents.

Recent questions around Jersey's resilience and crisis management have suggested that the Island has the capability to withstand crisis events. Can you confirm where CERT.JE fits into this resistance?

CERT.JE supports the Islands emergency planning processes. The Director is part of the Jersey Resilience Forum Executive chaired by the Government Chief Executive, and works closely with emergency planning officers. In the event of a major incident with cyber element, the Director chairs the Cyber Technical Advice Cell (C-TAC) such as that stood up by the Strategic Coordination Group (SCG) in response to Russia's war in Ukraine, in much the same way that the Chief Medical Officer chaired the STAC during COVID response.

Can you confirm how many attacks against Jersey are experienced in any given period (say one week) and how CERT.JE assists in reducing these?

The number of attacks varies constantly so there could be a period of few attacks followed by a period of increased attacks. Additionally, CERT.JE is only aware of attacks detected by CERT or voluntarily reported to it, which is a subset of attacks taking place. For example, in one 24 hour period in Jersey, CERT.JE identified 69 servers sending insecure data, 5 computers infected with a known malicious software variant, and 18 computers participating in botnets controlled by the Conti cyber crime gang. Currently data collection processes are manual whilst CERT.JE is connected to the Government of Jersey's IT network. During 2023 CERT.JE will be deploying an incident management platform that will allow more structured data to be produced including the number of attacks and vulnerabilities that are assessed, the number of issues notified to organisations and residents, and the number of incidents handled.

Can you confirm if it is possible for the larger number of incidents to be taken out by the filtering of web addresses and if so, how does that affect the answers above?

Unfortunately not. Incidents come from a variety of attack vectors and types. Web filtering is a control that may prevent a very small subset of these attacks. As an example, web filtering would not prevent a email phishing attack.

What industry consultation is being undertaken regarding the proposed law relating to CERT.JE, what are anticipated to be its statutory powers, what industry consultation is being undertaken regarding the content of the law and will responses to the public consultation be made public prior to the law being finalised?

Major industry sectors were consulted as part of the development of Jersey's Cyber Security Strategy in 2017, and reengaged by CERT.JE through a series of workshops and incident response exercises since 2021. The Department for the Economy released a consultation on the proposal for a draft Cyber Defence Law in Jersey, with face to face briefing sessions offered to all during January 2023. The consultation was directed at several sectors, key stakeholders including Jersey Regulators, Institute of Directors, Chamber of Commerce and Critical National Infrastructure organisations and voluntary groups such as Channel Islands Information Security Forum plus engaging those organisations deemed to be Operators of Essential Services (including finances services sector, hospitality and retail sectors and public authorities including the Parishes). During the consultation period a series of briefings were held both for specific sectors and groups, and for the general public. Views raised during the consultation have been reflected in the law drafting instructions and a Consultation Report is currently in development, and will be made publicly available by end of March.

It is expected that law drafting will commence early March 2023, with a further public consultation on the final draft legislation planned, expected May 2023, where views of all key stakeholders, interested parties and the public will be sought. As a follow-up from the private Scrutiny Pannel briefing held in January, Officers would also like to offer the Scrutiny Pannel the opportunity for a follow-up private briefing at this time, to review in depth the proposed draft legislation and to respond to any questions raised. Commencement of the legislation is planned for early 2024.

I hope the above provides clarity to the areas you have raised.

Yours sincerely,

Deputy Kirsten Morel
Minister for Economic Development, Tourism, Sport and Culture
E k.morel2@gov.je