JERSEY AUDIT OFFICE

Critical Infrastructure Resilience – Cyber Security

17 April 2026

The purpose of the Comptroller and Auditor General (C&AG), fulfilled through the Jersey Audit Office (JAO), is to provide independent assurance to the people of Jersey on the extent to which public money is spent economically, efficiently and effectively and on whether the controls and governance arrangements in place within public bodies demonstrate value for money. The C&AG's remit includes the audit of financial statements and wider consideration of public funds, including internal financial control, value for money and corporate governance.

This report can be found on the Jersey Audit Office website at https://www.jerseyauditoffice.je/

If you need a version of this report in an alternative format for accessibility reasons, or any of the exhibits in a different format, please contact enquiries@jerseyauditoffice.je with details of your request.

Report by the Comptroller and Auditor General: 17 April 2026

This report has been prepared in accordance with Article 20 of the Comptroller and Auditor General (Jersey) Law 2014.

Contents

Summary

Introduction

1. National Infrastructure are those facilities, systems, sites, information, people, networks and processes necessary for a jurisdiction to function and upon which daily life depends.

2. Not everything within a national infrastructure sector is judged to be 'critical'. Jersey's critical infrastructure can be described as those physical facilities, supply chains, information technologies and communication networks which, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact the social or economic wellbeing of Jersey or affect Jersey's ability to ensure national security.

3. There are broadly twelve sectors that could be considered to be critical infrastructure for Jersey as shown in Exhibit 1.

Exhibit 1: Jersey's critical infrastructure sectors

• Chemicals	• Energy	• Space
• Communications	• Finance	• Transport
• Defence	• Food	• Waste
• Emergency Services	• Health	• Water

4. Critical infrastructure systems within these sectors are particularly vulnerable to being damaged or disrupted.

5. Ensuring the security and resilience of Jersey's critical infrastructure is a responsibility shared by the States, infrastructure owners and operators. Each have different responsibilities for critical infrastructure depending on the system and/or the nature of the threats to be mitigated. Responses to a threat can involve the asset owner and operator, the technical and operational

lead for Government and emergency services or law enforcement. Co-ordination among entities is therefore required to prepare, rehearse and respond to critical infrastructure threats.

6. Cyber resilience is the overall ability of systems and organisations to withstand cyber events and, where harm is caused, recover from them. Critical infrastructure systems are prime targets for cyber-attacks due to their vital role in society. Potential cyber security threats do not just affect data and systems in government and business, but also critical infrastructure, including energy, health, transport, water and emergency services.

7. In October 2017, the Government published its Cyber Security Strategy. The Strategy is centred around the following five pillars:

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

8. To protect the Island, there is a need for Government to work with the private sector and the operators of critical national infrastructure. In addition, there is a need for Government to have robust cyber security arrangements over its own operations.

9. The Jersey Cyber Security Centre (JCSC) was established in 2021 to promote and improve the Island's cyber resilience. JCSC is part of the Department for the Economy but operates on an arm's length basis from Government.

10. The Government of Jersey has invested and is investing in a cyber security programme focussed on improved protection of Government of Jersey IT

systems and related infrastructure to improve its own arrangements. Exhibit 2 summarises the actual and committed expenditure on the cyber security programme within Government.

Exhibit 2: Expenditure on Government's cyber security programme

	Actual expenditure 2020 to 2024 £000	Budgeted expenditure 2025 to 2028 £000	Total actual and committed expenditure £000
Cyber Security Programme	19,055	10,171	29,226

Source: States of Jersey Group Annual Report and Accounts 2020-2024 and Budget 2025-2028

11. In May 2022 I published a report on *Cyber Security Arrangements* which focussed on the Government's cyber security programme at that time.

12. In January 2026 the States Assembly passed a new Cyber Security Law (the Cyber Law). Its objectives are to:

- establish a recognised technical cyber security advisory capability for the Island
- increase the cyber security of network and information systems and operational technology on which the Island's Operators of Essential Services (OESs) rely; and
- develop a trusted culture of cyber threat information sharing to mitigate cyber risks and raise cyber resilience.

13. Articles 11 and 20 of the Comptroller and Auditor General (Jersey) Law 2014 make provision for me to prepare reports arising from my work and forward them to the Greffier of the States to be laid before the States Assembly. Paragraph 65 of the Code of Audit Practice (December 2023) provides that in determining the content and timing of public reporting I should have regard to potential prejudice to the interests of the States of Jersey or other parties arising from public reporting.

14. Having regard to this provision and the subject matter of this report, I have elected to issue a shorter report than usual, excluding my detailed findings

and excluding the 23 recommendations arising from my work. I am, however, providing relevant officers with a supplementary report that sets out more details of my findings to assist them in responding to the recommendations that I have included in my supplementary report.

Key findings

15. The Cyber Law sets out clearer expectations for governance, incident reporting, and resilience planning. It also requires stronger co-ordination between government, regulators, and industry.

16. The UK National Cyber Security Centre (NCSC) has designed a Cyber Assessment Framework (CAF) for organisations who deliver essential functions. The CAF has been used as a basis for the regulatory regime in Jersey.

17. In April 2025, JCSC was reviewed virtually by the NCSC to conduct an initial evaluation of its process maturity levels. The NCSC produced a summary report which was largely positive towards JCSC in relation to its process maturity and comparison to other small-nation cyber incident response teams.

18. The Cyber Law will place greater demand on the JCSC given the complexity of the new regulatory regime and the obligations placed on OESs. No additional funding has been provided to the JCSC for implementation of the Cyber Law. The expectation is that current activities can be prioritised to deliver the new requirements and responsibilities.

19. I have considered arrangements for cyber security at four OESs. I found varying levels of cyber security maturity at these entities. The obligations on these entities has increased under the Cyber Law and all entities reviewed have work to do to ensure compliance with the new obligations placed on them.

20. Late in 2019, the Government commenced a Government-wide Cyber Security Programme (CSP 1.0), with the bulk of the work planned to be delivered in two, 12-month tranches. Tranche one was originally scheduled for completion

by March 2021. However, the COVID-19 pandemic and associated public health measures and restrictions inevitably led to some programme delays at that time. CSP 1.0 essentially ran from 2020 to 2023.

21. The stated aim of CSP 2.0 was to lift the Government to a maturity score of 3.0 across all National Institute of Standards and Technology (NIST) core functions.

22. Since CSP 2.0 was established the focus of the team has shifted to address critical operational weaknesses, rather than substantive implementation of defined deliverables. The shift has been as a result of growing global cyber security threats, including threats to Jersey.

23. The reactive operational posture necessitated by an evolving external threat landscape, has resulted in resource allocation patterns that prioritise immediate threat response over strategic programme execution.

24. Underpinning these operational and cultural factors is a foundation of technical debt that constrains progress across multiple CSP 2.0 workstreams. The continued dependency on legacy infrastructure slows implementation of CSP 2.0 and increases the complexity of planned initiatives. This has been recognised and the IT Infrastructure Improvement Programme is running in parallel to CSP 2.0 with close coordination between the two programmes.

25. The onboarding challenges experienced with external contractors, the change in Programme Manager in 2025 and the capacity limitations observed within internal teams (due to the focus on urgent operational cyber issues) have delayed some aspects of the overall CSP 2.0 programme delivery.

Conclusion

26. Jersey's cyber security is being strengthened through the implementation of the new Cyber Security Law and the supporting Framework. It is essential for the States and for Operators of Essential Services to ensure that their

arrangements meet the requirements and expectations placed on them under the new Law.

27. While Government has taken action to improve its own cyber security resilience there remains considerable work to be undertaken to ensure that the arrangements in place meet minimum expected maturity standards.

Objectives and scope of the audit

28. The audit's overall objective was to assess whether the Government has an effective approach to cyber resilience.

29. The scope of the audit included:

- the Government's cyber security programme
- emergency services and how they are integrated into cyber security governance arrangements
- how operators within the energy sector are integrated into cyber security governance arrangements
- how telecommunications operators are integrated into cyber security governance arrangements; and
- the arrangements in respect of the JCSC.

30. The audit has not considered arrangements in respect of private sector businesses on the Island.

31. More information on the audit approach can be found in Appendix One.

Appendix One

Audit Approach

This audit used a combination of a problem-oriented and system-oriented approach.

To assess if the Government's efforts to improve cyber security are providing value for money, the audit considered whether:

- clear, risk-based cyber resilience outcomes have been set for the programmes and arrangements put in place within the States
- the right support, incentives and monitoring procedures have been established to provide assurance over cyber security arrangements relating to critical infrastructure operated by the States of Jersey Group and by asset owners in the telecommunications and energy sectors; and
- actions taken by the States and the JCSC have appropriately prioritised, and built the capability to deliver, the cyber security they need to operate effectively.

The audit criteria included the following aspects of cyber security governance arrangements:

- Network Security: The adequacy of security of the network infrastructure, including firewalls, intrusion detection systems, and network segmentation within the States.
- Data Protection: How sensitive data is stored, transmitted, and accessed, ensuring encryption and other protective measures are in place within the States.
- Access Controls: User access controls operate to ensure that only authorised personnel have access to sensitive information and systems with the States.
- Incident Response Plan: A well-defined incident response plan is in place to address potential security breaches and minimise damage both within the States and Island-wide.

- Employee Training: Systems users within the States are trained in cyber security best practices and are aware of potential threats such as phishing attacks.
- Physical Security: Physical security measures in place within the States protect hardware and data from unauthorised access or theft.
- Compliance: There is compliance with relevant industry regulations and standards both within Government and in respect of Island-wide arrangements.
- Vulnerability Assessments: Regular vulnerability assessments and penetration testing are in place across States systems to identify and address potential weaknesses in systems.
- Security Policies: A comprehensive and up-to-date suite of policies is in place both within the States and in respect of Island-wide arrangements.
- Risk Management: A risk management framework is in place to identify, assess, and mitigate States and Island-wide cyber security risks.
- Business continuity: Effective plans are in place for critical services on the Island to respond in the event of a cyber attack.
- Horizon planning: Island-wide and States governance arrangements ensure that emerging threats, including the threats from improper or inadvertent use of Artificial Intelligence, are identified and integrated into the ongoing approach

The following people contributed information through interviews or by correspondence:

- Chief Information Officer, Government of Jersey
- Director JCSC
- Representatives from Digital Services
- Representatives from Island Energy Group
- Representatives from Jersey Electricity

- Representatives from JT
- Representatives from States of Jersey Police.

The fieldwork was carried out by affiliates working for the Comptroller and Auditor General, from June 2025 to January 2026.

JERSEY AUDIT OFFICE

LYNN PAMMENT CBE
Comptroller and Auditor General

Jersey Audit Office, Jubilee Wharf, 24 The Esplanade, St Helier, Jersey JE2 3QA

T: +44 1534 716800 E: enquiries@jerseyauditoffice.je

W: http://www.jerseyauditoffice.je