Australian Government
National Office of Cyber Security

National Office of Cyber Security | MediSecure Cyber Security Incident Evaluation Report

December 2025

This document is classified for 'OFFICIAL | TLP: CLEAR. More information on Traffic Light Protocol can be found at: Traffic Light Protocol (TLP) | Australian Signals Directorate.

Acknowledgements

The National Office of Cyber Security (NOCS) would like to acknowledge all government and industry stakeholders who supported and provided input to the MediSecure Evaluation.

Contents

Executive Summary

On 15 May 2024, the National Office of Cyber Security (NOCS) was informed that MediSecure Ltd. (MediSecure) had been the victim of a cyber security incident. The incident involved the reported exfiltration of approximately 6.5 terabytes of data, exposing the contact information and health data of approximately 12.9 million Australians. Following this notification, the NOCS supported MediSecure by coordinating the whole-of-government response to the incident. The NOCS provided consequence management support until formal coordination of the incident concluded on 30 September 2024.

On 3 June 2024, MediSecure entered voluntary administration, with FTI Consulting (FTI) appointed as administrators. MediSecure stated that voluntary administration was necessary due to its limited financial resources and the costs involved in responding to the cyber security incident. MediSecure and its administrators were represented and supported by a specialist cyber law firm (Mills Oakley) and a cyber security forensic firm (McGrathNicol) throughout the incident response.

In February 2025, the NOCS commenced an evaluation into the whole-of-government coordination of the response to the 2024 MediSecure cyber incident (the incident). The NOCS conducted a formal evaluation process and led the development of the MediSecure Evaluation Report (the Report). The Evaluation included extensive engagement with key Commonwealth, state and territory governments, health sector industry representatives, and MediSecure and its administrator's representatives.

In line with continuous improvement practices under the Australian Government Crisis Management Framework (AGCMF)[1], the NOCS continues to work with Commonwealth, state and territory government agencies, following the MediSecure incident, to improve cyber security preparedness and response arrangements, to best support the national response to significant cyber incidents.

[1] The AGCMF was endorsed by the Prime Minister in September 2024, and details the overarching policy framing Australia's crisis response arrangements across all-hazards.

Key Insights

The Evaluation identified 11 key insights in relation to the coordinated response to the incident, including that the coordinated response was effective and supported MediSecure, its administrators, government entities and the wider health sector, to manage the consequences of the incident.

1. **Central coordination as a practice continues to reduce the burden on the impacted entity in responding to a cyber incident.** This is especially true during a complex and evolving incident. It also supports a shared understanding of the incident and actions to be taken across all government stakeholders.
2. **Agile response arrangements assisted in managing the changing circumstances of the incident, in adapting to actions made by the threat actor and changes to the Australian Government's understanding of the equities involved.** This further assisted in convening government stakeholders to address novel developments such as MediSecure entering voluntary administration.
3. **Allowing for dedicated forums to facilitate engagement between various government agencies, and between government agencies and the health sector, helped to foster trust and enabled consideration of the diverse range of stakeholder needs and how to address them.**
4. **Effective, regular and early public communications are important in ensuring common understanding across the broad range of affected stakeholders.** Consideration should be given to the speed at which communications are first circulated and updated during a cyber incident.
5. **There are opportunities for the Australian Government to develop policies outlining how to respond to significant cyber incidents that specifically impact a business that subsequently enters voluntary administration or liquidation.**
6. **Assigned working group roles and responsibilities can be better defined and communicated with attendees at the outset.** This will assist in establishing clear expectations for working group scope and outcomes early, and support the awareness of both government and industry stakeholders, their role and how they will be expected to assist the response as part of a working group.
7. **Stakeholders require clearer guidelines outlining whether information can be shared more broadly among their communities,** reflecting both the 'Traffic Light Protocol' used during the incident and the limited use obligation established under the *Cyber Security Act 2024.*
8. **There is an opportunity for the Australian Government to further standardise its processes and procedures that outline how to conclude a coordinated response,** including clear notice to partners and industry stakeholder groups, as well as clear avenues for ongoing support.
9. **The Australian Government's role in a cyber incident involving a company in administration or liquidation will be an ongoing discussion for relevant agencies,** including consideration of legal, policy, communications and logistical challenges.
10. **Managing cyber risks for Small to Medium Enterprises is an important consideration for the Australian Government,** as despite their size, SMEs have the capacity to process and retain significant volumes of personal and/or sensitive data.

11. **There are significant opportunities to harness the personal networks and informal channels used to coordinate an effective cyber response into formal practices,** to ensure that stakeholders and government officials can replicate the successes of the MediSecure incident response in future.

Purpose

As Lead Coordinating Senior Official for Cyber Incidents under the AGCMF, the National Cyber Security Coordinator (the Coordinator) conducts post-response evaluations and supports integration of relevant lessons identified into the continuous improvement of the government's crisis management arrangements.

While whole-of-government coordination of the MediSecure incident occurred prior to the inclusion of an evaluation requirement in the AGCMF, the Coordinator recognises that a formal evaluation into the MediSecure response is an essential mechanism under which the NOCS can contribute to enhanced cyber security response and resilience across the Australian economy.

Evaluation processes are imperative to enhancing the government and industry's understanding of their evolving incident response requirements. The Evaluation process enables the incident response to be comprehensively considered, in order to understand what worked well, opportunities for improvement, and whether the government's intended results aligned with their actual results. The Evaluation considered the spectrum of response arrangements, including whether specific actions or processes should be retained, altered or reconsidered in the future.

The NOCS's evaluation methodology is based on the 'OILL' methodology, in alignment with the National Emergency Management Agency (NEMA) lessons management processes. This report presents insights for stakeholder consideration. The NOCS will support relevant parties to use this report to identify and integrate lessons into their consequence management processes.

The Evaluation included extensive engagement with key Commonwealth, state and territory governments, health sector industry representatives, and MediSecure's representatives.

OILL Methodology

OILL stands for[2]:

- **Observation**: a record of a fact or occurrence that someone has heard, seen, noticed or experienced as an opportunity for improvement or an example of good practice.
- **Insight**: a deduction drawn from the observations, which needs to be further considered. Insights may also identify an opportunity for further analysis. It is worth noting that insights can be positive or negative, and define the issue rather than the solution.
- **Lessons Identified**: a conclusion with a determined root cause based on the analysis of one or more insights and a viable course of action that can either sustain a positive action or address an area for improvement.
- **Lessons Learned**: A lesson is only learned once the approved change is implemented and embedded in the organisation.

[2] https://knowledge.aidr.org.au/resources/handbook-lessons-management/.

Scope

The Evaluation considered the following elements of the 2024 MediSecure cyber incident and the coordinated response:

- The **response arrangements** that supported the actions undertaken by and between the Commonwealth, state and territory governments, MediSecure, and the broader health sector during its duration as a Tier 3 incident under the AGCMF.
- How these response arrangements contributed to **decision-making** and **information sharing**.
- Specific **consequence management activities** related to cyber security.
- **Outcomes** and actions underway to enhance incident response arrangements.

The Evaluation did not consider:

- The cause or fault of the incident.
- MediSecure's cyber security posture or practices, prior to or following the incident.
- The nature of contractual arrangements, or otherwise, relating to the storage and handling of information.
- Whether parties to the incident were compliant with Australian regulatory frameworks.
- Any regulatory actions considered or undertaken.
- The ongoing threat posed by the threat actor, or other aspects related to law enforcement.
- The technical response to the incident.

The Incident

MediSecure operated a prescription delivery service to support the digital flow of prescriptions between health care providers and consumers. At the time of the incident, it was one of two prescription delivery services operating to exchange prescription information between prescribers (e.g. general practitioners) and pharmacies.

The Department of Health, Disability and Aging (DoHDA) advised that from 2010 to 2023, MediSecure operated in a private market without a contractual relationship with the government. Community pharmacies received government subsidies that were then passed on to MediSecure and other prescribing software companies. In 2023, DoHDA[3] finalised a tender to bring these services under a government contract, which was awarded to prescription delivery service eRx operated by Fred IT Group.

DoHDA advised that government contracted MediSecure for a brief period in 2023 to support MediSecure customer data and prescriptions to transition to the eRx service. After this period, DoHDA advised that MediSecure no longer had direct system connections with eRx, prescription software in primary care, government systems, or My Health Record.

On 15 May 2024, the NOCS became aware that MediSecure had experienced a cyber security incident. This incident involved the reported exfiltration of approximately 6.5 terabytes of data.

The incident exposed sensitive information, including contact and health information, of approximately 12.9 million Australians whose prescriptions were distributed by MediSecure's prescription delivery service during the approximate period of March 2019 to November 2023. Following months of public communications, data analysis and incident coordination, MediSecure's public statement on 18 July 2024 advised that the sensitive data included:

- Personal information (name, date of birth, email address, phone number, physical address);
- Health and Concession card information including card numbers, identifiers and expiry dates (Individual Healthcare Identifier (IHI), Medicare cards, Pensioner cards, Commonwealth Seniors cards, Veteran cards, and Healthcare Concession cards); and
- Prescription medication details (name of medication, strength, quantity, number of repeats, reason for prescription and instructions).

A number of health sector industry representatives and DoHDA officials reported that the incident caused a high degree of concern among Australians who believed that the cyber incident had affected their ability to fill prescriptions and access medications. It was a concerted effort by the NOCS, the Department of Health and Aged Care, and health industry partners to correct this perception and relay that Australians were still safe to access or extend prescriptions through normal means.

From 15 May 2024, the NOCS supported MediSecure, and later its administrators, in a coordinated Australian Government response to manage the consequences of this incident. This coordinated response lasted five months, and involved meetings with MediSecure, its legal representatives, its administrators and consultants, as well as a range of coordination

[3] At the time, referred to as the Department of Health and Aged Care.

meetings across the Commonwealth Government, state and territory governments, and the broader health sector.

Incident Timeline

Key developments relating to the incident included:

- 15 May 2024 – the NOCS became aware of the incident.
- 16 May 2024 – the Coordinator co-Chaired a National Coordination Mechanism (NCM) with NEMA Deputy Coordinator-General Buffone and held coordination meetings with relevant government and non-government representatives, to establish facts and consequences.
- 17 May 2024 – the Coordinator and NEMA Deputy Coordinator-General Buffone co-Chaired an NCM with relevant government and non-government representatives.
- 18 May 2024 – the NOCS published advice on a dedicated webpage of the Home Affairs website, to provide a central reference point for government agencies receiving inquiries from the public, and to advise both medical professionals and the public on what steps or precautions to take in response to the incident. The Coordinator also issued a public statement on LinkedIn and X (formerly Twitter).
- 24 May 2024 – the Coordinator and NEMA Deputy Coordinator-General Buffone co-Chaired an NCM with relevant government and non-government representatives.
- 3 June 2024 – MediSecure entered voluntary administration, with FTI appointed as administrators.
- 18 July 2024 – MediSecure and FTI released a public statement to describe the nature and magnitude of the incident and data breach.
- 13 September 2024 – the Office of the Australian Information Commissioner (OAIC) released a public statement advising it had closed its inquiries into the MediSecure data breach and would not pursue an investigation into the personal information handling practices of MediSecure.
- 30 September 2024 – the Coordinator formally concluded the Government's coordinated response to the incident.

Following the conclusion of coordinated support, the Coordinator determined that a formal evaluation process be undertaken in alignment with the AGCMF.

The Coordinated Response

Designation

The NOCS designated the incident 'Nationally Significant' and the Coordinator led the response given the potential consequences or impacts the incident posed. This included the likelihood of a large number of Australians being impacted, the requirement to coordinate across all jurisdictions, and the high media interest in an incident of this nature.

Coordination

During the period of coordination from 15 May 2024, the NOCS convened or co-chaired over 64 meetings and briefings, including:

- **3** NCMs, which were attended by key representatives from the Australian, state and territory governments.
- **21** Interdepartmental meetings, focussed on communication planning and advice, state and territory briefings and technical discussion.
- **12** Operational level working group meetings, focussed on communication and identity services and security considerations and other sensitive issues.
- **8** Health sector, industry and peak body briefings.
- **20** other bilateral meetings with impacted entities, regulators and professional services.

Public communications

The Coordinator and the NOCS coordinated a public advice campaign to update the Australian public on the MediSecure cyber security incident. This included news television appearances by the Coordinator, social media posts on X (formerly Twitter) and LinkedIn, as well as the novel use of a public advice page on the Department of Home Affairs website[4].

The MediSecure public advice page included context on the Australian Government's understanding of the incident, and highlighted additional support networks and resources available to help Australians protect themselves online if they were concerned about their personal information having been impacted in the incident. This approach was novel, though deemed necessary in light of MediSecure's limited financial resources to engage support services to support impacted individuals and meet legal obligations, as is common in response to large data breaches.

[4] https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/cyber-coordinator/medisecure-cyber-security-incident.

The Evaluation Process

In early 2025, to inform the Evaluation, the NOCS hosted a number of engagement sessions with:

- MediSecure and its representatives.
- Key Australian Government agencies.
- State and territory government entities.
- Health sector industry representatives.

Key insights were observed across a breadth of themes, including:

- The benefit of the NOCS coordinating responses to significant cyber security incidents.
- The establishment and operation of working groups, including the quality of meetings and whether they were fit-for-purpose.
- The importance of establishing trust between the NOCS and MediSecure, including their legal and cyber security advisors at Mills Oakley and McGrathNicol, to support the response to a significant cyber incident and further the national interest.[5]
- The importance of setting clear expectations of stakeholders and communicating them effectively, particularly early in the coordination of an incident.
- The effectiveness of advice and communication materials distributed throughout the incident.
- The role of the Australian Government in managing or supporting cyber security incidents affecting businesses entering or under financial administration.

Key observations were grouped into insights under the categories of:

- **What worked well** and should be considered for future consequence management activities.
- **What was challenging** and should inform additional or different approaches in future incidents.
- **What was novel** or unique to the response that we can learn from for future consequence management activities.

[5] It was noted by MediSecure's advisors that the incident occurred prior to the establishment of the 'Limited Use Provision' within the *Cyber Security Act 2024* (passed on 29 November 2024), which further reinforced the importance of the NOCS undertaking the engagement in good faith.

What worked well?

Key Insights

1. **Central coordination as a practice continues to reduce the burden on the impacted entity in responding to a cyber incident. This is especially true during a complex and evolving incident.** It also supports a shared understanding of the incident and actions to be taken across all government stakeholders.
2. **Agile response arrangements assisted in managing the changing circumstances of the incident, in adapting to actions made by the threat actor, and changes to the Australian Government's understanding of the equities involved.** This further assisted in convening government stakeholders to address novel developments such as MediSecure entering voluntary administration.
3. **Allowing for dedicated forums to facilitate engagement between various government agencies, and between government agencies and the health sector, helped to foster trust and enabled consideration of the diverse range of stakeholder needs and how to address them.**
4. **Effective, regular and early public communications are important in ensuring common understanding across the broad range of affected stakeholders.** Consideration should be given to the speed at which communications are first circulated and updated during a cyber incident.

Discussion

- **MediSecure's representatives and government stakeholders acknowledged the benefits of a centrally coordinated consequence management function.**
  - Central coordination reportedly reduced the burden on the entity as it navigated complexities relating to its pending administration, and supported the consistent sharing of important information among the large number of relevant government and industry stakeholders.
  - Government and industry stakeholders felt informed through the provision of briefing by the Coordinator and the NOCS on MediSecure's behalf, which MediSecure and its representatives appreciated. These actions also supported MediSecure's management of the incident, as the NOCS was able to consolidate queries and concerns from across the government and the health sector, and disseminate MediSecure's responses back to these stakeholders.
  - This greatly assisted in building and maintaining trust between the government and MediSecure, allowing for greater transparency and speed in the information flowing between the two.
  - Representatives from Commonwealth and state and territory governments, noted the benefit of receiving regular situation reports, talking points and briefings. This approach supported harmonised communication to stakeholders and fostered trust in the whole-of-Australian-Government response.

- **Government agencies acknowledged improvements in the Australian Government's coordinated response activities over time, reflecting on its coordinated response to previous significant cyber incidents.**
  - When Government stakeholders reflected on the lessons they learned from previous incident responses, notably during the 2022 Medibank Private incident and the 2023 HWL Ebsworth incident, they identified significant improvements to the processes used by the NOCS and its government partners.
  - Several agencies stated that seeing the commitment of the NOCS and its partners to continuously improve, even between notably different types of cyber incidents, allowed them to develop a deepened appreciation for the level of collaboration required for such nationally significant incidents.
  - A number of the learning opportunities identified for Government in the 2024 HWL Ebsworth Lessons Learned Review[6] were appropriately actioned in the time between that incident and the MediSecure incident. This included careful management by government of working group membership, consideration of broad groups of stakeholders, careful consideration of the impacts of identity credential information, and supporting consistent and accurate public communications.
- **The agile approaches employed by the NOCS enabled it to effectively respond to the fast-paced and unprecedented nature of the incident, and quickly engage with agencies and organisations relevant to the response.**
  - Coordination and response actions within the first two weeks of the incident required the NOCS to contend with several challenges including the size and complexity of the impacted dataset, the unpredictable actions of the threat actor and the uncertainty of MediSecure as a going concern.
  - During this time, the NOCS was able to swiftly stand up a dedicated response team to coordinate government and industry working groups, as well a number of other engagements across government to address the broader policy concerns.
  - Both MediSecure and other stakeholders described the NOCS's facilitation of meetings and communications to be of high quality overall. However, the fast-paced nature of the incident resulted in many stakeholder meetings being held with minimal notice, which caused some representatives to delegate attendance, or rearrange their schedules and attend with minimal briefing.
  - Support from operational agencies was invaluable in briefing the Coordinator on developments of the investigation into the threat actor and the evolving risks of the data being more widely published, which informed her decisions as the Lead Coordinating Senior Official to help mitigate those risks.
  - MediSecure's representatives particularly valued the Coordinator's facilitation of engagement with relevant industry leaders to discuss particular challenges of the incident response.
  - It is important to note that the need to coordinate numerous working groups across affected stakeholders, coupled with the unpredictable movements of the threat actor, impacted on the health and wellbeing of some individuals responding to the incident.

[6] https://www.homeaffairs.gov.au/reports-and-pubs/PDFs/nocs-hwl-ebsworth-lessons-learned-report.pdf.

These impacts were felt by all stakeholders that were actively involved in the incident response, across both government agencies and the incident response firms. It was widely recognised that a cyber security response over a sustained period can have significant effects on staff mental health and wellbeing including stress, burnout and anxiety.

- **Working groups provided appropriate forums for stakeholders to discuss their needs and address the various complications of the incident as it developed.**
  - The NOCS convened the following working groups to coordinate consequence management activities: the Communications Working Group, the Health Sector Government Working Group, the Health Sector Industry Working Group, the Sensitive Issues Working Group, and the eDiscovery Working Group. The NOCS worked jointly with NEMA to facilitate the NCM for wider situational awareness and Australian Government coordination. Additional groups were convened throughout the incident as necessary to address questions of identity protection, policy or legislative challenges.
  - Stakeholders generally agreed that these working groups were effective in allowing for thematic discussion on various aspects of the incident, and in sharing information to build a common understanding of the incident.
  - Health sector representatives identified difficulties in early working group meetings due to the lack of information on the exact nature of the impacted dataset, which limited the advice the government was able to share with working group participants. As the data analysis process continued, the government worked with MediSecure to produce public advice, communications and briefing to officials that better reflected the type of data compromised and the potential implications for impacted individuals.
- **Communications products issued by the NOCS and government were considered to be effective, efficient and clear.**
  - Many stakeholders noted the success of the MediSecure Cyber Security Incident public advice page, which acted as a central source of information for reference by relevant agencies, health organisations and the general public. While the full suite of advice took several days to prepare, the webpage served as a reference for crisis communications of the broader health sector. There are opportunities to expedite the creation and clearance of advice from across government during a nationally significant cyber incident. The use of public advice pages should be considered for future incidents.
  - Government and industry stakeholders also noted their appreciation for the quality and frequency of communications products shared by the NOCS, including situation reports and advice. These assisted in addressing common concerns such as ongoing impacts on prescription services, impacts on identity documents, and how to protect medical information online.
  - Communications and Media stakeholders also noted the success of the Coordinator's social media posts. Analytics were reported to have demonstrated both the significant reach of this messaging during an active incident and the strong community demand for information. While this was one element of a multi-faceted communications plan involving television and radio interviews, future incidents may involve an increase in use of the Coordinator's social media platforms as an incident management tool (in addition to other avenues for communication).

What was challenging?

Key Insights

5. **There are opportunities for the Australian Government to develop policies outlining how to respond to significant cyber incidents that specifically impact a business that subsequently enters voluntary administration or liquidation.**
6. **Assigned working group roles and responsibilities can be better defined and communicated with attendees at the outset.** This will assist in establishing clear expectations for their scope and expected outcomes early, and support the awareness of both government and industry stakeholders, their role and how they will be expected to assist the response as part of a working group.
7. **Stakeholders require clearer guidelines outlining whether information can be shared more broadly among their communities,** reflecting both the 'Traffic Light Protocol' used during the incident and the limited use obligation established under the *Cyber Security Act 2024.*
8. **There is an opportunity for the Australian Government to further standardise its processes and procedures that outline how to conclude a coordinated response,** including clear notice to partners and industry stakeholder groups, as well as clear avenues for ongoing support.

Discussion

- **MediSecure's representatives and government stakeholders acknowledged the significant challenge posed by managing the consequences of a cyber incident when the victim entity enters administration.**
    - Stakeholders widely recognised that the legal requirements of a company under voluntary administration would restrict the use of company funds for cyber incident management purposes, cyber forensics or analysis of the scope of the impacted data. Government stakeholders further noted that at the time of the incident, there was no established process determining how impacted individuals should be notified of a data breach by a company entering administration, or what the government's role would be in this scenario.
    - Government stakeholders central to the response suggested that successful management of the incident and its consequences was possible in large part due to the willingness of the firms which stepped in to support MediSecure and its administrators. These firms noted that they took into account the national significance of the incident and the national interest as a whole, in deciding to continue to support the administrators and work with the NOCS. However, it is clear that similar arrangements cannot be relied upon by government for future incidents affecting entities under administration, or other entities without the resources to expend on incident management firms.
    - It was noted across government that, outside of law enforcement and investigative functions, there is no agency with the appropriate legal authority and technical capability to conduct data analysis of a compromised dataset for consequence management purposes. Creation of a data analysis capability would require both

funding and skilled personnel, as well as the legislative authority to store and analyse compromised datasets concerning personally identifiable information of individuals. During the MediSecure incident response, a data analysis solution was provided by eDiscovery specialists engaged by MediSecure's and the administrator's legal representatives.

- It was also widely acknowledged by stakeholders that the Australian Government could more broadly consider arrangements for the management of future incidents involving a business entering or under administration.

- **Multiple stakeholders expressed a need for greater clarity of working group roles and responsibilities early in the incident, suggesting that governance documents should be established to strengthen understanding.**
  - Industry stakeholders suggested that early working groups did not adequately convey the purpose of the NOCS, the role of the industry representatives at these meetings, or what was needed from the forum before centralised advice could be produced. Health sector stakeholders suggested that this may have impacted the clarity of outcomes from early Health Sector Industry Working Group meetings, potentially leading to delays in the creation of targeted industry advice. Some industry representatives suggested that working groups be provided with advice upfront to outline the role of the NOCS and the working group, reflecting that this advice would assist industry representatives to provide their views and equities to government faster.
  - Similarly, several government stakeholders reflected that working group meetings would benefit from clarity about roles and responsibilities, in order to support them with preparing to represent their departmental equities and inform government decisions. They noted that a statement circulated ahead of working group meetings to articulate its purpose and the expected roles of attendees would assist.
  - Representatives of both the NOCS and DoHDA noted that the NOCS's Health Sector Playbook,[7] published six months following the MediSecure incident, could provide non-government entities with clarity about how the NOCS will coordinate the national response and consequence management activities for a future incident impacting an entity in the health sector. However, they further posited that additional details may be required during a live incident in order to acquaint them with specific expectations.

- **The eDiscovery Working Group, created to update government stakeholders on the progress of analysing the impacted dataset, was challenged by stakeholders' different understandings of its scope and purpose.**
  - Data analysis efforts faced two key constraints: the complexity and volume of the impacted dataset, and the nature of the eDiscovery contract. This meant that any scope increase for the data analysis would be lengthy to perform and difficult to agree with the provider.
  - While the Australian Government does not have an eDiscovery capability for consequence management, government stakeholders were keen to understand statistics and metadata about the impacted dataset, and identify what information was pertinent and possible to extract.

[7] https://www.homeaffairs.gov.au/cyber-security-subsite/files/health-sector-playbook.pdf.

- All relevant stakeholders agreed that future working groups of this nature should commence with a clear vision of the scope and what outcomes are to be expected from the process.

- **Multiple health sector stakeholders expressed that they would like greater clarity about how much of the information and government communications can be shared with their communities.**
  - Health sector stakeholders indicated a strong need for government to be clear about what information can be shared beyond the working groups. Understandings differed between government and health sector stakeholders on whether early information on the incident, ahead of public statements by MediSecure, could be shared more broadly with health organisations or their communities.
  - Stakeholders would also appreciate clarification on the meaning and use of the 'Traffic Light Protocol' – a system of markings commonly used by the critical infrastructure and incident coordination and response communities, which was used by the NOCS to classify and designate the sensitivity of information shared with non-government entities, to ensure it was appropriately protected. This clarification will support industry bodies as they develop and issue statements or advice in relation to cyber security incidents.
- **There are opportunities to consider how to strengthen the effectiveness and focus of the Sensitive Issues Working Group.**
  - The working group was created to explore the risk of harm to various cohorts of the Australian population considered to be at heightened risk as a result of the MediSecure incident. The working group brought together officials across Commonwealth and State and Territory jurisdictions, representing agencies including public health, law enforcement, and community justice.
  - However, the nature and extent of the data exposed through the MediSecure incident required officials to speak on behalf of a broad range of vulnerable cohorts with specific sensitivities.
  - The broad range of roles and remits in attendance made it difficult for agencies to reach consensus around prioritisation of groups impacted by the incident, the role of the Commonwealth as distinct from the States and Territories, actions that should be taken following a data breach but before a cybercrime is identified, and what types of exposed data, including prescriptions, heightened an individual's vulnerability.
- **The conclusion of coordinated response activities for the incident highlighted opportunities to develop a formal and standardised process of incident closure.**
  - Following five months of coordinated consequence management activities, the NOCS ceased government coordination of the response to the incident, while remaining alert to new information.
  - In 2024, the Government's Lessons Learned Report into the HWL Ebsworth incident noted 'the clear need for earlier communication of the cessation of coordinated activities during future incidents'. The coordinated response to the MediSecure incident demonstrated an improvement to the government's closure processes, with government and entity stakeholders given advanced notice of the closure.
  - However, many stakeholders expressed confusion during the Evaluation when informed of the date that the incident response was declared 'closed' from the

Commonwealth's perspective. It was noted by incident responders that a lack of clarity on the date of closure complicated post-incident engagement with government and industry stakeholders, creating a reputational risk.

- Both government and industry stakeholders suggested that the process of closing an incident be further standardised and made more transparent. They proposed that this would bring clarity to stakeholders regarding the cessation of coordinated management activities and better inform their actions and responsibilities post-incident.

What was novel?

Key insights

9. **The Australian Government's role in a cyber incident involving a company in administration or liquidation will be an ongoing discussion for relevant agencies,** including consideration of legal, policy, communications and logistical challenges.
10. **Managing cyber risks for Small to Medium Enterprises is an important consideration for the Australian Government,** as despite their size, SMEs have the capacity to process and retain significant volumes of personal and/or sensitive data.
11. **There are significant opportunities to harness the personal networks and informal channels used to coordinate an effective cyber response into formal practices,** to ensure that stakeholders and government officials can replicate the successes of the MediSecure incident response in future.

Discussion

- **The incident prompted stakeholders to consider the Australian Government's role in a significant cyber incident when an entity providing third party services to the government enters administration, including the question of financial support or direct government action to advise individuals of their equities on the entity's behalf.**
  - MediSecure's public statement on 18 July 2024 stated that it requested funding from the Australian Government to assist in the costs associated in responding to the incident. This request was denied, but led to a number of discussions across the government.
  - Throughout the incident and evaluation process, the government explored the legal, policy and logistical challenges of a government-led effort to analyse the dataset and notify impacted individuals. Following this report (as detailed in the 'Applying the lessons' section), the NOCS and Coordinator will encourage discussions throughout government on opportunities to further enhance cyber security response and resilience in Australia, including on potential solutions to this challenge.
- **This was one of the first cyber incidents impacting an SME with a significantly outsized impact on Personally Identifiable Information (PII)[8] relative to its size and annual turnover.**
  - At the time of the incident, MediSecure was considered an 'APP Entity' under APP11 of the *Privacy Act 1988*, as it had an annual turnover of more than $3,000,000 and was a health service provider in its capacity of holding individual health information. This meant that MediSecure had obligations under the Notifiable Data Breaches Scheme.
  - MediSecure's representatives noted that the company had a small staffing footprint at the time of the incident, and only a small budget with which to fund a media strategy, communications strategy and legal strategy including during the period prior to its

[8] Referred to as 'personal information' in the *Privacy Act 1988*.

voluntary administration. Contrasted with their limited resources, the compromised dataset contained prescription information for 12.9 million Australians.

- This incident highlights the fact that even small organisations may be exposed to substantial privacy risk.
- It was noted by stakeholders that because MediSecure was not classified as a 'Critical Infrastructure' entity under the *Security of Critical Infrastructure Act 2018* (SOCI), it was not legally obligated to report cyber security incidents to www.cyber.gov.au within 72 hours of the incident's detection.
- During the Evaluation, stakeholders from both government and industry made comments regarding the ability of SMEs to adequately fund and protect their networks and data holdings from sophisticated cyber actors. SMEs often face resourcing constraints during cyber incidents when compared with larger and well-resourced entities, which can make them more attractive targets to cyber-criminals.
- Opportunities identified by the stakeholders to help mitigate cyber risks for Government contractual arrangements with SMEs included: developing more robust cybercrime reporting obligations, requirements for supply chain audits, and the importance of cyber insurance for SMEs.
- The NOCS will use lessons identified to support the Department of Home Affairs in its development of Horizon 2 of the 2023-30 Cyber Security Strategy.

- **Stakeholders noted that informal networks across government and industry were invaluable during the response, and can be better formalised for future incidents.**
  - The coordination across government agencies during the response was strengthened by existing informal networks of working-level staff, as well as relationships between senior decision makers across Commonwealth, and state and territory government agencies. It was suggested that codifying these practices into standardised operating procedures or other operational documents could improve the consistency of response operations.
- **The MediSecure incident occurred prior to the passage of both the *Cyber Security Act 2024* on 29 November 2024, and the *Privacy and Other Legislation Amendment Act 2024* on 10 December 2024. Government stakeholders noted that similar incidents could now benefit from enhanced clarity and information sharing.**
  - The 'limited use obligation' under the *Cyber Security Act 2024* ensures that information shared by the impacted entity with the NOCS can only be disclosed for a permitted cyber security purpose and is not admissible in criminal or civil proceedings for contravention of a civil penalty provision[9] against the impacted entity.
  - This level of information protection could have assisted in the sharing of information about the MediSecure breach during the early Communications Working Group meetings, and some government stakeholders suggested that this mechanism could have allowed for advice to be disseminated throughout the government more quickly.
  - Among a variety of other functions, reforms under the *Privacy and Other Legislation Amendment Act 2024* clarified APP entities' obligations under APP 11.1, which requires entities to take reasonable steps to protect the personal information they hold

[9] Except under Part 4 of the Act.

from misuse, interference and loss, and unauthorised access, modification or disclosure.

- The *Privacy and Other Legislation Amendment Act 2024* also introduced APP 11.3, which specifies that '*reasonable steps*' in APP 11.1 includes '*technical and organisational measures*'. The Explanatory Memorandum to the *Privacy and Other Legislation Amendment Bill 2024*[10] provides examples of both technical and organisational measures. Examples of technical measures include protecting information through physical measures, software and hardware. Examples of organisational measures include steps and processes that an entity should implement, such as employee training on data protection.

[10] Privacy and Other Legislation Amendment Bill 2024: Explanatory Memorandum.

Applying the lessons

Following the MediSecure incident, the NOCS began identifying opportunities for internal improvement, and continues to apply the lessons identified to its response processes. As immediate next steps from the Evaluation, the NOCS will:

1. Conduct further engagement with the health sector on the role of NOCS during a cyber security incident and how impacted organisations can request coordinated support from the government to manage the consequences of cyber incidents.
2. Better define and communicate the expectations around the roles and responsibilities of working groups and attendees, and consider updates to the NOCS Health Sector Playbook[11] for cyber incidents.
3. Develop processes to better support effective engagement with industry and government agencies during a cyber incident, including the creation of materials to be distributed during the early phases of an incident, especially for the establishment of working groups.
4. Encourage discussions throughout government on opportunities to further enhance cyber security response and resilience in Australia, including with small and medium enterprises.
5. The NOCS will share lessons identified to support the Department of Home Affairs in its development of Horizon 2 of the *2023-2030 Australian Cyber Security Strategy*.

[11] https://www.homeaffairs.gov.au/cyber-security-subsite/files/health-sector-playbook.pdf