Forescout Technologies PTY LTD. C/O We Work. 333 George Street, Office No. 05-128 Sydney, NSW, 2000 Australia

Toll-Free (US) 1.866.377.8771 **Tel (Intl)** 1.408.213.3191 **Fax** 1.408.371.2284 **Website** www.forescout.com

auscyberstrategy@homeaffairs.gov.au

Forescout is pleased to provide this response to the 2023 – 2030 Australian Cyber Security Strategy Discussion Paper.

With more than 20 years of experience providing automated cybersecurity at scale, Forescout[1] has earned the trust of Fortune 100 organisations and government agencies across the globe, including Australia. This document will not seek to elaborate on Forescout's technology or use cases for that technology; instead, it will seek to answer some of the questions raised in Attachment A of the Discussion Paper, particularly those questions where our experience or intellectual property underpins the Forescout perspective.

Specifically, Forescout has actively participated in several initiatives of the US Government, including the Comply-to-Connect program[2], designed to improve cybersecurity across government agencies. If replicated in Australia, this program will significantly accelerate the achievement of several Cybersecurity Strategy objectives to strengthen network resilience, detect and mitigate threats and respond to cybersecurity incidents.

Forescout's experience working with government and enterprise clients around the world, providing tangible support to help identify and mitigate potential threats, respond to incidents, and improve overall security posture, leads us to recommend the adoption of a standardised approach for securing networks of devices that provides key protection and mitigation strategies. For example, using the Comply-to-Connect common framework, the US Department of Defence (DoD) ensures devices are secure while delivering insights into operating compliance across its agencies in the US and abroad[3]. This framework has provided benefits through increased cyber resilience by protecting large data sets and utilising automation and integration to use scarce resources more effectively.

[1] Forescout Technologies Pty Ltd, ABN 99 607 749 771, https://www.forescout.com
[2] https://www.forescout.com/wp-content/uploads/2017/08/ForeScout-Comply-to-Connect-Brief.pdf
[3] https://www.c4isrnet.com/it-networks/2020/04/21/for-the-navys-hospital-ships-networking-is-yet-another-challenge/

Forescout Technologies PTY LTD. C/O We Work. 333 George Street, Office No. 05-128 Sydney, NSW, 2000 Australia

Toll-Free (US) 1.866.377.8771 **Tel (Intl)** 1.408.213.3191 **Fax** 1.408.371.2284 **Website** www.forescout.com

To assist in explaining the importance of the Comply-to-Connect framework for the Australian Government in the context of the 2023-2030 Cyber Security Strategy, Forescout would like to respond to the following questions raised in the Discussion Paper:

> Question 6: How can Commonwealth Government departments and agencies better demonstrate and deliver cyber security best practices and serve as a model for other entities?
>
> Question 10: What best practice models are available for automated threat-blocking at scale?
>
> Question 17: How should we approach future-proofing for cyber security technologies out to 2030?

Comply-to-Connect is a US DoD security framework designed to dramatically improve the level of assurance for authentication, authorisation, compliance assessment and automated remediation of devices connecting to enterprise networks. Within the framework, devices are authenticated and assessed for compliance against DoD security policies before granting access to enterprise network resources. Forescout believes that the same drivers for the US DoD to develop and adopt this framework also applies to the protection, management and assurance of devices managed by the Australian Government.

Only compliant devices gain full access to the network through a 'zero trust' approach. Non-compliant devices receive limited access to network services and are automatically remediated, reassessed as compliant and granted network access once compliant. Unauthorised devices are restricted and unable to access the network.

In the United States, Comply-to-Connect has been developed and adopted by the Department of Defence because of the following:

- the increasing reliance on evolving IT systems and networks to conduct military operations and perform critical functions, such as logistics, budgeting, building automation and power distribution.
- the urgent need for secure configuration and other defensive fundamentals because leaders can no longer afford to view the safeguarding of "cyber things" and "physical things" as distinct, siloed responsibilities.
- the need to align security more tightly across connected devices, facilities and other platforms is a long-sought, closely-watched objective.
- an all-inclusive view of cybersecurity that is becoming even more urgent as lines continue to blur between traditional office IT, internet-of-things enabled devices, operational technology governing energy, facility access and other physical systems, and medical devices based in our hospitals and healthcare networks.
- the increasing use of "enterprise of things" devices, recognising information technology and operational technology as a singular, united network environment, requiring a holistic, integrated cybersecurity strategy and a unified approach.

Comply-to-Connect enables IT teams to authenticate endpoints, including:

- physical and virtual workstations,

- physical and virtual servers,
- networked user support devices and peripherals,
- mobile devices,
- network infrastructure devices,
- platform information technology devices, and
- internet-of-things devices.

The high value of Comply-to-Connect is that it also applies to non-traditional networked endpoints, including internet of things (IoT) and operational technology (OT) devices such as industrial control systems, building automation systems, weapons and other tactical systems, medical equipment, and many other mission-supporting endpoints.

It combines all systems and their components "in one house" as an integrated whole. With the integrated, zero-trust approach, personnel supporting these systems do not need to search for new, piecemeal tactics for defending these blended systems.

What is necessary is that there must be continuous, real-time device visibility, including complete discovery, classification, security posture assessment and automatic remediation of every network-connected device. Periodic inventories, by definition, do not discover all the devices on the network in real-time. Therefore, obtaining complete visibility through network monitoring techniques to identify multiplying numbers and types of connected endpoints is necessary before any other security tools can be effective.

Automated orchestration of security and management processes is the next step. The greatest value of true network visibility is acting on what is found and governing the systems by extensive compliance and configuration management tools. To drive return on investment, Comply-to-Connect ensures the automation and orchestration of necessary actions to both ensure and, where necessary, restore systems to a trusted state. Where the devices are not compliant, there is control of the level of access to network data, applications and services until a trusted state is achieved.

The most compelling aspect of Comply-to-Connect is its continuous monitoring and oversight of all the components connected to a network. With vast numbers of devices and connected systems across networks and the framework's scope across offices, data centres, cloud, facility and other non-traditional systems, the visibility and ability to monitor the state of the devices on the network is vital. The US National Institute of Science and Technology (NIST)'s Cybersecurity Center of Excellence calls this Continuous Diagnostics and Mitigation (CDM), also being adopted into US federal civilian agencies.

The Comply-to-Connect framework offers more than blocking unauthorised devices and mitigating cyber risks; its more extensive value comes from continuously assessing connected devices and users to ensure the integrity of the data sharing and other services these networks provide.

All users share the same concerns about "what" is connected to their network and "who" is accessing "which" data, applications and services. Fully utilising the framework provides the technical assurance of minimising the risks of one key vulnerability: managing, controlling and having visibility into what is connected to complex networks.[4]

Forescout welcomes further discussion about this highly useful framework that will transform the device management approach in Government while reducing the resources needed to manage networks of devices.

Forescout, therefore, recommends that:

> The Australian Government adopts the Comply-to-Connect framework in a manner that is suitable for the Australian Government environment to ensure devices connected to Government networks are fully compliant and secure.

In response to the key questions asked by the Cyber Security Strategy 2023 – 2030 Discussion Paper, Forescout provides the following answers:

1. To make Australia the most cyber-secure nation by 2030, Forescout recommends the Strategy includes:
   a. Strengthening public-private partnerships for better collaboration and innovation so government and industry work even more closely to better understand threats *through better collaboration, including sharing best practices for early detection and cyber response exercises*.
   b. Continuing the implementation of comprehensive cyber education and awareness programmes.
   c. Investing in research and development of advanced cybersecurity technologies.
   d. *Enhancing* incident response capabilities through a coordinated national approach.
   e. Promoting cybersecurity standards and best practices across all sectors by learning from the US Government's Comply-to-Connect programme.
2. The Australian Government should pursue legislative and regulatory reforms that:
   a. Introduce mandatory operational cybersecurity standards using a mix of legislation, regulation, and regulatory guidance.
   b. Revise the Security of Critical Infrastructure Act to include customer data and systems within the definition of critical assets.
   c. Obligate company directors to address cybersecurity risks and consequences.
   d. Consider implementing a comprehensive Cyber Security Act, drawing inspiration from the US Government's Comply-to-Connect programme, which covers standards, incident reporting, and enforcement mechanisms.
   e. Streamline existing regulatory frameworks to minimise the burden on businesses.

[4] This information has been extracted from:
https://www.nationaldefensemagazine.org/articles/2020/12/3/comply-to-connect-protects-military-systems

f. Prohibit the payment of ransoms and extortion demands in specific circumstances, considering the potential impact on victims, companies, and insurers.
g. Clarify the government's stance on ransom payments and when they may breach Australian law.

3. To build regional cyber resilience, Australia should:

   a. Offer capacity-building assistance to neighbouring countries to assist them in minimising their vulnerabilities.
   b. Encourage regional information sharing and collaboration.
   c. Promote the development of regional cybersecurity frameworks and best practices.

4. Australia can elevate its existing international partnerships by:

   a. Strengthening bilateral and multilateral cooperation on cybersecurity, drawing upon the US Government's Comply-to-Connect programme, so it becomes the standard for Australia and its neighbours.
   b. Participating in joint cyber exercises and information-sharing initiatives.
   c. Collaborating on research and development projects.

5. Australia should actively participate in international standards-setting processes by:

   a. Contributing to developing international cybersecurity standards by bringing Australia's experience to this process.
   b. Promoting responsible state behaviour in cyberspace through diplomacy and collaboration.
   c. Encouraging the adoption of these standards and norms within the region.

6. The Australian Government should:

   a. Adopt cybersecurity best practices across all departments and agencies, such as the US Government's Comply to Connect programme.
   b. Regularly assess and report on their cybersecurity posture, s*haring with industry what good looks like, so industry and government can benchmark effective cyber practices against their own operational experiences.*

7. To improve information sharing, the Australian Government should:

   a. Further develop the secure platform for cyber threat intelligence sharing by engaging with industry and offering a method for all Australian businesses and citizens to opt-in
   b. Continue encouraging collaboration and trust-building between the public and private sectors, *recognising this has commenced, but more can be done.*

8. *Introducing* an explicit obligation of confidentiality upon ASD/ACSC would improve engagement and information sharing during a cyber incident.
9. Expanding the notification regime would improve public understanding of ransomware and extortion, only if it was associated with a significant public information and education campaign. The government needs to ensure vulnerable groups are provided awareness training through community programs, schools and public announcements on all media channels.
10. Best practice models for automated threat-blocking at scale include rule-based and AI-powered threat detection and response systems and machine learning-based threat intelligence platforms, such as those used in the US Government's Comply to Connect programme.

11. Australia requires a tailored approach to uplifting cyber skills beyond the broader STEM agenda, focusing on specialised training and development programmes, targeting talented students early in their education with scholarships and cadetships, working with academia and industry to develop ongoing learning programs.
12. The Australian Government can support the cybersecurity workforce by:

    a. Investing in cybersecurity education and training programmes.
    b. Attracting international talent through immigration policies.
    c. Promoting professional accreditation and certification.

13. The Australian Government should:

    a. Establish a single reporting portal for all cyber incidents to streamline reporting.
    b. Develop a coordinated national response plan for significant cyber incidents.

14. An effective post-incident review and consequence management model should involve information sharing, lessons learned, and continuous improvement.
15. The Australian Government and industry can work together to:

    a. Develop cybersecurity best practice guidelines and resources inspired by the US Government's Comply to Connect programme.
    b. Support and assist small and medium businesses in managing cybersecurity risks.

16. The Australian Government can enhance the cybersecurity ecosystem by:

    a. Investing in research and development initiatives.
    b. Supporting public-private partnerships and innovation hubs *and share learnings and best practices for making these successful.*
    c. Promoting the adoption of cybersecurity technologies, with reference to the US Government's Comply to Connect programme.

17. Futureproofing for cybersecurity technologies out to 2030 should involve:

    a. Ongoing investment in research and development*, including in artificial intelligence and automation, to strengthen and step-up responsiveness to threats and attacks.*
    b. Encouraging innovation and collaboration between academia, industry, and government.
    c. Fostering a culture of security by design in technology development.
    d. Bring the community along on the journey through community awareness programs

18. The Australian Government can better use procurement as a lever to support the cybersecurity ecosystem by:

    a. Collaborating with industry and academia via regular briefings so that all levels of government, industry and academia work together to develop the tools and resources required.
    b. Ensuring all cyber procurements are conducted fairly to ensure the best value-for-money solutions from competitive tendering.
    c. Not limiting cyber procurements to Australian-developed products but ensuring a high level of knowledge transfer to Australian academia and industry if products are sourced from overseas.

19. The Strategy should evolve to address emerging technologies by:

    a. Encouraging the adoption of security by design principles, drawing from the US Government's Comply to Connect programme.
    b. Supporting research into the cybersecurity implications of emerging technologies *to better understand how they can be used in offensive and defensive ways*.
    c. Collaborating with industry and academia to develop best practices and standards for new technologies.

20. The Australian Government should measure its impact in uplifting national cyber resilience by:

    a. Regularly monitoring and reporting on key cybersecurity metrics *sharing the information publicly and with industry in particular*.
    b. Assessing the effectiveness of implemented policies and initiatives *using data and analysis to understand better what is working, where the gaps are and what needs improvement*.
    c. Conducting periodic *focused* reviews of the Strategy's progress and making necessary adjustments.

21. Evaluation measures to support ongoing public transparency and input regarding the implementation of the Strategy should include:

    a. Regular public reporting on the progress of the Strategy's implementation*, the key initiatives and how they are progressing, the results they are delivering and emerging gaps*.
    b. Engaging stakeholders through consultations, workshops, and conferences *to keep all the stakeholders, government and industry in particular across developments informed of what else is needed*.
    c. Encouraging feedback and input from industry, academia, and the public on the Strategy's effectiveness and future direction.