

SMX Email Security Report 2026

DMARC

MTA-STS

TLS-RPT

BIMI



Prepared by
SMX

Coverage
~1,900 FVEY government domains + 6 sectors

Edition
2026

Introduction

SMX has been monitoring the uptake of DMARC in the local Australasian market since 2022.

We've been publishing an annual report tracking the penetration of DMARC – this protocol represents the most important email security upgrade since email was released in the 1980s in the local Australasian market.

Over the five years we've been running this report, we have seen some interesting trends, including a general DMARC uptake increase. We have also seen different deployment models of organisations and how they contrast with industry best practice.

For example, most of the survey results show the Australian sector (including government and ASX-listed companies) as having higher uptake of DMARC than its New Zealand counterpart. This included DMARC in enforcement mode. As a New Zealand-owned email security company, it has been great to see email security improving in this part of the world – an emotion tempered by frustration that we're being beaten by the Aussies, yet again.

This year, we decided to extend the report to include the email security protocol MTA-STS, and its partner TLS-RPT. This follows the decommissioning of the New Zealand government's venerable SEEMail system and the transition to the Secure Government Email (SGE) framework, an open standards-based framework.

The MTA-STS and TLS-RPT combination works in partnership with DMARC and DKIM to provide government-grade email security:

- DMARC stops spoofing by stopping third parties from sending email using your domain.
- DKIM enables legitimate senders to sign their emails with a digital key.
- MTA-STS and TLS-RPT ensure only email sent over TLS-encrypted links are received.

Therefore, with both DMARC and MTA-STS in place, email is protected from domain spoofing (AKA forgery) as well as being intercepted in transit.

Extended analysis to Five Eye partners

New Zealand and Australia are both members of the Five Eyes Security Alliance, so we have also extended the analysis to compare the uptake of these protocols among other partner countries: the UK, Canada and the United States of America. These are added to our usual six sectors:

- New Zealand government
- Australian government
- Top 100 companies in New Zealand
- ASX-listed companies
- SMX's customers
- Organisations sending to SMX

By monitoring those six sectors and Five Eyes governments for DMARC, MTA-STS and TLS-RPT uptake, we can present a much more complete picture of email security. Happy reading!

What are DMARC and MTA-STS and why do they matter?

DMARC is an email security protocol released around 2015, which took a few years to be widely adopted. When properly set up and deployed, DMARC & SPF let a domain owners define which sending sources they'll allow. Add DKIM, and owners can digitally sign their emails, proving they come from an authorised sender.

While DMARC is critical for securing email sent on behalf of an official domain, it doesn't affect the other side of the email pathway, receiving email. MTA-STS completes the loop. MTA-STS requires that emails are sent over a TLS-encrypted link. When correctly deployed and enforced, DMARC and MTA-STS secure emails being sent from and to the domain.

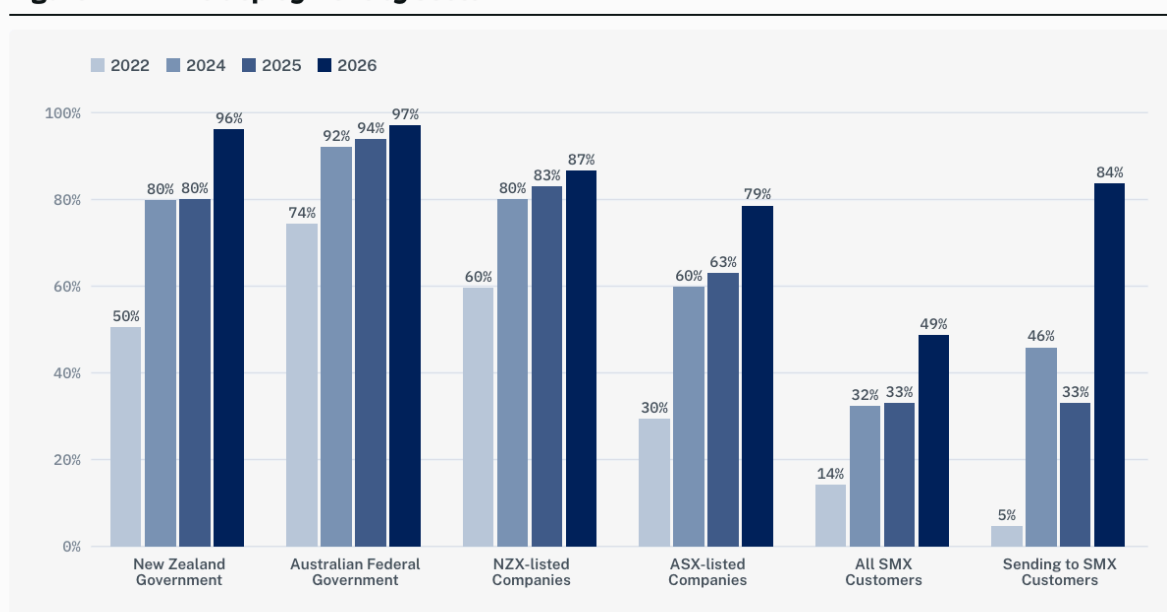
Both protocols are essential security mechanisms for agencies and organisations managing sensitive data. For example, for those core New Zealand government domains with high DMARC and MTA-STS deployment, email between agencies travels over encrypted links, and only authorised senders can send as those domains. This means citizen data stays protected in the cloud era. By contrast, jurisdictions with low DMARC and MTA-STS uptake are putting their citizens' data at risk.

DMARC Report

Adoption rates

When we first ran this survey back in 2022, DMARC was still a fairly obscure protocol, with very low adoption among corporates and government agencies alike. Around 50% of NZ government domains had a DMARC record that year, but actual enforcement was abysmal, sitting at just 21%.

Figure 1 • DMARC deployment by sector

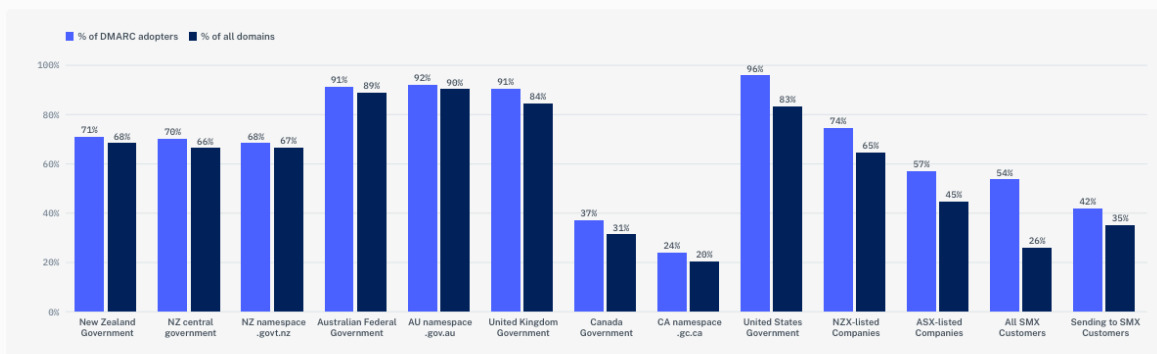


Fast forward to 2026 and the picture's very different, with NZ government enforcement up 3.2x and 68% of agency domains now enforcing who can send email as them. It's great to see our government agencies getting behind the push to secure email in this country.

However, this data shows there is still just under a third of NZ government agency domains not enforcing their email. When compared with our Five Eyes partners, that's still a big gap. The USA leads the way with 81.5% of federal agency domains enforcing email with a DMARC policy of p=reject:

The graph below makes the contrast easy to see. It shows DMARC enforcement levels across all monitored sectors, both as a share of all domains and of domains that publish a DMARC record:

Figure 2b - DMARC enforcement, all thirteen sectors



LOWLIGHTS

Among all the good news stories about DMARC and enforcement stats, there are of course some lowlights. A significant proportion of Canadian central government agencies, 14%, don't have any DMARC records at all. Additionally, the number of USA central govt agencies without any DMARC records is also quite significant, at 12.7% (162).

Table 3b - Policy mix, all thirteen sectors

The 2026 policy mix across all thirteen sectors.

SECTOR	DOMAINS	VALID DMARC % of all domains	P=NONE % of valid DMARC records	P=QUARANTINE % of valid DMARC records	P=REJECT % of valid DMARC records	INVALID % of all domains	NO DMARC % of all domains
New Zealand Government	291	96.2% 280	26.4% 74 of 280	21.4% 60 of 280	52.1% 146 of 280	0.3% 1	3.4% 10
of which central	185	94.6% 175	26.9% 47 of 175	16.6% 29 of 175	56.6% 99 of 175	0.5% 1	4.9% 9
of which in the government namespace .govt.nz - .parliament.nz - .mil.nz	120	97.5% 117	28.2% 33 of 117	11.1% 13 of 117	60.7% 71 of 117	0.8% 1	1.7% 2
Australian Federal Government	180	97.2% 175	8.6% 15 of 175	33.1% 58 of 175	58.3% 102 of 175	0.0% 0	2.8% 5
of which in the government namespace .gov.au	144	97.9% 141	7.8% 11 of 141	31.9% 45 of 141	60.3% 85 of 141	0.0% 0	2.1% 3
United Kingdom Government	194	93.3% 181	5.5% 10 of 181	23.8% 43 of 181	70.7% 128 of 181	0.0% 0	6.7% 13
Canada Government	229	84.7% 194	61.9% 120 of 194	20.6% 40 of 194	17.5% 34 of 194	0.0% 0	15.3% 35
of which in the government namespace .gc.ca - .canada.ca	161	85.7% 138	75.4% 104 of 138	9.4% 13 of 138	15.2% 21 of 138	0.0% 0	14.3% 23
United States Government	1,279	86.9% 1,111	4.1% 45 of 1,111	2.3% 26 of 1,111	93.6% 1,040 of 1,111	0.5% 6	12.7% 162
NZX-listed Companies	127	86.6% 110	24.5% 27 of 110	33.6% 37 of 110	41.8% 46 of 110	0.8% 1	12.6% 16
ASX-listed Companies	1,489	78.6% 1,171	41.9% 491 of 1,171	31.5% 369 of 1,171	26.6% 311 of 1,171	0.3% 5	21.0% 313
All SMX Customers	2,805	48.7% 1,366	43.0% 588 of 1,366	26.8% 366 of 1,366	30.2% 412 of 1,366	0.3% 9	51.0% 1,430
Domains Sending to SMX	49,112	83.7% 41,109	56.4% 23,187 of 41,109	22.1% 9,082 of 41,109	21.5% 8,840 of 41,109	0.7% 362	15.6% 7,641

Almost 13% of USA and 14% of Canadian central govt agencies have no DMARC record at all, let alone one in enforcement mode. (SPOILER ALERT: .ca and .gov domains also score badly for MTA-

STS and TLS enforcement – see below). More than a fifth of ASX-listed companies are in the same boat.

On the positive side, only two NZ central govt agencies have no DMARC at all: the best stat of any sector we surveyed this year.

DMARC REPORTS GOING NOWHERE

This year we've uncovered a couple of interesting stats related to the DMARC reports.

The first is the proportion of organisations, whether they're government agencies or commercial companies, that are self-referential with their RUA (that is, pointing their RUA reports at their own domain).

Potentially more worrying: the proportion of organisations with an RUA reporting address but with a reporting domain that hasn't been authorised by the receiving service. –this is a reasonably common gotcha seen in DMARC misconfigurations and is relatively low in central government, with New Zealand again leading the pack. That said, there is a worrying proportion of self-referential and unauthorised external RUA among surveyed commercial sectors.

For the domains using self-referential RUA (i.e., sending RUA reports to an address within their domain), this usually means the organisation isn't properly set up. They haven't been given budget for a DMARC aggregator service such as Redsift OnDMARC, and so are sending those reports internally. Usually those reports just sit in a mailbox unread, so they never get used to improve the organisation's email security.

Organisations in the reporting-only state (p=none) are unlikely to proceed to enforcement mode. Those in enforcement mode may be unaware of new sending sources (or unauthorised use of existing authorised sources). This is a vector attackers can use to spoof the domain in question.

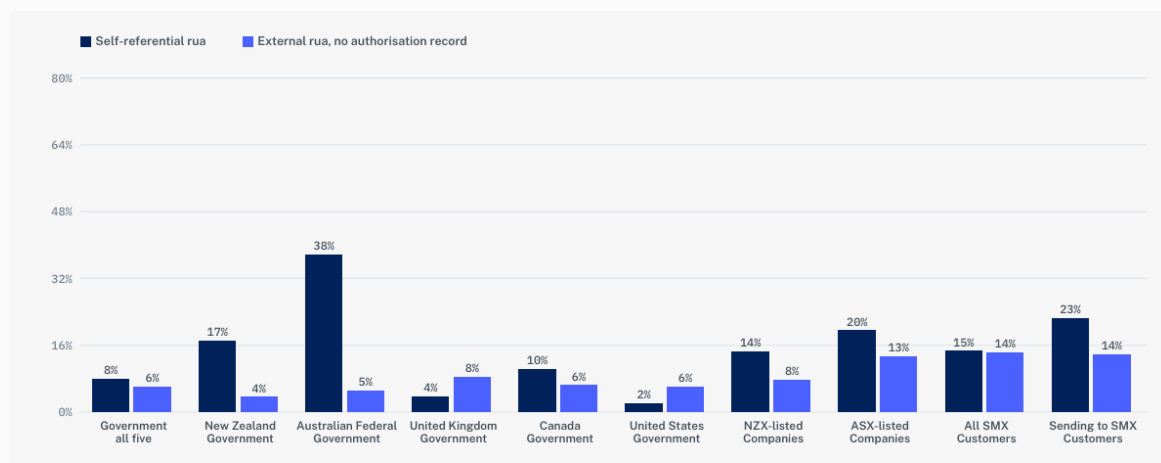
At the more serious end of the DMARC misconfiguration spectrum are external RUAs with no authorisation record. That means those reports are not even being accepted by the domain aggregator (DMARC reports are automatically accepted if the reporting domain is the same as the domain in the RUA address).

Usually, this misconfiguration occurs when a customer hasn't set up their external DMARC report aggregator correctly, so the aggregator is not accepting those reports. The customer is therefore completely unaware that those reports are not being read. The organisation is definitely not looking at the DMARC record reports, otherwise they would notice that the reports weren't arriving. This is probably a double indicator to an attacker that the organisation does not take their email security seriously.

Remember, this is all public information – we can see it and so can the bad guys.

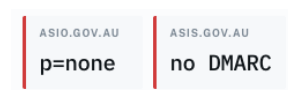
More than a third of Australian federal government agencies are self-referential for DMARC reports. In some commercial sectors, unauthorised RUA records account for up to 14% of companies:

Figure 9 · Where DMARC reports go, and whether they arrive



Aussie intelligence agencies – the exception to the rule

While we congratulate the Australian government on its very good rates of DMARC uptake and enforcement, there are a couple of standout exceptions.



The two primary Australian intelligence agencies are absolutely bucking the trend. While 97.3% of Australian government agencies publish a DMARC record and more than 90% publish an enforcement record, ASIO – the Australian Security Intelligence Organisation – is in reporting mode only (p=None). The Australian Secret Intelligence Service doesn't publish a DMARC record at all. Sure, these two agencies know exactly what they're doing, and they're probably doing it for good reasons, but maintaining p=None and being self-referential does indicate that ASIO is not taking DMARC seriously. The Australian SIS not publishing DMARC at all tells a completely different story. I would note for the record that the New Zealand intelligence agencies' equivalents, GCSB and NZSIS, both have deployed DMARC and are in enforcement mode (p=reject). Just saying, Australia :)

NZ govt leads in BIMi deployment

New to this year's report (the 2026 edition) is BIMi (Brand Indicators for Message Identification).

BIMi lets organisations publish a certified logo (an SVG file) in their DNS, which shows up in the customer's mail app next to the sender name. Only verified marks can do this, indicating to customers that emails are legitimately from that brand.

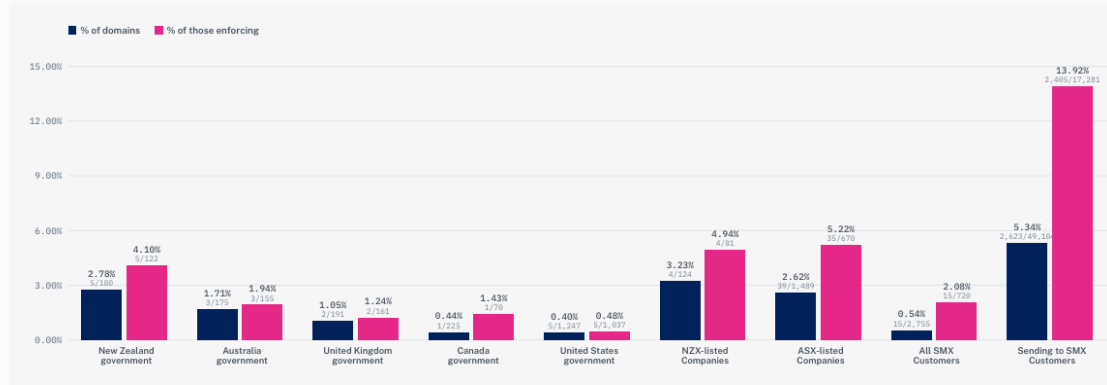
While it's not an email security protocol per se, BIMi is only available to organisations that have DMARC in enforcement mode and a certified trademark. This is verified by a provider into a digital certificate that's then published in the DNS. As a result, when a brand appears in a mail app, it has been certified at each step: domain ownership, trademark ownership and the image.

All of that creates greater trust between the brand owner and the person receiving the email, while building a stronger overall security environment for everyone sending and receiving.

This is the end state every domain owner should be aiming for:

- DMARC in enforcement mode
- MTA-STS ensuring TLS-encrypted links
- BIMI providing brand assurance to email recipients

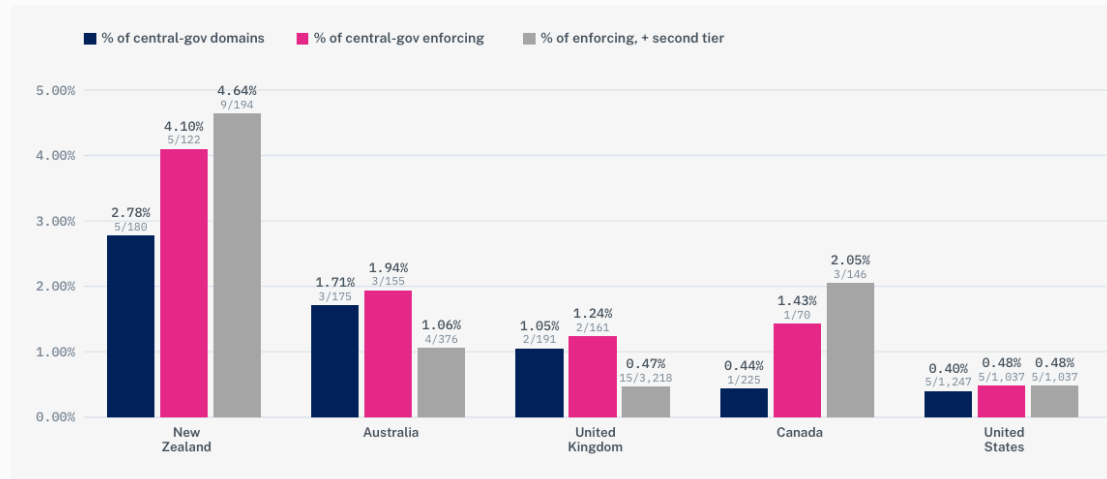
Figure 13b • BIMI, government against commercial



The NZ government is leading BIMI deployment among the Five Eyes governments; 4.1% of those are also enforcing DMARC. BIMI adoption among domains sending to SMX customers is skewed because of the proportion of bulk-sending services that make up this traffic.

The companies and agencies with published BIMI records are consumer-facing and are showing the way for the rest, especially compared to the extremely low number in the other jurisdictions. These domains are exhibiting best-practice email security: everything is secured on the DMARC, TLS and brand sides, with a strong relationship with customers.

Figure 13 • BIMI adoption, government



And again, NZ leads the Five Eyes (FVEY) governments at 4.64%. The other results are pretty dismal by comparison.

NZ shows Five Eyes how it's done

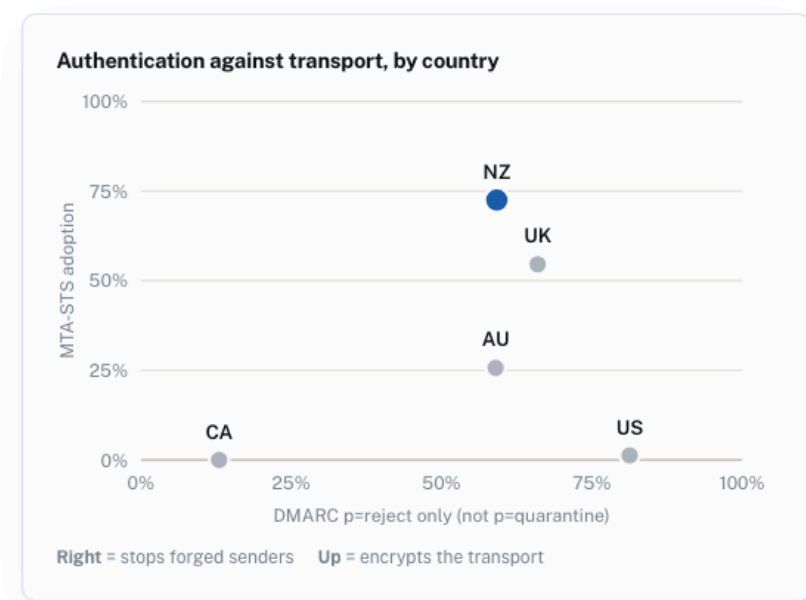
For the first time, we've looked at almost 2,000 FVEY central government agencies for their DMARC and MTA-STS/TLS-RPT configuration, plus BIMBI adoption. Comparing the results across the FVEY governments threw up some interesting numbers.

Email Security Matrix

The matrix we built for this report plots DMARC in enforcement mode (p=reject) on the X-axis against MTA-STS deployment on the Y-axis. The USA is close to 100% on DMARC but practically 0% on MTA-STS: they've solved one part of the puzzle, sending, but have zero protection on the other, receiving.

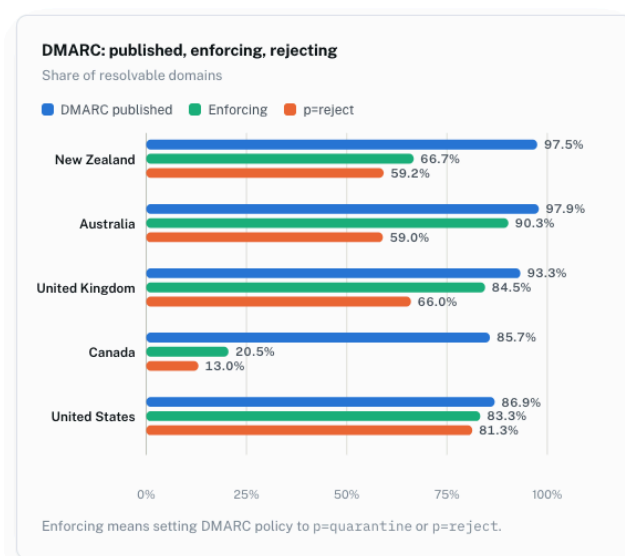
Conversely, little old New Zealand is sitting around 75% for both DMARC and MTA-STS, leading the Five Eyes pack by a considerable margin. This small table really contrasts the difference between how some of the best-resourced countries in the world choose to secure the email their citizens depend on, and New Zealand, with its much more modest government resourcing.

New Zealand's place on the matrix looked very different at the end of last year – a lesson in the importance of a targeted delivery date and a well-managed project in delivering a wholesale upgrade to an entire country's email security.



Authentication

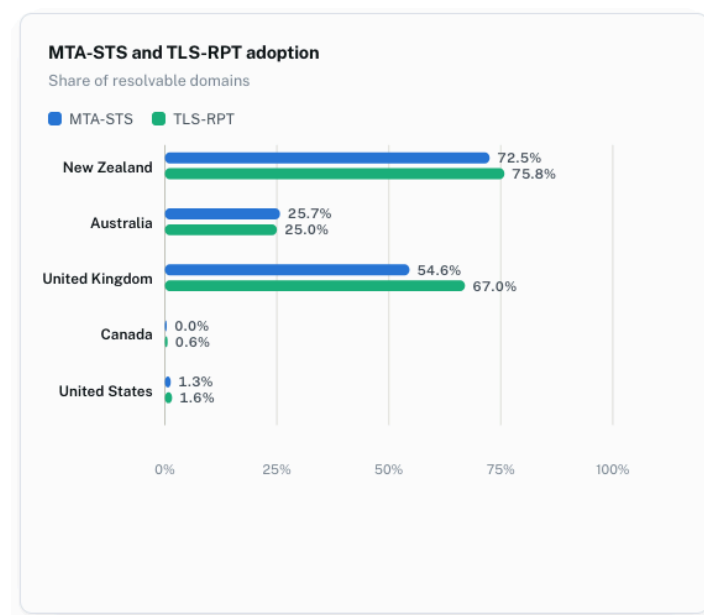
All of the Five Eyes countries have deployed DMARC widely, which is fantastic to see. We certainly didn't think we'd be writing this when we first published this report in 2022. Australasian governments lead the way in DMARC deployment, with less than 0.5% separating Australia and New Zealand. The two largest countries, the United States and Canada, are still in the 80s, which is still an admirable result, but enforcement is where the US is streaking ahead. The USA's mandate to deploy DMARC in enforcement mode has obviously had a big impact, and we can see the same happening in New Zealand. Australia and the UK have increasing numbers of



enforcement, around 60%, but Canada is the standout example, and not in a good way. Its extremely low levels of enforcement aren't much higher than where New Zealand was sitting back in 2022.

Unfortunately, we don't have stats for Canada back then, but I suspect today's numbers represent good progress. Still, 20.5% of government agencies in Canada have DMARC in enforcement mode, which is a disappointing result and puts others in the network at risk.

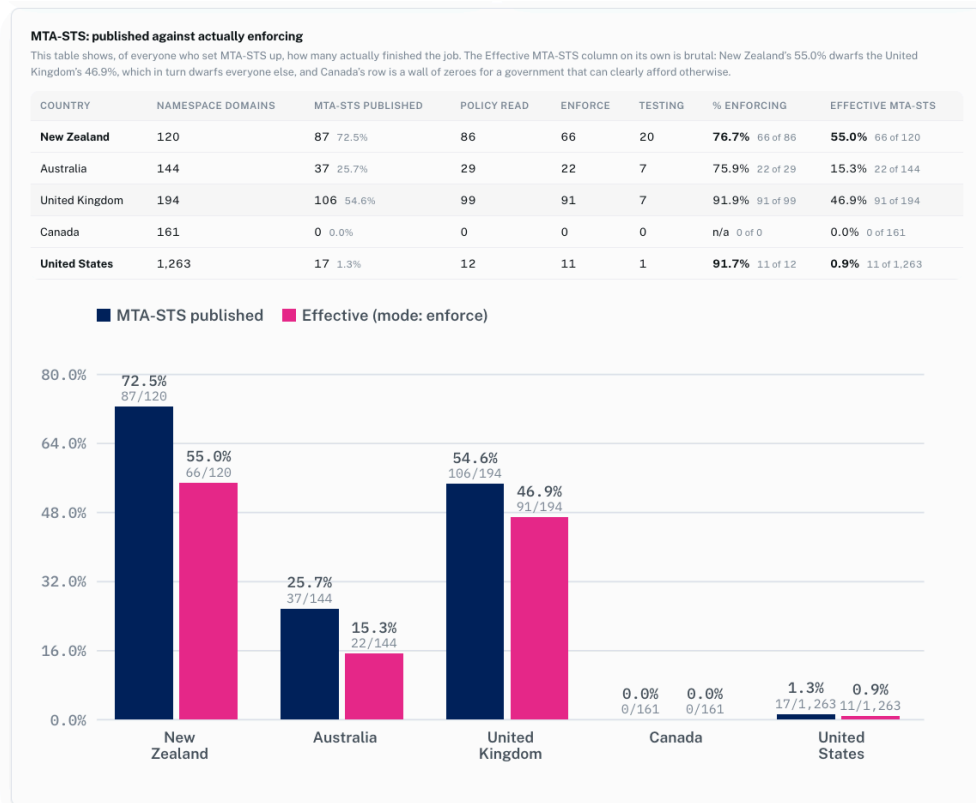
Transport



An interesting stat: the New Zealand government has the highest uptake of MTA-STS and TLS-RPT amongst all of the other Five Eyes countries. As previously mentioned, this is largely due to the Secure Government Email (SGE) framework being rolled out amongst the country's core government agencies. This position is only likely to increase – MTA-STS is now baked into the official recipe for government domains. That will flow through to other organisations like tier 2, local government and state-owned

enterprises and will generally increase the security of the country as a whole. Organisations that communicate with government departments will likely also upgrade their email to match that of their government partners.

It's impressive to see that New Zealand, a country of 5.4 million people and a GDP of US\$280bn, is again streets ahead of larger allies on enforcing MTA-STS – the United States is barely above zero, and Canada is exactly zero.



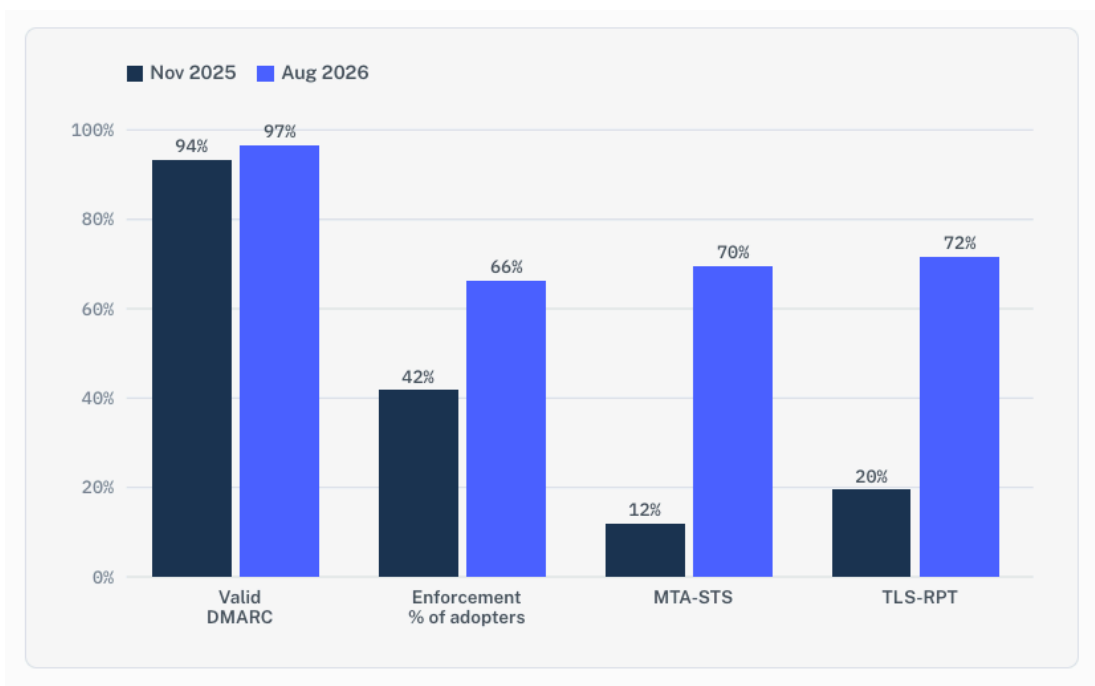
The United States has the highest DMARC enforcement of any FVEY country, but that only secures the sending side. On the receiving side, American citizens emailing their own government agencies have no assurance it will arrive securely. These controls are free to implement, yet neither government shows any sign of resolving half the risk profile of email.

The New Zealand government has shown the way by upgrading its government-grade email security platform to an open standards-based framework. Those same controls are available to all email users around the world. For governments to withhold reciprocal email security when those controls are available for free is a failure to consider their citizens' best interests.

Canada has an abysmally low enforcement rate of 20.5% for outbound email sent through DMARC and is at 0% for enforcing TLS encryption on email sent to government agencies. If this was a school report, they would definitely be getting an “E”.

THE NEW ZEALAND GOVERNMENT EXAMPLE

The replacement for the legacy framework SEEMail in New Zealand, SGE uses open standards to deliver session rather than message encryption for emails. Those open standards are the core protocols we survey in this report: DMARC, MTA-STS and TLS-RPT. It's great to see the New Zealand government embracing open standards to deliver world-class encryption along with world-leading adoption of these standards.



It wasn't always so rosy in NZ government email security. Between November 2025 and August 2026, MTA-STS deployment among NZ government agencies rose massively from 12% to 72.5%. That's the biggest increase we've seen in any monitored sector, driven by the mandate to decommission SEEMail by November 2026. The NZ government is on track for this milestone, and shows how large-scale projects can be delivered quickly and efficiently. This work has resulted in a meaningful increase in the email security of an entire nation. Well done to the Government Digital Delivery Agency and its partners.

The risk of the ever-shrinking pond

Depending on the sector and country, DMARC enforcement at government level runs between 85% and 97%, which is very high. That means, though, that agencies and organisations that haven't deployed DMARC or MTA-STS have become more of a target – they are now the few remaining fish in an ever-shrinking pond. For example, we uncovered the following stats:

- **Domains with no DMARC record:** 10.7% (203 of 1,898) of all FVEY government domains have no DMARC record. This includes the UK's Attorney General's Office (ago.gov.uk) and the AI Safety Institute (aisi.gov.uk).
- **Domains parked at p=none:** Thousands of domains look protected but aren't, because their DMARC records are set to p=none.
- **Subdomains exempted by sp=none:** 38 central government domains publish an enforcing apex policy while explicitly leaving every subdomain unprotected. The UK accounts for 14.
- **Silent domains that still serve a live website:** The working website lends a forged email credibility.
- **Reporting that nobody reads:** A concerning artefact: the number of government domains pointing at aggregators that are unauthorised to do so. 101 out of 1,841 domains, 5.7%, are in this state. New Zealand has five and Australia has seven, but the United States has 69 federal government domains like this. The reporting is literally not being read because the reports are not being sent.

COHORT	VALID DMARC	SELF-REF	OF WHICH P=NONE	UNAUTHORISED	% OF EXTERNAL RUA
Gov, all five	1,836	147 (8.0%)	34	101	6.2%
Gov New Zealand	175	30 (17.1%)	11	5	3.7%
Gov Australia	175	66 (37.7%)	8	5	5.1%
Gov United Kingdom	181	7 (3.9%)	0	14	8.4%
Gov Canada	194	20 (10.3%)	8	11	6.5%
Gov United States	1,111	24 (2.2%)	7	66	6.2%

Link to the Five Eyes report

You can read the full Five Eyes Email Security Report [here](#).

A story of two halves

There is a lot of change happening in our monitored sectors, especially in government, where a relatively small number of agencies are empowered and funded to make significant changes to their email security setup by deploying the latest controls.

That movement is positive – more agencies and organisations are deploying DMARC, MTA-STS and BIML. There are also some clear leaders, with the New Zealand government following mandates to replace the legacy SEEmail product and the UK government having a similar mandate around MTA-STS and DMARC.

There seems to be no similar progress around MTA-STS policy from US or Canadian government agencies.

We first started recording enforced MTA-STS in the New Zealand government in November 2025, when it was measured at 12%. Only nine months later, that number is now 72.5%, an incredible achievement in such a short period. A 2022 prediction that the New Zealand government would be leading the Five Eyes countries for email security by 2026, would have been ROFLMAO-worthy. However, only five years later, that is the reality, with New Zealand again a shining light for other countries to follow.

Upgrades are not the end of it. We live in an era that requires continuous monitoring, with breaches happening within minutes or seconds and mis-configurations being a leading cause of impersonation attacks.

To maintain security compliance, it's critical that organisations deploy managed services to protect and monitor domains and other digital assets. Email continues to be a vital tool for organisations of all sizes, and yet many fail to deploy the protocols to secure their – and their customers' – data. These protocols are free to deploy and make a massive difference to email security – and ensure you're not left behind.

With DMARC now fairly well adopted amongst governments, we encourage corporates and other organisations to follow their lead. Secure email with DMARC, MTA-STS and ideally, BIML as well, to provide complete coverage for your staff and your customer data.

Methodology

To build the survey, we accessed publicly available data in the DNS (the domain name system) and found the list of agency domains from authorised sources. The United States and the UK have very good authoritative sources for government agencies. Australia and New Zealand had relatively good sources. We struggled with the Canadian sources but came up with a good list in the end.

There was no hacking of government sites or data to create this information. Once we'd built the list of domains, we created scripts to analyse the data via both DNS queries and HTTPS queries for the MTA-STS policy files.

Analysis compared data from this to past regional surveys. This year, the MTA-STS survey meant that we were able to provide a bit more perspective, with both sending and receiving email now able to be secured (sending with the likes of DMARC, DKIM and SPF, and receiving with the likes of MTA-STS and TLS-RPT).