



**National Security Agency
Central Security Service**

April 2013

Information Paper

(U) Subject: NSA Intelligence Relationship with New Zealand

(U) Executive Summary

(U//FOUO) NSA's relationship with New Zealand is supportive and cooperative. New Zealand's Government Communications Security Bureau (GCSB) highly values its relationship with NSA/CSS and will continue to seek and support mutually beneficial efforts that demonstrate its commitment to national and international security through its foreign partnerships, in spite of budget and other resource challenges.

(S//REL) GCSB is New Zealand's operational lead on the cyber threat, giving it impetus to be an active participant in the global tipping and cueing architecture as well as resources and capabilities to contribute to Five Eyes efforts. GCSB continues to be especially helpful in its ability to provide NSA ready access to areas and countries that are difficult for the United States to access. Mr. Ian Fletcher, GCSB Director since February 2012, faced his first major challenge when GCSB came under investigation for allegedly exceeding its authority when assisting New Zealand law enforcement. The review that followed made several recommendations, some already underway, to strengthen GCSB's compliance program.

(U) Key Issues

(S//REL) GCSB recently gained agreement to roll out a single TOP SECRET network across the New Zealand government with all agencies' TOP SECRET networks collapsing into a single domain. As part of a strategic decision to collocate intelligence functions, the New Zealand Secret Intelligence Service (NZSIS) will move into the new building recently occupied by GCSB with GCSB providing the infrastructure support.

¹ (S//REL) AFSC - Australia, Belgium, Canada, Denmark, France, Germany, Italy, Netherlands, New Zealand, Norway, Spain, Sweden, United Kingdom, and United States

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20340501



(U) What NSA Provides to Partner

(S//REL) NSA provides raw traffic, processing, and reporting on targets of mutual interest, in addition to technical advice and equipment loans.

(U) What Partner Provides to NSA

(TS//SI//REL) GCSB provides collection on China, Japanese/North Korean/Vietnamese/South American diplomatic communications, South Pacific Island nations, Pakistan, India, Iran, and Antarctica; as well as, French police and nuclear testing activities in New Caledonia. [REDACTED]

(U) Success Stories

(S//SI//REL) [REDACTED]

(S//REL) GCSB is a charter member of SIGINT Seniors Pacific (SSPAC)², a group comprising national SIGINT agency leaders from ten countries with interests in the Pacific Region. GCSB completed its 2-year term as chair of both the SSPAC Executive Board and Analytic Working Group in 2012. During its tenure, GCSB secured active participation in the forum from previously silent partners, garnered unprecedented high levels of participation in analytic synchronization sessions, and secured a relationship between SSPAC and SIGINT Seniors Europe (SSEUR)³.

(U) Problems/Challenges with the Partner

(S//REL) GCSB continues to focus and invest its limited resources on the highest New Zealand national priorities, with the recent compliance review consuming much of its resources and attention over the past six months. GCSB's highest priority, cyber, will be developed to meet the demands of the New Zealand government and Five Eyes partners. NSA will continue to encourage GCSB's efforts towards technical interoperability.

² (S//REL) SSPAC - Australia, Canada, France, India, Korea, New Zealand, Singapore, Thailand, United Kingdom, and United States

³ (S//REL) SSEUR - Australia, Belgium, Canada, Denmark, France, Germany, Italy, Netherlands, New Zealand, Norway, Spain, Sweden, United Kingdom and United States

(U//FOUO) Prepared by:

[REDACTED]

Foreign Affairs Directorate
Country Desk Officer, New Zealand

[REDACTED]

SIGINT Development Forum (SDF) Minutes

Location: NSA-W

Date: 8-9 June 2009

8 June 2009

Developments in SD – NSA ([REDACTED])

5 key imperatives for SSG:

Target trends – to include the percentage of budget which these efforts influence. Effort is linked to the joint SSG/SINIO report on the top 13 technologies, the top 5 are now being broken down into the level of effort being applied, what NSA's capability against them is and the degree of budget investment and impact. NSA are looking to improve their ability to identify new technology trends, the CT product line is already engaged and closely partnering with on this, but SSG is now engaging the wider product centres to seek the top 2 technologies of interest seen in their domains. NSA POC is [REDACTED] [REDACTED]@nsa.ic.gov), Chief Target Technology Trends Center (T3C)

Shaping – in this context NSA means increasing cross access coordination efforts. It was highlighted that the definition of "Shaping" differs amongst the partners (CSEC and GCSB have a narrower definition that is classified at a higher level and focused on activities such as industry engagement and collection bending). NSA is working to increase their focus on router ops, understanding EREPO and increasing CNE survey efforts. NSA POC is [REDACTED] [REDACTED]@nsa.ic.gov)

Pattern of life – increasing NSA capabilities in this realm, working to ensure NSA developments in this realm are not made project dependent (ie. Spread algorithms across tools/accesses). NSA also see PoL having CND applicability. Current focus includes: travel, FTM, alternate ID, SNA and content mining. NSA POC is [REDACTED] [REDACTED]@nsa.ic.gov)

IP geolocation – working to broaden NSA geolocation strategy to cover IP, RF and GSM realms. This imperative has been transitioned out as it's now considered core business, Convergence has taken it's place in the top 5 imperatives. NSA POC is [REDACTED] [REDACTED]@nsa.ic.gov), NAC TD

Convergence – particularly focused on the assessment of Convergence impact upon Sigint and what Sigint should be concerned about. NSA POC is [REDACTED] [REDACTED]@nsa.ic.gov)

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20340601

Human capital – exploring how to train and maintain the NSA analytic workforce, to include the exploration of certification levels and their associated assessment mechanisms. NSA POC is [REDACTED] ([REDACTED]@nsa.ic.gov)

NB: ADD SD reports to NSA leadership quarterly to report on the above and be tasked by leadership.

Other key issues on SSG's radar for the next year:

Privacy issues – (which includes the issue of 2P auditing). [REDACTED] explained that 2 years ago the SID Director expressed concerns over NSA's ability to provide oversight and compliance on Sigint data access. It was determined that the Oversight & Compliance team at NSA was under-resourced and overburdened. As a result, there is increasing effort to scrutinize who, how and why users have access to NSA databases (to include the skill level of analysts who get access). This effort is being worked across S1 and S2, with increasing S3 involvement (as S3 elements do require access to Sigint databases). Mission delegations are being reviewed more closely and NSA have found that these delegations stretch beyond production centers to include the likes of RAD and ADET.

It was flagged by GCSB and DSD that there is no easy equivalent NSA TOPI to sponsor and audit analyst accounts. CSEC indicated they had engaged NSA to discuss the possibility of CSEC funding audit billets. This was initially shot down but has since come back onto CSEC and NSA radars. DSD and GCSB mentioned they are engaging their SUSLOs to explore new alternatives to this issue (eg. Use of spouses or interns). There was some mention of AUS, CAN, GBR and NZL possibly also having to consider implementing "super users", whereby database accounts are limited to a subset of their workforce and those users run queries for their counterparts.

CND – [REDACTED] indicated that this will be a key area of focus and effort for SSG in the coming year, particularly as USCYBERCOM is established. He anticipates there being increasing outreach to key NSA CND elements and stakeholders to see where greater SIGDEV support to CND can be provided.

Developments in SD – GCSB ([REDACTED])

The key areas of SD focus for GCSB are:

Survey analysis and network analysis capability development - GCSB is establishing their first Network Analysis team in October 2009, DSD's [REDACTED] will PCS to GCSB for 2 years to lead this team. The new team will initially be focused on access development and is aimed at proving the utility of Network Analysis such that a push can be made for additional GCSB billets (which can then increase support to STATEROOM and CNE realms)

Continued effort against the South Pacific region - GCSB's access development activities will be focused on the South Pacific region and entail close partnering and

engagement with DSD, NZSIS and ASIS. This is seen as a continuing high priority issue given the increasing rollout of cable in the South Pacific region

SIGINT/IA cyber cooperation - GCSB will be running a one month project in Sept/Oct 2009 involving cooperation and fusing of effort between GCSB SIGINT and GCSB Information Assurance on cyber topics (this effort will include a CSEC TDY). [REDACTED] believes the CND issue may have an added benefit of pushing the priority up on GCSB cable access effort and capabilities

Auditing issue – [REDACTED] indicated that 20% of GCSB's analytic workforce does not have accounts or access to key NSA databases. This is a particularly significant issue for GCSB as they provide NSA with NZL data which they have traditionally accessed via NSA tool/database interfaces (ie. GCSB analysts are unable to query or access NZL data). GCSB are also working to gain connectivity to DSD XKEYSCORE (as a first step towards connecting to other 2P XKs)

(U//FOUO) SUSLOW Monthly Report for March 2013

(U) March highlights:

- (U) Intelligence update:

- [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
- (TS//SI//REL TO USA, FVEY) GCSB has a **WARRIORPRIDE** capability that can collect against an **ASEAN** target. The authorization has expired; GCSB is working to reestablish it. GCSB is also working on the data transfer mechanism from GCSB to NSA.
- (S//SI//REL TO USA, FVEY) Provided input to the GCSB 3-5 year **HF strategy**. The strategy outlines recommended improvements to the Tangimoana station, to include replacing the antenna system and upgrading the collection capability to a wide-band GLAIVE. The proposal should go to the GCSB Board of Directors shortly for final decision.
- (U//FOUO) [REDACTED], **Deputy Director Intelligence**, is on a six month assignment to the Department of Internal Affairs. He doesn't anticipate returning to GCSB. [REDACTED] is Acting DDI until 10 April. A longer term replacement has not been named yet.

- (U) IA/Cyber update:

- (S//REL TO USA, FVEY) GCSB has identified the following 4 **key investment objectives** in response to the **increase of targeted cyber threats** within New Zealand:
 - Make networks and systems less vulnerable to cyber exploitation
 - Improve detection of intrusions that use known tools/techniques
 - Increase discovery of new and previously unknown tools/techniques
 - Actively disrupt the source of intrusions before they cause harm
- (U//FOUO) GCSB participated in a VTC with the **Community Gold Standard** team to discuss the use of the CGS capability areas to support a more holistic approach to network security and assurance. GCSB provided an overview of their risk management/asset management program and the CGS team provided background on CGS and the Manageable Network Plan. They also offered to align the existing GCSB mitigations with NIST 800-53 and then crosswalk these against the CGS capabilities. A follow-up VTC will be scheduled.
- (C//REL) The 23rd **Key Management Strategy Group (KMSG)** event was hosted by GCSB from 19-22 March 2013 and was attended by representatives from each of the FVEYs partners. The NSA team participated via VTC along with the local NSA IA liaison.

Classified By: tfirmin
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20371001

- (U//FOUO) Established an information sharing link between the **DIA's Malware Analysis Team** and FVEYs partners. Responding to positive feedback to a DIA report that was shared with GCSB cyber analysts, DIA agreed to add FVEYs partners to their distribution.

(U) Issues:

(U//FOUO) Three **legislative proposals** are being deliberated in NZ government that will affect GCSB's operations:

1. (S//REL FVEY) Updates to the **GCSB Act** of 2003 to expand GCSG's core functions to include support to external government agencies, and allow for support to the private sector for information assurance and cyber security.
2. (U//FOUO) Strengthened **oversight** from the Inspector General and the Intelligence and Security Committee
3. (U//FOUO) **Network and supply chain security** for NZ government organizations.

(U//FOUO) The internal **compliance review** is complete. The report has been provided to Government. It will be shared with the FVEY partners the week of 8 April and will be made public on 17 April.

(S//REL) The most recent development in the **Dotcom litigation**: the plaintiffs (Dotcom) have agreed to separate the GCSB case from the NZ Police case. NSA general counsel is working with GCSB's chief legal advisor to understand any impact on NSA equities.

(U) **Senior visitors in March:** None

(U) Upcoming senior visitors for April:

- (U//FOUO) ██████████, PTC

(U//FOUO) POC: ██████████, SUSLOW, ██████████ [@nsa.ic.gov](mailto:████████@nsa.ic.gov), ██████████