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]@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]@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]@nsa.ic.gov)

Human capitol – 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)