Post PSN Assurance Process (P2AP) Strawman

Mark Brett mark.brett@nlawarp.net
Programme Director NLAWARP / C-TAG
April 2021 Version 0.5 – Status: DRAFT FOR COMMENT – NOT POLICY

Background

The Local Government Information Assurance regime has its roots in the GSi Code of Connection which goes back over fifteen years. The world has moved on towards using the Internet [1] and the government policy is now Internet First[2], with a move away from the PSN, which is now considered a legacy network.

Traditional ICT is also moving to a cloud first approach [3]. Cyber related assurance is also moving to the Minimum Cyber Security Standard (MCSS) [12] owned by Government Security Group in Cabinet Office[3a] which will replace Local Government Information Assurance for central government departments connected to PSN by April 2023.[11]

At some point in the future PSN will no longer be used, therefore Local Government Information Assurance will no longer exist and the standard for cyber will be the MCSS. In the meantime there are opportunities to prepare the local sector for this eventuality and one such opportunity is to take on responsibility, through a local body, for Local Government Information Assurance whilst the PSN is still operational as a stepping stone for moving towards MCSS

This is a component part of a bigger picture which covers the whole legacy ICT issue, which is being driven by the Cabinet Office for Central Government, that will in due course impact on Local Government. Todays leading edge technology will become tomorrows legacy. We are also now seeing the introduction of both hybrid and multi-cloud technologies and approaches being introduced in organisations. [10]

Issue

The Compliance at present is gained through a code of connection submission, which comprises a network diagram detailing what is in scope, a penetration test, a remedial action plan and a statement of compliance, being a set of assertions, detailing how the Local Government Information Assurance conditions are met through the code of connection. This process is a compliance regime, not an assurance regime.
The current process is still time intensive to administer and is being used by other government bodies, the police and NHS as a level of assurance to facilitate a baseline on which they share information and interact. The current approach is a once a year snapshot, like the MOT on a car. Taxis and other police vehicles have a different regime, which is on-going. Police vehicles are constantly services and reviewed. Police Traffic cars have their speedometers calibrated and are subject to stringent checks[13].

Network and systems assurance is only one component of a wider requirements. There are issues around legacy ICT systems, where the platforms, applications and operating systems are being legacy, (deprecated and going obsolete.) This paper can only focus on this aspect, it is however an integral part of the whole. There needs to be consideration for applications which rely on components that are obsolete, that is no longer supported [5] (old JAVA / FLASH, Internet Explorer etc.).

Councils with legacy equipment are likely to be subjected to more cyber attacks. This increases their need to be even more vigilant in protecting their network boundaries, running their platforms and supporting their applications. Local Authorities are all sovereign democratic entities. Any directed government intervention is termed as a “new burden” [6], there is a mechanism to do it but the cost would need to be picked up by central government. This is further complicated by devolution.

An alternative Local Government Information Assurance process

Background

In an ideal world all PSN connected organisations would have the whole network and infrastructure assured through ISO 27001. This is however very expensive and would not be cost effective, if however Councils have ISO 27001 covering the required scope, that would be acceptable to cover 1 & 3 below, subject to scope.

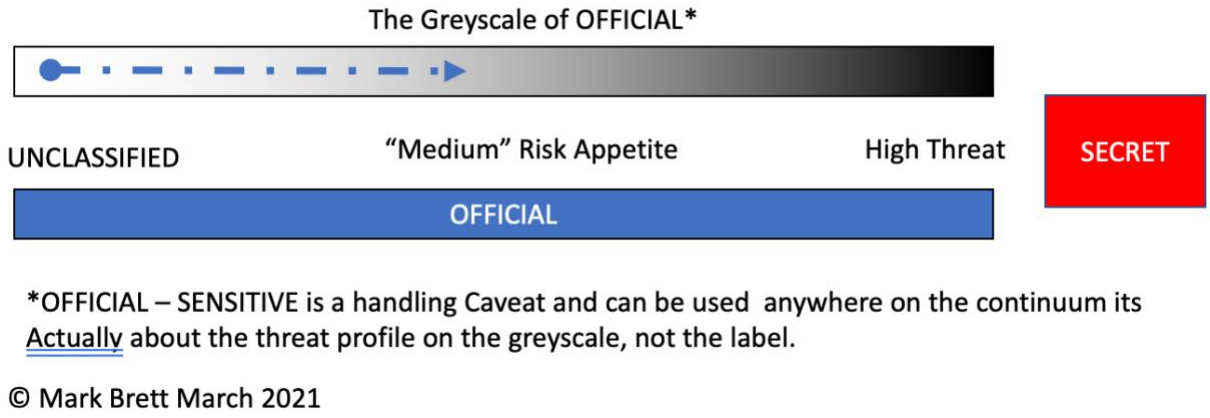
This process below will address the interim requirements as an alternative to PSN code of connection compliance and pave the way to post-PSN assurance supporting the Future Networks for Government (FN4G) Programme. The current Local Government Information Assurance regime is explained at: https://www.gov.uk/guidance/public-services-network-psn-compliance

The PSN network is designed for the OFFICIAL level within the HMG protective marking scheme [9] the threat profile and risk appetite of the PSN is OFFICIAL, using the baseline security controls that reflect commercial good practice. The same applies to the baseline encryption where applicable being commercial good practice.

Currently the PSN relies on an historic penetration testing regime, historically was called an Information Technology Health Check (ITHC), this is an independent penetration test carried out annually. Over the past few years a whole industry has grown up to mechanize and automate this process, using freely available tools and techniques. The NCSC CHECK scheme, when used for this purpose is robust, and fit for purpose, but is also expensive. The monthly scanning requirements will highlight issues in a more effective way than a single annual test. We continue advocate penetration testing for applications and infrastructure as best practice.

Greyscale approach to Threat Profiles at OFFICIAL

All of this approach for use across either just Local Government or the Wider Public Sector (WPS) will be at the OFFICIAL protective marking level. The OFFICIAL level has a grey scale from unclassified white to the more sensitive Black end of the slider within OFFICIAL, often wrongly referred to as OFFICIAL-SENSAITIVE being a separate level “Stripping OFFICIIAL”, that’s not the case. OFFICIAL_SENSITIVE is a handling caveat, not a separate level however there is a need for nomenclature to describe the top end of the OFFICIAL protective marking which is still below the threshold for SECRET. We therefore need to think of the sliding grey scale as a useful analogy.[14] The point being OFFICIAL-SENSATIVE can be used for need to know where the threat profile is towards the unclassified end of the scale, (say a Personnel issue or investigation etc.) not just at the High Treat end. SECRET is a whole different tier. The Problem was caused in 2014, when the Asset Classification Scheme went from six to three levels, loosing CONFIDENTIAL that was used extensively by the Police and others. The move has since been to use “OFFICIAL-SENSITIVE” as a proxy for CONFIDENTIAL, below SECRET.



Suggested approach (Requirements) requiring evidence and assertions

The proposed alternative process will require a number of components which will provide An equivalent to the existing PSN code of connection.

The Post PSN Assurance Process (P2AP) would comprise of:

1) IASME Cyber Essentials Plus as a minimum covering.

1.1 The Corporate ICT Core Network
1.2 The Social Care systems
1.3 The Corporate CRM System
1.4 The Corporate websites
1.5 Corporate email
1.6 remote network access services
1.7 Wireless network access
1.8 BYOD
1.9 Remote (Home) working

2) Adherence to and reporting on the Minimum Cyber Security Standard [8]
3) Adherence to and reporting on NCSC legacy guidelines:
https://www.gov.uk/guidance/managing-legacy-technology
3) Monthly internal vulnerability scans of the core network and servers.
Ensuring core network components are not legacy, especially firewalls.
Scanning all core network devices;
3.1 Firewalls including configuration, patching, whitelists and rulesets.
3.2 Core routers, configurations and patching.
3.3 Ensuring servers are properly managed (if legacy) and patched.
4) Monthly external network scans of websites, services and publicly exposed Endpoints, including API endpoints.
5) Monthly scanning and reporting of;
5.1 All digital certificates in use.
5.2 The DNS servers, services and configurations.
6) Deployment, reporting and active use of NCSC Active Cyber Defense (ACD);
6.1 Webcheck
6.2 Mailcheck
6.3 PDNS (or acceptable alternative if not technically possible).
6.4 NEWS Network Early Warning Service

6.5 Logging Made Easy (or Acceptable alternative)
6.6 Have an NCSC point of contact (POC) email box in place.
6.7 Have an active NCSC CISP account.

7) Have carried out a Cyber Incident exercise within the last twelve months.
8) Have suitable Information Governance, training and awareness regime in place
8.1 SIRO/ IAO / DPO appointed.
8.2 Adherence to the Local Public Services Data Handling Guidelines Version 6.
8.3 Member of Regional WARP.
9) Documented Cyber Incident Response process and plan in place.
10) Key data backup / isolation processes in place.

The proposed process

1) Continue to accept the PSN community documents including the code of connection.
2) Provide evidence of Cyber Essentials Plus.
3) Provide evidence of monthly internal and external scans with an agreed mitigation plan and evidence of improvement against the plan through the monthly scans evidencing the patching and other compensating controls and mitigations are in place and being implemented.
4) Evidenced return against the Minimum Cyber Security Standard.
5) Evidence of information governance regime.
6) Evidence of NCSC ACD take up.
7) Evidence of Cyber exercise.
8) Evidence of key data backup compensating controls.

Supporting future Strategy

This process will encourage a move towards proactive information assurance and cyber resilience. We are encouraging the take up of the NCSC ACD and supporting the minimum cyber security standard. Monthly vulnerability scanning will drive improvement and encourage a robust patching regime. Focusing on the automation of scanning and reporting will eventually get to a point of near real time reporting and posture checking.

Glossary

DWP Department of Work and Pensions
LDS CIC Local Digital Services Community Interest Company
LGD Lead Government Department
ICT Information and Communications Technology
MOU Memorandum of Understanding
New Burdens - Where central government instruct a local authorities to do something and picks up the associated costs for doing it.
NHS National Health Service

References (Accessed February 2021)

[1] https://www.gov.uk/government/speeches/the-future-of-the-internet
[2] https://www.gov.uk/guidance/moving-away-from-legacy-networks
[3] https://www.gov.uk/guidance/use-cloud-first
[3a] https://www.gov.uk/government/publications/the-minimum-cyber-security-standard
[4] https://www.legislation.gov.uk/ukpga/2006/32/notes/data.xht
[5] https://www.gov.uk/guidance/managing-legacy-technology
[6]https://www.gov.uk/government/publications/new-burdens-doctrine-guidance-for-government-departments
[7] https://iasme.co.uk/
[8] https://www.gov.uk/government/publications/the-minimum-cyber-security-standard
[9] https://www.gov.uk/government/publications/government-security-classifications
[10] https://www.packtpub.com/product/multi-cloud-architecture-and-governance/9781800203198
[11] https://technology.blog.gov.uk/2020/09/08/the-road-to-closing-down-the-psn/
[12] https://www.gov.uk/government/publications/the-minimum-cyber-security-standard
[13] https://www.mylondon.news/news/north-london-news/police-speed-vans-need-mot-15916667
[14] https://www.sans.org/reading-room/whitepapers/ActiveDefense/sliding-scale-cyber-security-36240