Chief Executives' Group – North Yorkshire and York

19 June 2014

Public Service Network (PSN)

1 Purpose of the Report

1.1 This report provides an overview on the stricter compliance regime being imposed by the Cabinet Office in relation to connection to the Public Service Network (PSN) for Local Government Authorities.

2 Background

2.1 The PSN provides a secure infrastructure platform to allow connectivity to the central government network. The PSN enables:

- secure access to central government applications and databases
- secure and convenient access to NHS services and applications
- ability to deliver shared services at the local and regional level by enabling multiple public sector organisations to securely access local authority hosted services and applications
- secure email exchange with central government, police, NHS, and other local authorities
- bulk file transfer between local and central government.
- share data securely between public sector agencies, local authorities, central government, police, and the NHS.

2.2 Through its connections to the NHS (N3), PSN significantly helps council service areas that work with the health sector to share information about their customers securely and more efficiently. The network enables local authorities to share citizen data securely with key partners – speeding up processes and helping to deliver joined-up services.

2.3 Secure information sharing with partners, including sensitive and restricted level data is at the heart of effective partnership working. It enables integrated service delivery, centred on the citizen. Information can be captured once and transferred securely and quickly across organisations. This sharing of information and intelligence across the various agencies involved in service delivery provides the basis for place-based service delivery, based on customer needs and planned in a pro-active manner.

2.4 Development of intelligence-led services between partners opens up new opportunities for effective multi-agency working and allows better use of scarce resources and skills to identify and target shared priorities.

2.5 In areas such as trading standards and 'Blue Badges', where services are subject to national rules and usage but are administered locally, PSN enables the sort of real-time, coordinated action that is required for efficient service delivery.

2.6 The PSN delivers the required levels of security and improved speed of access when compared to traditional methods of sharing information, PSN facilitates a simpler transfer of information between councils and partner organisations reducing risk of human error and double handling of data.

3. NYCC PSN configuration

3.1 NYCC has configured their connection to the PSN as part of a segregated network solution. Connection is enabled by use of a client application installed on the workstation and configured to the local profile of the employee who has been authorised to use the PSN. Dedicated servers separated from the corporate network deliver exchange (email), domain controllers (authentication) and file storage. The PSN exchange server is configured with mail filtering software that enables NYCC to instigate local control over PSN emails. All NYCC users of PSN services have a PSN account which is separate to their corporate account.

3.2 The current configuration of the NYCC connection to the PSN has an annual cost to the authority of £21,694.

3.3. NYCC were amongst the first authorities to successfully be certified to the PSN code of connection 2.7 in May 2013 and have successfully recertified to this code of connection in May 2014.

4 Cost Saving

4.1 PSN enables a move away from insecure, costly and inefficient communications to instantaneous, cheaper and secure communications, leading to service improvements and cost savings. The traditional methods of delivering confidential information included use of fax and postal services which, as well as being insecure were also slower, more prone to risk in terms of arriving at the correct destination and more expensive when all costs were considered.

4.2 Although some cost benefits can be realised immediately (replacement of courier, postal and fax costs), it is in fact the increase in operational capability and the mutual confidence leading to improved intelligence sharing and partnership working with other agencies that will deliver major long-term benefits.

4.3 These long term benefits include faster sharing of sensitive information amongst agencies involved in safeguarding children leading to better outcomes for children at risk. The implementation of the 'Tell us once' system has reduced the burden on service recipients and proactively providing information to other services to meet their needs. Connection to the central blue badge system has assisted in reducing misuse of blue badges (which reduces the car parking revenue received by councils). Instant and secure communications between the public sector in emergencies and natural disasters. Reducing avoidable contact through having and sharing 'right first time' data about customers.

5. The way ahead

5.1 The PSN has enabled the council to support our business needs and serve our customers and local communities more effectively and efficiently and assists in continuing to deliver improved services, in local areas, with reduced resources.

5.2 The PSN is of increasing importance as the council seeks to work more closely with partners to tackle more issues affecting its shared customers, whilst reducing operational costs. This includes supporting an aging population and identifying and protecting children and risk.

5.3 The further development of the use of PSN by NYCC will assist in reducing duplication, cutting operational and delivery costs, delivering efficiencies, improving service delivery and facilitating joint working between the districts, other councils,

central government and other public sector agencies. The PSN should be an integral part of any move towards shared service delivery.

5.4 The main barrier to effective information exchange is that staff in general (within all organisations), perceive the Data Protection Act and other governance legislation as barriers to the exchange of information rather than being enablers for the legal exchange of information. To overcome this incorrect perception staff need to be made aware of the legal framework and what it allows (rather than what it prohibits).

5.5 To further reduce costs and to assist the districts with compliance to the strict PSN code of connection the development of an aggregated gateway to PSN services should be explored. The deployment of a local PSN would streamline the connection to the PSN for all the districts and county council. The local PSN would be a managed network based upon Multi-Protocol Layered System (MPLS). Partners would therefore be able to connect into this local PSN via managed connections within a secure virtual private network.

6. Reasons for failure to certify to PSN Code of Connection 2.7

6.1 The PSN has adopted a zero tolerance approach to connections to the secure extranet. Any and all actions identified as not being compliant to the code of connection must be remedied prior to connection being granted. If an authority does not gain certification to the code they will be disconnected from the network.

6.2 The zero tolerance approach was launched by the Cabinet Office on 29 April 2013; however at that time it was unclear exactly what was meant by zero tolerance, what additional security controls would be required and how much these would add to the costs. Since 29 April there have been a number of clarifications and considerable attempts by local authorities to reduce the impact.

6.3 There has been considerable challenge to the way these Zero Tolerance compliance rules have been implemented, and local government networks including the SOCITM, have made a series of representations to the Cabinet Office. Some changes to the timescale and approach to applying this have been offered in response but not to the underlying Zero Tolerance approach. However it is important that where such an approach creates extra cost or other barriers for councils we continue to use our networks to seek further modifications; and these may need to include more representation through Chief Executives and elected Member networks.

6.4 Although zero compliance was flagged back in Apr 13; its implications and additional requirements identifying extra costs have emerged over the months that followed. It is the case that better support and guidance has been issued and some aspects have been clarified which reduces the potential cost.

6.5 The Cabinet Office have re-emphasised that authorities will no longer be allowed to fail and given time to submit and enact a remedial action plan in a letter issued in June 2013 it said “The mandate exists to suspend organisations that fail to reach compliance”. On 4 October they further reviewed this and agreed to allow councils more time to achieve compliance in 2013 only; but that the Zero Tolerance would remain for future code of compliance submissions.

6.6 Some of the recent reasons for authorities failing to gain certification are listed in Appendix 1.

7 Recommendations

7.1 NYCC having been certified to PSN CoCo 2.7 for two years and are willing to assist where possible with knowledge transfer to support colleagues in the district authorities.

7.2. Acknowledge the need and implication of the introduction of mandatory Personal Baseline Security Standard checks for employees accessing PSN hosted systems or PSN originated data with effect from 01 April 2014. For some authorities that do not have a segregated network this brings all employees into scope and there will be a significant cost to comply.

7.3. NYCC are willing to investigate the feasibility of introducing a Common Infrastructure shared by all authorities in North Yorkshire based on the infrastructure that NYCC uses, thereby creating a North Yorkshire Local Public Service Network. This local PSN would provide the connection to the Central Government PSN.

Robert Ling, Assistant Director Technology and Change, North Yorkshire County Council

13th June 2014

Appendix 1

Security Infrastructure

Security infrastructure deployed to support the environment not meeting HMG guidelines This included out of date firewalls, no defense in depth solution in relation to virus detection, malicious code or scripts, out of date risk management matrix's and out of date accreditation documents. Several authorities had not deployed full disc encryption to their mobile devices

Wireless Environment

Non-compliant wireless environment connecting to PSN Services. These included unmanaged devices being used by third parties

Information Assurance

Information assurance not deemed a high priority. No protective marking or protective monitoring in place.

Single Point of Failure

Skills required to manage the environment were with key individuals who carried most of the knowledge around in their heads (e.g. not documented). This became a single point of failure. Additionally when key individuals were sick, on courses or annual leave, the skills within the rest of the team were not to a standard; each time they had an issue (irrespective of how small it was) it took hours to resolve

Non-compliant remote access solution

Remote access solution not fulfilling the requirements as detailed in CESG GPG 10 – Remote Working or CESG Architectural Pattern 2 - Walled Gardens for Remote Access. Additionally no thought had been given to addressing the issue of encrypting "data-at-rest" on laptops.

Non Compliance to BPSS (BASELINE PERSONNEL SECURITY STANDARD)

Employees not undertaking pre-employment checks or induction training

Port blocking of USB devices not enabled or monitored

ITHC not scoped correctly

The ITHC submitted only covered external penetration testing. The PSN requires a full IT Health Check covering internal and external vulnerability testing including servers, desktop and laptop equipment and mobile and remote access devices that consume PSN Services.