PSN Compliance

Case Study: PSN Compliance

CNS have helped a number of Public Sector Customers who required assistance in adhering to PSN compliance requirements.

PSN Public Services Network

These below examples demonstrate the ability and in-depth experience CNS maintains in the understanding and interpretation of Government requirements/standards into practical solutions with a technical and procedural basis. CNS have conducted a number of PSN CoCo's and have also been heavily involved in getting Public Sector organisations "out of trouble" when they have either failed compliance or when they need to turn to a company to seek advice about solutions that have been deployed. CNS are independent advisors in such matters.

London Borough Council

Non-compliant remote access solution

Issues: The council were looking to deploy a remote access solution but had not considered 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.

CNS were called in to conduct an HMG IS1 Risk Assessment. Additionally we conducted a gap analysis utilising the baseline control sets (BCS) as dictated in HMG IS1 Part 2 to understand what the technical and procedural gaps were. We then created a risk treatment plan to address all issues. Our job then was to consult on what they could do to ensure compliance without spending the councils money (money which they did not have). A good example of the monies saved came from the fact that the incumbent 3rd party who provided the contract was attempting to sell the council FIPS140/2 (US Government encryption standard) accredited SSL VPN gateways. The costs of these versus the standard devices was some £70K difference.

CNS provided guidance around their requirements and instead of spending the £70K advised the council to author some sensible but stringent policies and tighten the physical security of the data centre. CNS CLAS and technical consultants then met with the SIRO explained our actions and justifications and once understood they were happy to sign off the risk.

Royal Borough Council

Failed their PSN Code-of-Connection

Issues: The PGA (Pan Government Accreditor) failed them on their PSN CoCo due to a number of reasons. Information assurance was not deemed a high priority within the council and they had not introduced any type of protective marking or protective monitoring.

CNS advised on a methodological approach which resulted in us consulting on a new infrastructure that meant they did not have to spend an absolute fortune to remediate (such as deploying OS hardening via GPO's, re-drafting policies and disseminating them correctly to their staff). CNS then consulted around them deploying a working protective monitoring solution that fit in with their needs (e.g. met the PMC's as detailed in CESG GPG 13). This included providing them with a security taxonomy and realistic incident handling procedures.

Government Department

Non-compliant wireless environment and not deployed to offer true innovation

Issues: The Government agency had been sold a wireless solution from their 3rd party incumbents who managed their infrastructure. They have been told that they had the right experience and knowledge to deploy wireless for Government use. It transpired that they had never actually deployed one (which at the time had to be deployed in accordance with CESG Manual Y but has now been superseded in accordance with CESG Architectural Pattern No. 12 – Wireless Networking). They had also purchased a number of costly devices and applications that were not required to be deployed.

CNS re-designed the infrastructure to meet CESG Manual Y (and then CESG AP 12). We removed all irrelevant devices and integrated it with their existing infrastructure. This not only meant the management overhead was drastically reduced but also significantly cut support and maintenance costs.

We were also able to deploy it in a number of ways that mean that it could be used across the entire region. This also reduced the costs of 3G and 4G transmissions from vehicles as well. It also gave the Agency the ability to provide data and voice signals where typically there were none.

UK Police Force

Non-compliant infrastructure that was based around non-commercial (open source) or not "main stream" technologies.

Issues: 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. This effected daily Police operations and was deemed unacceptable.

Additionally the security infrastructure deployed to support this environment did not meet HMG guidelines (such as non CESG CPA encryption, EAL4 firewalls, no "defence-in-depth") and their RMADS was woefully out of date.

CNS were called in to initially audit the Force's compliance status. This produced a report that provided some evidence as to the critical state they were in. This resulted in CNS being seconded to site for a year and a half to manage the department as a whole. In that time the CNS consultant managed to resolve all issues and ensure compliance with their CJX CoCo. This included updating all their policies, upgrading the infrastructure in line budget, implementing proper incident handling and staff rotas and provided a compliant remote access solution that enhanced their security perimeter. The CNS consultant also designed and deployed their IL4 (CONFIDENTIAL) infrastructure. They were the first Police Force to be signed off as compliant with the national PND (Police National Database) environment. We also only used around 70% of the budget assigned to the project.