Cyber Security Requirements – Requests for identifiable or re-identifiable NDIA data

This document is referenced at Section 6.3 of the 'External Research Request Form for identifiable or re-identifiable data and other requests'.

These are the **minimum** Cyber Security Requirements for the storage and handling of identifiable or re-identifiable NDIA data:

1. All data is to be encrypted at rest and in transit, including transit between systems to the minimum level shown below:
   a. NDIA Cyber Security endorsed algorithms for encryption session key exchange shall meet one of the following criteria:
      - Use the ECDH algorithm with a key size of 256 bits or higher in the ephemeral variant, and where selectable, use a FIPS186-4 conformant curve, or
      - Use the DH algorithm with a modulus of at least 2048 bits, in the ephemeral variant.

   b. NDIA Cyber Security endorsed algorithms for digital signatures shall meet one of the following criteria:
      - Use the ECDSA algorithm with a key size of at least 256 bits and, where selectable, use a FIPS 186-4 conformant curve, or
      - Use the DSA algorithm with a modulus of at least 2048 bits.

   c. The NDIA Cyber endorsed hashing algorithm is Secure Hashing Algorithm 2 (SHA-2). Specifically, for NDIA solutions, the SHA-256 variant is the minimum acceptable requirement.

   d. For NDIA systems, the approved symmetric encryption algorithm is Advanced Encryption Standard (AES) using a cipher key length of at least 256 bits.

   e. Digital Signature algorithm is ECDSA, specifically NIST P-384

   f. TLS cipher suites (TLS 1.2 or better) shall meet the following:
      - An AES symmetric cipher of 256 bits in length shall be used, in Galois Counter Mode (GCM) where available.
      - ECDH or DH shall be used for session key exchange, in the ephemeral variant for forward secrecy. ECDH is preferred over DH.
      - Anonymous DH shall NOT be used.
      - The Message Authentication Code shall use a SHA-2 algorithm of at least 256 or 384 bits in length.

2. Access to NDIA identifiable data **must** be restricted to staff with a defined "need to know". All access to the also needs to be logged and audited. These logs **must** be protected and stored separately and be available to NDIA on request.
3. All NDIA identifiable data and data that may be re-identified **must** be stored within Australia. No NDIA identifiable data is to be stored or accessed from offshore. This applies to all backups, archives and copies.

4. The receiver of NDIA identifiable data **must** have an approved and tested Cyber Incident Management process.
5. The receiver of NDIA identifiable data **must** agree to tell NDIA at cyberops@ndis.gov.au if they become aware of a compromise to their systems or NDIA data. NDIA Cyber will tell the receiver if they become aware of a data compromise through our monitoring tools.
6. The receiver of NDIA identifiable data **must** provide a copy of their cyber security plan for the processing and handling of NDIA data in their systems and services.
7. The receiver of NDIA identifiable data **must** certify that systems storing and processing NDIA data are operating at N[1] or N-1 and that the organisation has a process to maintain N or N-1.
8. The receiver of NDIA identifiable data **must** have a Vulnerability Management Plan for the systems storing and processing NDIA identifiable data.
9. NDIA **must** be provided certification of the destruction of NDIA data to cyberops@ndis.gov.au. Destruction must meet the standards in the Australian Government Information Security Manual - Guidelines for Media.

[1] Current Version of Software