Ministry of Defence

JSP 886
THE DEFENCE LOGISTICS SUPPORT CHAIN MANUAL

VOLUME 3
SUPPLY CHAIN MANAGEMENT

PART 11
LOGISTIC INFORMATION SYSTEMS DATA MANAGEMENT

THE MASTER VERSION OF JSP 886 IS PUBLISHED ON THE DEFENCE INTRANET.

FOR TECHNICAL REASONS, EXTERNAL LINKS ON THIS INTERNET VERSION HAVE BEEN REMOVED.

VERSION RECORD		
Version Number	**Version Date**	**Version Description**
1.0	11 Feb 09	First Publication
1.1	11 Dec 09	Changes to Ownership and Points of Contact
1.2	28 Nov 12	Re-format of Document.

TABLE OF CONTENTS

CHAPTER 1: INTRODUCTION

PURPOSE

1. The purpose of this instruction is to outline the policy for the management of Support Chain Data. This will include data supporting logistics processes and those used on Logistic Information Systems (Log IS). This is to ensure that only permissible data definitions are used and that data values and fields are correctly harmonised.

2. The requirement for correct Data Management in support of common processes is particularly relevant with the rollout of the Tri-Service change projects such as Management of the Joint Deployed Inventory (MJDI), Management of Materiel in Transit (MMiT) and Modernisation of Base Inventory System (MBIS).

OWNERSHIP AND POINT OF CONTACT

3. The policy, processes and procedures described in the Defence Logistics Support Chain Manual (JSP 886) is owned by Director Joint Support Chain (D-JSC). Head Supply Chain Management (SCM-Hd) is responsible for the management of JSC policy on behalf of D JSC.

4. This instruction is sponsored by DE&S LogNEC who should be approached in case of technical enquiries about the content:

DESLogNECProg-DataCoe-DMT2a@mod.uk
Tel: Civ: 01264 381840, Mil: 94391 7840

5. Enquiries concerning the accessibility and presentation of this instruction should be addressed to:

DESSCM-PolComp-JSP886@mod.uk
Tel: Mil: 9679 80953. Civ: 03067 980953

THE GLOSSARY

6. Specific business terms used in this document are declared either as a footnote and / or in JSP 886 Volume 1 Part 1a.

LINKED PUBLICATIONS

7. The following publications are linked to this instruction:

a. JSP 329 - Information Coherence for Defence.

b. JSP 602 - Mandated Communication Information Systems Interoperabilty Policy - Directions and Guidance.

c. JSP 886 Volume 2 Part 4 - NATO Codification in the UK.

d. JSP 886 Volume 3 Part 1 – The Standard Priority System.

e. JSP 886 Volume 30 – Logistic Information Systems User Guides and Operator Manuals.

f. Controlled Values Repository (CVR).[1]

[1] CVR was formerly known as the Defence Data Repository

CHAPTER 2: DATA MANAGEMENT

BACKGROUND

1. The requirement for a single and clear approach to the management of logistics data resulted from the convergence of legacy single-Service Logistics policy into Joint Defence Support Chain policy. The new converged Logistics policy specifically supports single sets of Log IS processes which are required to enable tri-Service applications, such as MJDI and MBIS, to be implemented across Defence. This means that the definition of data and the permissible values and fields to support the data must be coordinated across Defence to achieve this single approach.

2. Consequently there is a requirement to identify all data fields used by the full array of Log IS and the values that can be used in each of these data fields. The process requires the identification of the owners of each data value, harmonisation of the data fields and values across interfacing Log IS and supported by a single set of definitions. This will aid the accurate creation and management of items on the systems by allowing all stakeholders, including Industry, to work to a coherent set of data.

SCOPE

3. **Policy.** This policy is applicable across the Defence Support Chain. It applies to those data elements originating within Log IS, which will include:

   a. Base Inventory / Warehouses Systems.

   b. Deployed Inventory Systems.

   c. Commodity Supply Systems.

   d. Consignment Tracking (CT) Systems.

   e. Engineering and Asset Management (E&MA) Systems.

   f. Interfaces to other Capability area systems, such as those used in Finance, Commercial areas and Industrial Partners[2].

4. **Instruction.** This instruction sets out the higher level policy only. It does not contain detail of individual data elements, which are contained in the Controlled Values Repository (CVR) and other documents.

DATA POLICY FRAMEWORK

5. **General.** The Sponsor of Support Chain Data Management policy is ACDS Log Ops, AD Def Log Pol. However, responsibility for the implementation and execution of this policy is delegated to DSCS. Detailed management is exercised through the Data Quality Working Group (DQWG) (see Chapter 3).

6. **Framework.** The framework of Defence Logistics Data policy is owned by ACDS Log Ops, AD Def Log Pol. The Data Policy Framework provides the basis for exerting governance for:

[2] This policy applies to Industrial Partners operating Contractor Logistic Support (CLS) arrangements in support of IPTs.

a. Data Standards.

b. Data Architecture.

c. Policy and Processes.

7. **Data Standards.** The required standards to be applied to data and the use of data are:

a. **Definitions and Taxonomies.** Definitions and Taxonomies provide a common and consistent way for organisations to share data through a common understanding of the meaning of data, structure, its usage and a way of avoiding its duplication.

b. **Master and Reference Data.** Master Data is the core element which is associated with the business. Reference Data is the data which is held to categorise other data.

c. **Exchange Standards.** Exchange Standards are used for exchanging and carrying data between systems sharing that data.

8. **Data Architecture.** Data Architecture provides definition and construct. To be effective the following should apply:

a. **Enterprise Data Model.** Enterprise Data Model is a data architectural model used to aid integration by giving a single view of integrated data across the enterprise. It is a framework which supports planning, building and implementation of data systems.

b. **Configuration.** Data configuration needs to be measured against an Enterprise Data Model. There then needs to be a change management process in place to ensure the data configuration is maintained. This process needs to be cognisant of all types of data and should include:

(1) Reference Data.

(2) Master Data.

(3) Metadata[3].

9. **Policy and Process.** Defining the rules for data management will include:

a. **Business Rules.** The business rules that are identified, documented and managed for data structure and data management.

b. **Performance Management.** The agreed performance criteria that the data should be measured against, these should cover data attributes such as accuracy, timeliness, security, accessibility and consistency.

c. **Access.** Access to data is critical to data management. This must include:

(1) Those who have permission to access the data.

(2) Those who have authority to create, update and delete the data.

[3] Metadata is other data and information that supports the main data.

10. **Execution.** Execution of the framework includes:

a. **Roles and Responsibilities.** What each Business Area is allowed to do and what they are prevented from doing with regard to the data must be defined. This will include the roles and responsibilities of the:

(1) **Data Owner.** The Data Owner is the specific Business Area that has overall responsibility for ensuring that the data, its definition and values are correct.

(2) **Data User.** The Data User is the Business Area or system that utilises the data for its role.

(3) **Data Custodian.** The Data Custodian is the repository holding the definition and values of the data. Ultimately this will be the CVR.

(4) **Data Steward.** The Data Steward is the body that ensures that coherent and consistent data is applied across the Support Chain. This function is carried by the DQWG.

b. **Training and Education.** Training and Education implications involve the determining the skill set required for each of the roles described above and the following:

(1) Provision of training packages required to provide the necessary skills.

(2) Training packages for both generic and specific applications.

11. **Coherent and Consistent Data.** All of the above elements lead to a coherent and consistent set of data which allows:

a. **Interoperability.** The ability to access data regardless of source or structure.

b. **Availability.** That the right data is available to those who need it at the right time.

c. **Quality.** Data that meets the requirement of the user.

d. **Security.** Ensures the secure storage and authorised use of data.

e. **Compliance.** Ensure the provenance and historical trail of data adhere to internal and external policies and legislation.

CHAPTER 3: SUPPORT CHAIN DATA

1. **General.** Support Chain Data is to be managed based on the policy, framework and guidelines set out in Chapter 2 above. The aim is to provide all Data Users with a single reference, in a database or in a document which will provide accessible information for the Data. For the purposes of this policy, 'Data' can be described as a single piece of information with an agreed set of values associated with it. These values give the user flexibility to apply the appropriate requirement to meet the business management needs.

2. **Ownership of Data.** For each piece of data there will be a designated Data Owner. The Data Owner is responsible for:

a. Ensuring there is a process for the management of the Data. This includes the methodology for creating, amending and deleting the values and notifying Stakeholders.

b. Ensuring the Data is current and correctly defined, with its values, using the approved common language.

c. Ensuring the Data is held, with the correct values, on Log IS applications.

d. Progressing further requirements and implementing necessary changes to the Data.

e. Reviewing existing values and/or adding or deleting values for the Data.

f. Assessing the impact of proposed changes on Log IS applications and stakeholders business.

g. Ensuring that the necessary requirements for change are passed to the Future Logistics Information Systems (FLIS) organisation so that the correct changes can be made to the Data on the appropriate Log IS applications.

h. Ensuring that changes are promulgated to all stakeholders and policy documents are amended.

i. Providing the interfaces for all stakeholders for issues relating to the Data.

j. Ensuring the Data is current and properly stored in the appropriate Data Repository by the Data Custodian.

k. Ensuring all stakeholders understand the Business Context and Log IS functionality linked to the Data.

3. **Data Standards.** The corporate policy on Reference Data is set out in JSP 329 Chapter 3. The set of values associated with a piece of Data are to be agreed by the relevant stakeholders. In the Logistics environment the following additional aspects are required:

a. **Legal or Health and Safety.** The source of this data is often in legislation and therefore mandatory, so it is imperative that it is properly managed, understood and complied with. An example of this category of data is UN Hazardous and Department for Business, Enterprise and Regulatory Reform classifications and codes.

b. **NATO Standard.** This includes STANAGs and other Treaty obligations. An example of this category of data is the NATO Codification System (JSP 886 Volume 2 Part 4).

c. **Specialist Areas.** Special areas of subject matter expertise often have their own data elements. These areas are often covered by DEFSTANs. An example of this category of data is Stores Packaging codes.

d. **Business Led.** Data elements that stem from business led policy requirements owe their authority to that policy. An example of this category of data is the Standard Priority System (SPS) (JSP 886 Volume 3 Part 1).

e. **Additional Logistics Data.** This is the lowest level of data and is to enable a specific business process to operate on an individual Log IS application for a special purpose. Therefore, one-off special data elements may be built into specific IS transactions as part of overall system functionality once agreed by the Data Quality Working Group (DQWG). These data elements must be clearly defined and must not conflict or be confused with other data elements. In addition, where appropriate they must be harmonised if other systems require using them downstream. An example of this category of data is the individual Log IS Data Repositories, such as the Stores System 3 (SS3) Data Code Book (access through the 'DSG Land Supply Telford web page; follow 'Trove Documentation Web' on the left hand column of this web page).

4. **Data Values.** The requirement for any number of data values to support the overall data definition will depend on the complexity of the process the data is to support. However, all of the subsequent values used must have agreed definitions, which support the business processes used throughout the Support Chain. It is imperative that these values are current, relevant, correctly applied and understood. Data Owners must ensure that data values are managed in accordance with Paragraph 2 above.

5. **Data Repositories.** The Data is to be named and defined by the Data Owner and must have a single and specific meaning as agreed by the DQWG. The Controlled Values Repository (CVR) is the corporate data repository. All other authoritative Business Area repositories that exist (as detailed in the supporting documents) are to be included and referenced out from the CVR. The Data Custodian for the CVR will maintain the system in accordance with the service level agreement between AD Def Log Info and Information Coherence Authority for Defence (ICAD) on behalf of the Logistics community. Defining data elements to meet business needs remains an evolving process and there will always be a number of individual pieces of data that are not registered. It is the responsibility of each project or manager of the system requiring a new or changed data element to apply to the Data Owner for these new data elements to be included in the Data Repository. The process for this can be found in JSP 329 or by contacting ICAD Help Desk.

6. **Data Users.** The Data User is the Business Area or system that utilises the data for its role. This may include the capability to apply data values to Log IS, via an approved application transaction, to the standard as laid down by the Data Owner. For example, the amendment of data tables where the User has permission. It is the Data Users responsibility to:

a. Apply the accurate data value for the individual transaction.

b. Ensure this value is maintained accurately.

c. Fully understand the utilisation of any data and its effect on functionality within the particular Log IS application.

d. Where the Data is not meeting the Users requirements, to apply to the Data Owner for changes to the data, setting out clearly the requirement.

7. **Data Steward.** The Data Steward is the body that ensures that coherent and consistent data is applied across the Support Chain. This function is carried by the DQWG. Terms of Reference (TOR) for the DQWG are at Annex A.

ANNEX A: TERMS OF REFERENCE (TOR) FOR THE DATA QUALITY WORKING GROUP

(Introduced at Paragraph 7)

1. **Purpose.** The Data Quality Working Group (DQWG) is to ensure coherent and consistent Data is applied across the Support Chain.

2. **Tasks.** The tasks of the DQWG are to:

a. Ensure every data element used within the Support Chain has a Data Owner. Where no owner exists, to identify the appropriate owner.

b. Identify areas where there are data quality problems.

c. Create a work plan for addressing identified data quality problems.

d. Ensure action is taken to resolve data quality problems. This includes:

(1) Stakeholder approval.

(2) Funding.

(3) Log IS application changes.

(4) Policy dissemination.

e. Ensure data definitions are properly articulated and disseminated.

f. Ensure this JSP 886 instruction remains correct and current.

3. **Members.** A list of the members of the DQWG is at Table 1 below:

Figure 1: List of DQWG Members.

Serial	Core Members (At Working Level)	Consulted
1	ACDS Log Ops – Chairman	SCS (MFPT)
2	SCS (Pol) Dev	DSG
3	SCS (Progs) Data Mgt	FLIS
4	SCS (Inv Opt) – 3 areas	DSDA
5	SCS (IM)	FLCs
6	SCS (PS) – 3 Environment and UKNCB	Other SMEs[4]
7	SCS (Pol) –Secretary.	

4. **Reporting.** Business level reporting is to the Joint Supply Chain Committee (JSCC). Escalation of issues and data conflicts is through ACDS Log Ops.

2. **Working Practices.** Meetings will be held regularly.

[4] This will include consultation with DE&S Chief Operating Officer (COO) and Chief of Materiel (Sea, Land and Air) if appropriate.