History of the DoDAAD

In 1949, Congress passed the Federal Property and Administrative Services Act which, among other things, created the General Services Administration (GSA) and established the National Supply System of the Federal Government and directed the mutually supporting roles of the GSA and the DoD for maintaining and facilitating the System. Part of the DoD responsibility for this effort included providing standardization and cataloging of Supply information. The requirement for standardization is what ultimately led to the development of such things as the National Stock Number (NSN) and eventually, the Military Standard (MILS) methodology for standardization in business transactions.

Prior to 1960, and before the advent of Information Technology, the identification of activities relied upon manually-maintained five-digit codes called Unit Identification Codes (UIC). There was no central repository for these codes, and there was no way to differentiate them from one DoD Component to another. With the advent of information technology, and with the requirement for standardization, the ability to accommodate interoperability requirements in a joint environment was possible by the introduction of a sixth digit added to the front of a 5-character UIC that identified the Service to whom the UIC belonged. This Service Code coincided with the advent of the Military Standard (MILS) information technology implementation (i.e., MILSTRIP/TRAP/BILLS/TAMP/CAP) of the 1960s, and the birth of the DoDAAC as the six-character code that identified an activity across the DoD Supply Chain enterprise. While many people continue to refer to it as a UIC, the DoDAAC is now the DoD business system standard for identifying an activity, and this same code was also used by the GSA for its supply chain system needs.

From its birth in the early 1960s, the DoDAAF (as it was originally called) was a mainframe-based flat file directory of addresses for activities, which could be printed out for end users but in very large and unmanageable computer printouts. It was maintained through a network of users who would submit MILS TA_ transactions to the Defense Automatic Addressing System (DAAS) in order to keep addressing information current. These transactions were originally keypunched on hard punch cards at local communications centers. With advances in information technology, the DoDAAF was eventually re-engineered in 2005 into its current form, as an interactive, relational database with unlimited potential for further modernization to meet ever increasing IT demands. It is now maintained by a series of Central Service Points who are responsible for real-time updating of the database on behalf of their respective Components and Agencies.

While the DoDAAD was originally conceived to facilitate supply chain business system processes, today, the DoDAAC is used by nearly every functional domain of the DoD Business Enterprise Architecture and expanding uses by the Federal Government.

The DoDAAD is administered by the Defense Logistics Management Standards Office of the Defense Logistics Agency, on behalf of the DoD. From a policy perspective, the Under Secretary of Defense for Acquisition, Technology, and Logistics is the sponsor of the DoDAAD, and through the longstanding Agreement with GSA, the DoD maintains Federal Agency equities of the DoDAAD as well.

The UIC still exists today, but it too is now a six-character code created by the DoD Components to identify an activity in manpower and readiness reporting systems. Prior to the advent of the DoDAAC, the UIC was a five-digit code used for financial resources, readiness, and manpower. When the DoDAAC was conceived, the use of the UIC also changed to a 6-character construct, but its use and maintenance was kept separate from that of the DoDAAC (in the DoDAAD). In spite of the 6-character

UIC's continued use, certain Services and systems maintained use of the 5-character construct (Navy), while others simply used the DoDAAC as the UIC. This has obviously caused confusion over the years.

The Office of the Under Secretary of Defense for Personnel and Readiness (OUSD P&R) is the DoD policy owner of the UIC. The database that contains all DoD UICs is the Unit Identification Code Search System (UICSS) which is administered by the Defense Manpower Data Center (DMDC) of the Defense Human Resource Activity (DHRA). This system obtains data from the Components' manpower systems. The Army uses the 6-digit UIC. Navy uses a 5-digit UIC and applies an "N" to the beginning of their codes. Air Force uses the Personnel Accounting System (PAS), and the Marine Corps uses the Reporting Unit Code (RUC) for personnel reporting, and the UIC for reporting of structure requirements. Currently, however, the Marine Corps system that provides data to UICSS is the Marine Corps Total Force System (MCTFS) which provides the RUC information. Suffice it to say that while the DoDAAC is a very specific code which can only be found in one Authoritative Data Source (ADS) – the DoDAAD – the UIC is less specific and from where it is derived depends upon the DoD Component, and the use in question. In many cases, when people refer to the "UIC," they are often really intending the DoDAAC.

The RIC is a 3-character, alpha-numeric code that uniquely identifies a unit, activity, or organization that requires system ability to route transactions or receive transactions routed to it (e.g., source of supply) within logistics and financial business systems using DLMS and legacy 80 record position format transactions. The first position of the RIC designates the particular service/agency ownership, the second and third characters are determined by the Central Service Point (CSP). The RIC was originally conceived as an abbreviated form of a seven-character Communication Routing Identifier (COMMRI) in order to facilitate routing of transactions in the limited format of the MILS 80 record position transactions. It was intended to identify a "node" in a supply process/system for the sake of routing the transaction for fulfillment, but its use has since expanded. The RIC is associated to a "RIC_DODAAC," in systems, because the RIC facilitates routing, while the DoDAAC to which the RIC is associated identifies the actual activity to which transactions are to be routed by the RIC. By way of analogy, consider your home. The RIC is like your phone number, but the DoDAAC is name and street address.

This directory was made available largely to anyone who asked for a copy of it. It was considered unclassified, and, as such, during the 1970's and 1980's, there was little concern for security of the information contained within the directory, even as it related to Operational Security (OpSec). Over time, with modernization of the DoD's logistics systems, the use of the codes within the directory began to evolve into uses beyond the DoD Supply Chain. In the 1990's, the use of the DoDAAC grew prolifically as further modernization efforts were undertaken by the DoD across all functional business domains. With each of these, and with the growth of the internet, information assurance protocols in DoD systems became more prevalent.

Recognizing the sensitivity of DoD information technology (IT) systems, in 1999, at the direction of Congress, the Defense Manpower Data Center (DMDC) began to implement smart card technology within DoD as a means to control access to systems. In 2001, with the advent of the attack on New York City and the Pentagon, the age of Cyber Security was thrust upon us as a nation. Coincidentally, in 2001, efforts were set in motion to reengineer the DoDAAD from the manual, batch transaction updated flat file directory into the dynamic, unlimited, and online updated database it is today. Those efforts culminated in the release of the re-engineered DoDAAD database in 2005. Shortly after the release of this new DoDAAD, the DoD launched a new CAC in 2006, in compliance with Homeland Security Presidential Directive-12 (HSPD- 12), which established a new federal standard for identification credentials issued to all federal employees and eligible contractors. In keeping with this, when the reengineered DoDAAD was released, access to the system was based largely on the requestor having a CAC and submitting a System Access Request (SAR) to the DAASC Help Desk. These basic access requirements remain relatively unchanged.