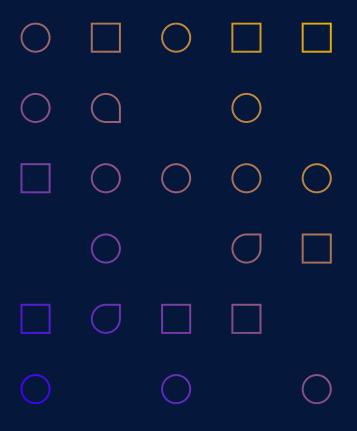# How the United States Marine Corps Targets War Records

A case study.

The U.S. Marine Corps had accumulated a massive amount of NIPR (Non-classified Internet Protocol Router Network) and SIPR (Secret Internet Protocol Router Network) data after ten years of operating in Afghanistan. The data was unstructured and potentially contained vital information covering the Marine Corps' presence and legacy in the region. The data consisted of emails, record message traffic, Microsoft Office files, PDF documents, images, personally identifiable information (PII) and collections of hour-by-hour, day-by-day records of events, incidents, actions and outcomes.

Developing a stronger data strategy

After extensive vetting, the Marine Corps selected ActiveNav to analyze, sort and organize this massive corpus of data. A Standard Operating Procedure (SOP) document was created to outline the data analysis and migration process in 5 steps:

Discover: Conduct an initial skim of the data

Cleanse: Remove redundant, obsolete, and trivial (ROT) data

Organize: Classify content using metadata tags

Evaluate: Review rule sets and modify workflows as needed

Migrate: Transfer data to temporary or permanent storage locations

At a glance

CHALLENGES

- Non-compliance with DoD Instruction 5015.02.
- Limited data visibility
- Vast amount of data containing PII
- Data spillage

BENEFITS

- Achieved records management compliance
- Quarantined sensitive data
- Significant ROT identification and removal
- Gained operational insight

ABOUT

- United States Marine Corps
- Federal Government
- Washington, DC
- 47,000+ Employees

ACTIVENAV

Meeting Mission Goals

By deploying ActiveNav to automate the processing of their wartime data, the Marine Corps can confidently manage their ever-increasing growth of data. The Marine Corps is able to continue to meet mission goals and leverage its data as a strategic asset.

ActiveNav helped the Marine Corps quarantine sensitive data including Personally Identifiable Information (PII) and medical information. Additional data spillage was also identified and properly handled.

The original Afghanistan war record data was unstructured and out of compliance with DoD Instruction 5015.02. By managing their data in line with government policies, the Marine Corps achieved records management compliance.

After developing best practices, the Marine Corps is expanding the project to additional units to gain insight into the operational history and evaluate training project plans (TPPs) and doctrine.

RESULTS

Indexed over 100 TB of data

77% of the data analyzed was ROT

Tens of thousands of sensitive data files were identified within unclassified data collections

Millions of documents were categorized using the DON Standard Subject Identification Code (SSIC)

Continued Operational Insight

After developing best practices, the Marine Corps is expanding the project to additional units to gain insight into the operational history and evaluate training project plans (TPPs) and doctrine.

Real-World Application

• **Intel Targeting Reports:** A collection of records that outline who, how, when, and where our forces conducted missions

• **Improvised Explosive Device (IED) Case Files:** A collection of records that contain descriptions, images, and plans regarding various IED attacks for lessons learned

GET STARTED TODAY. SEE ACTIVENAV IN ACTION. REQUEST YOUR DEMO.