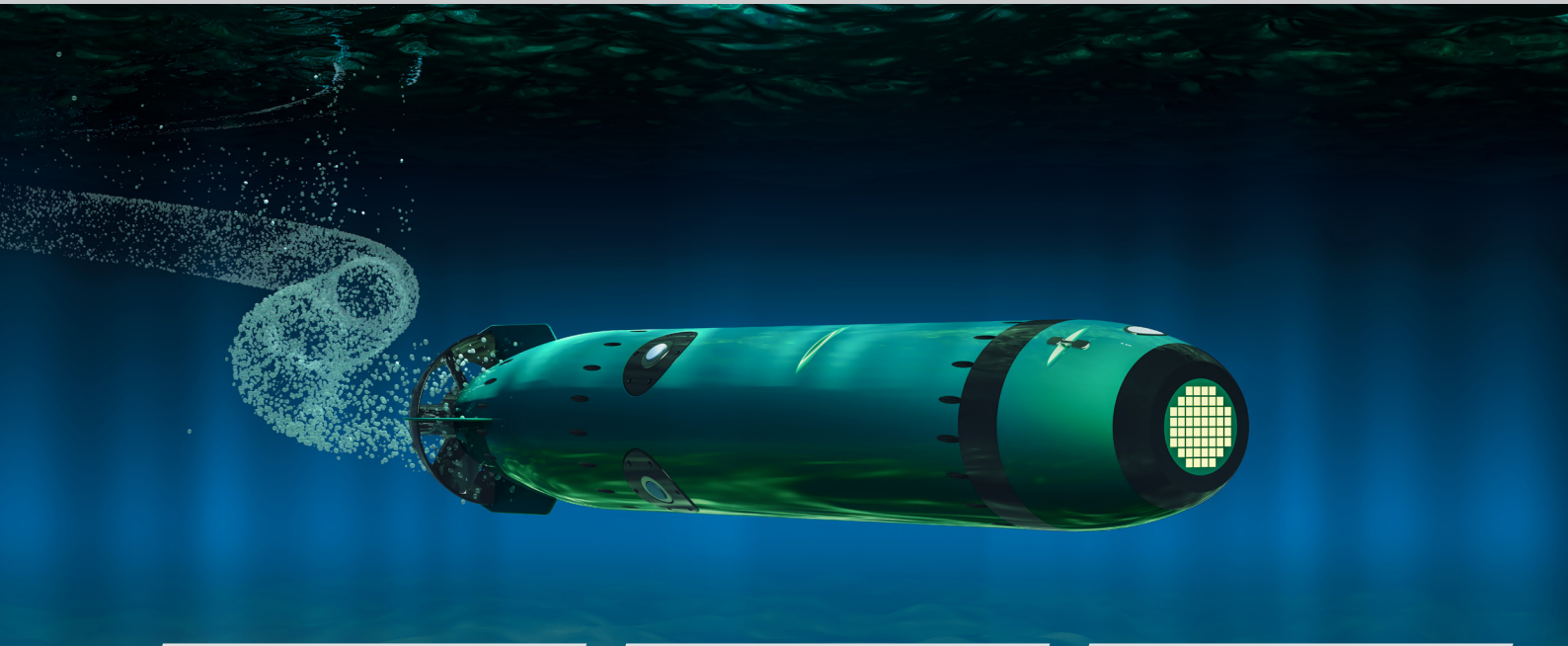


# Unmanned Underwater Vehicle NAS Protects Terabytes of Top Secret Mission Data

**CURTISS-  
WRIGHT**
**DEFENSE SOLUTIONS**


## Challenge

- Size constrained UUV
- High-capacity removable storage
- Protection for critical data at rest

## Solution

- SWaP-optimized DTS1
- 4TB Removable Memory Cartridge with path to 8TB
- NSA CSfC-approved 2-layer encryption

## Results

- Reduced SWaP enabling longer missions
- Large storage capacity with room for growth
- Top Secret data protected in transport

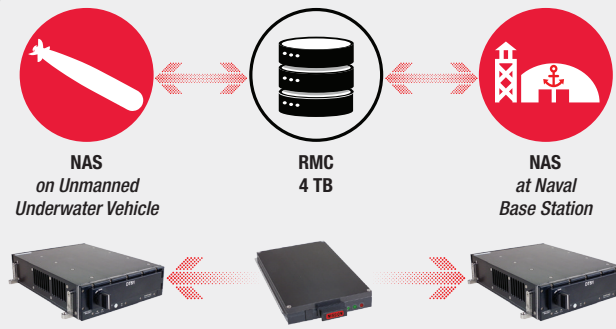
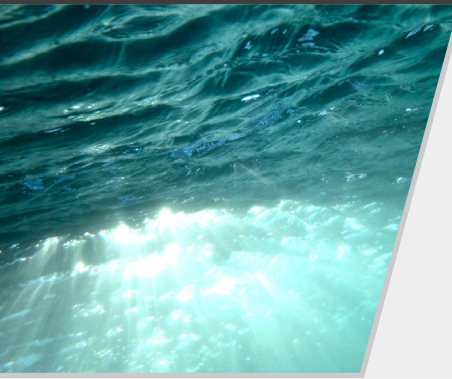
## Challenge

Unmanned underwater vehicles (UUV) provide an efficient way for the armed forces to autonomously perform critical underwater missions. These underwater drones often travel thousands of miles, remain on station for long periods of time, and collect massive amounts of data.

In search of a small form factor network attached storage (NAS) solution for a new UUV, an engineer at a defense contractor reached out to Curtiss-Wright. The UUV required a high storage capacity solution to store critical mission data on long-range missions. In order to conserve power and allow for longer, sustained missions, the UUV has a narrow cross-section to minimize drag as it moves along, which results in a space-constrained environment for onboard

systems, including the NAS. Weight is also an important consideration, since a lighter UUV requires less power for propulsion. As well, minimizing the power required for the UUV's embedded computing systems frees up more power for propulsion, enabling longer missions. Therefore, minimizing size, weight, and power (SWaP) was a major requirement of the contractor's.

Modern UUVs are equipped with a variety of sensors depending on the mission profile. At a minimum, the UUV's location, direction, and speed must be measured; however, environmental sensing is also critical in order to avoid obstacles (such as rock, shoals, and sand bars) and threats (such as surface vessels, other UUVs, and aircraft).



Collected by a sonar system, this environmental sensing data is gathered and stored so that it can be processed by a mission computer and used to navigate and complete the mission. The sonar data is also saved for post-mission analysis at the base station and provides valuable insights into the success of the mission.

However, as the 2016 capture of a UUV by the Chinese proved, sensor data must be protected – even simple oceanographic information like salinity or depth. Since their UUV would be collecting Top Secret data, the manufacturer required that the data at rest (DAR) be protected by agency-approved encryption techniques.

The UUV manufacturer asked Curtiss-Wright to propose a SWaP-optimized data storage solution that provided certified encryption and transportable high capacity storage to protect the platform's valuable mission data.

## **Solution**

After extensive trade studies, Curtiss-Wright's Data Transport System (DTS1) was studied and subsequently chosen for its small size and weight, high capacity, and internationally certified encryption technology.

The DTS1 is the industry's first commercial off-the-shelf (COTS) DAR NAS solution that supports two layers of full disk encryption in a single device. The DTS1 is a small form factor file server that weighs just three pounds, occupies less than 50 cubic inches, and provides scalable storage of up to 4 TB on a single removable memory cartridge (RMC), with a path to 8 TB, which can be easily transported.

The DTS1 provides two layers of Commercial Solutions for Classified (CSfC) approved encryption (one hardware and one software layer). CSfC is an NSA-approved approach for protecting classified National Security Systems (NSS) information. The two DTS1 encryption layers have each been certified by National Information Assurance Partnership (NIAP) under the Common Criteria (CC) program and are also listed as approved NSA CSfC components. Because the DTS1 layers are NSA CSfC approved, the customer could securely store Top Secret data onboard the UUV and then safely transport the data on the RMC. The RMC is considered unclassified when removed and unpowered.

## **Results**

CSfC-approved encryption was very important for the end customer, since the DTS1's NSA CSfC approval lowered the technical risk compared to other devices on the market that had not already been approved. While not a current requirement, the use of a COTS NAS device allowed the UUV to be considered for export to other allies around the world, in comparison to government off-the-shelf (GOTS) encryption techniques which are usually ITAR controlled with limited possible export customers.

Because the DTS1 has been approved for protection of Top Secret data when unpowered, the classified data could be safely transported between the base station and UUV. With adversaries targeting data during transport, this significantly lowered the data security risk.

It was also important to the customer that the DTS1 was available off the shelf. The customer (and their end customer) did not have to invest scarce non-recurring engineering (NRE) dollars in development or agency certification; instead, the device was quickly ready for system implementation. The small form factor DTS1 minimized schedule, technical, and security risk, all in one low-SWaP, off-the-shelf product, while also increasing mission efficiency and ensuring the protection of data during and after the mission. Designed for the general deployed marketplace, the DTS1 proved a perfect fit for this new UUV.