

# Pentagon Reviews Unisys Stealth

The United States Joint Forces Command (USJFC) is currently evaluating Unisys Stealth technology at the Joint Transformation Command for Intelligence (JTC-I) in Suffolk, Virginia.

"Unisys Stealth Solution for Network lets an organization set up "communities of interest" through a group policy using Microsoft Active Directory, with session-specific encryption keys scrambling data that can only be decrypted by those belonging to each group. Stealth works to "bit-split" data into multiple packets and re-assemble it to authorized users, which alone can decrypt it."



A Unisys press release further states that USJFCOM will be testing "cryptographic bit-splitting" as a way to converge DoD Global Information Grid networks operating at different security levels into a single network infrastructure.

"This technology can address a longstanding challenge for the Department of Defense and other government agencies: how to simplify their networks without sacrificing security, while delivering significant cost savings," said Jim Geiger, managing partner, Department of Defense, Unisys Federal Systems. "Unisys will draw upon its extensive experience with the Unisys Stealth Solution for Networks to support the Joint Forces Command and the Joint Transformation Command for Intelligence in this pioneering effort to promote secure data and information sharing among various communities within the DoD. This solution is now the double-encryption security mechanism protecting the Unisys Secure Cloud solution."

[December 2008 post](#) I described cryptographic bit splitting as a new approach for securing information. Its advantages include: Enhanced security from moving shares of the data to different locations on one or more data depositories or storage devices (different logical, physical or geographical locations

- Shares of data can be split physically and under the control of different personnel reducing the possibility of compromising the data.
- A rigorous combination of the steps is used to secure data providing a comprehensive process of maintaining security of sensitive data.
- Lack of a single physical location towards which to focus an attack

My company, Dataline LLC, is also leveraging this technology during the Trident Warrior '10 fall lab experimentation period. As I posted in US Navy Experiment With Secure Cloud Computing, the Secure Cloud Computing experiment has been designed to explore the use of a commercial Infrastructure as a Service (IaaS) platform as a viable means of supporting a specified subset of US Navy mission requirements for global connectivity, server failover and application access. Goals for the experiment include:

- Demonstrating the establishment and use of trusted communication paths on a global public computing infrastructure; and
- Demonstrating dynamic, mission driven, provisioning of information via trusted communication paths on a global public computing infrastructure

>I'll keep you posted on the outcome of both DoD activities.

{ *Thank you. If you enjoyed this article, [get free updates by email or RSS](#) - KLJ* }

Follow me at [http://Twitter.com/Kevin\\_Jackson](http://Twitter.com/Kevin_Jackson)