SPYRUS®

SPYRUS DFARS Security

Safeguarding Covered Defense Information and Cyber Incident Reporting for Contractors and Subcontractors

The Problem

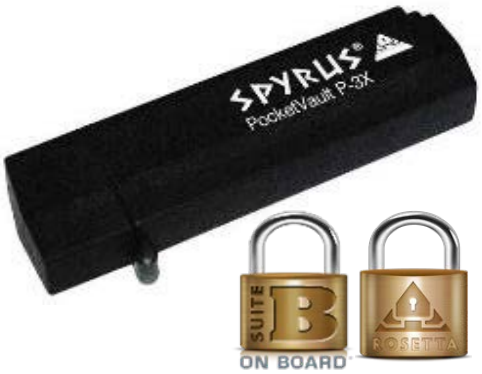
As of the end of 2017, guidance from the Undersecretary of Defense detailed the final implementation deadline for DFARS Clause 252.204-7012 “Safeguarding Covered Defense Information and Cyber Incident Reporting” with no further delays. DFARS compliance is required in all DoD contracts except for those solely for the acquisition of COTS items. Controlled Unclassified Information (CUI) is sensitive federal government information routinely processed, stored, or transmitted by a contractor in the course of its work providing essential products and services to federal agencies. In addition, contractors must include the clause in subcontracts for which performance will involve covered defense information or operationally critical support.

The Solution

SPYRUS solutions allow any organization to immediately meet the recently implemented DFARS Clause 252.204-7012 deadline for Safeguarding Covered Defense Information and Cyber Incident Reporting. The SPYRUS hardware roots of trust security solutions offer data protection assurance and continuity of operation at a cost-effective price point that will also address the security needs of your organization's global traveler workforce on assignment for U.S. Government projects.

SPYRUS Product Solutions

The SPYRUS Systems Engineering team can quickly recommend a high assurance security solution based on your specific needs and use cases that will ensure the protection of your organization's sensitive program information and data securely.



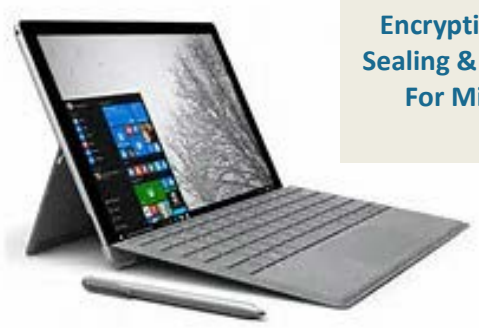
The **PocketVault P-3X USB 3.0** secure storage device is a high-security, use-anywhere encrypting solid-state disk (SSD) drive that protects data like a bank vault. The combination of USB 3.0 and SSD storage adds up to the fastest performance available. PocketVault drag files to it as you would with any USB drive. Every file on the PocketVault P-3X is securely protected in its encrypted solid-state storage. Cryptographic components in every SPYRUS secure storage device are designed, engineered, and manufactured in the United States by carefully vetted personnel. The PocketVault P-3X PKI smartcard is used for two-factor authentication to Windows PCs and cloud services requirements.

SPYRUS®

PocketVault p-3x Secure USB 3.0 with PKI

- Suite B on Board® Suite: XTS-AES 256 bit hardware encrypted storage, SHA-2 384, ECDH P-384
- Rosetta Hardware Security Module for MFA and PKI smartcard services
- FIPS 140-2 Level 3 overall and also the Rosetta security module
- Keys are always generated in the device, never exported
- Patent pending technology reconstitutes keys as required—they are not stored anywhere
- Passwords are never stored on the device, even in hashed form - MEK
- Password Policy Enforcement w/SEMS Device Management System
- Hardware Read-Only mode at logon for malware protection - on untrusted computers
- Undergoing CSfC in Canada
- Read –Only "Courier Mode" places control to alter data with admin, not end user
- Command line utility to assist in "restoring" of Windows operating system backups
- Capacities – 32, 64, 128, 256, 512 GB and 1 TB - uniquely
- SEMS: Ability to capture metadata for all file transfers on and offline mode

Securely sharing information from remote locations is made easy and secure with the **SPYRUS Rosetta® NcryptNshare™ (RES) products** Integrated with the Microsoft suite of productivity tools, including Office 365, you and your workforce will not have to be concerned about any data sharing transmission. The SPYRUS RES tools securely wrap all data, only accessible to the destination device and/or individual, so that the cloud or other unsecured communication paths can be used with the highest levels of confidence.



Hardware-based File Encryption, Authentication, Sealing & Sharing Applications For Microsoft Windows Platforms

RES Disk™	RES Pro™	RES4Office	RES4Outlook	RES Admin™	RES Publisher™
Virtual Disk Data Vault w/ PKI Sharing	Windows Explorer Extension Protects All File Types at Rest or in Transit for Secure Sharing	Microsoft Office Add-on for Protection from within MS Office Applications	Microsoft Outlook Add-on for Protection from within Outlook	Enterprise Admin Utilities that Stream-line Deployments	Publish w/ Read-only & Expiration Features for Mass Distribution

SPYRUS®

With sizes from 32GB to 1TB, SPYRUS Windows To Go and the Linux2Go USB 3.0 live drives provide for booting directly from the Windows To Go device and bypassing the host machine, while safeguarding the operating environments necessary with today's mobile workforce. The global traveler can carry their secure drive in their pocket and plug into any personal or local company computer confident that no information can be transmitted or lost through potential malware attacks.

	Portable Workplace	WorkSafe	SPW	SPW Xtreme	WorkSafe Pro	WSP Xtreme	Linux2Go & Xtreme
SSD & High Performance Random Read/ Write Speeds Critical to Boot OS	✔	✔	✔	✔	✔	✔	✔
Signed Firmware Prevents USB Attack	✔	✔	✔	✔	✔	✔	✔
Secure Boot Process	N/A	N/A	✔	✔	✔	✔	✔
Hardware Encryption XTS AES 256	✘	✘	✔	✔	✔	✔	✔
FIPS 140-2 Level 3 Certified (#2685)	✘	✘	✔	✔	✔	✔	✔
BitLocker Supported	✔	✔	✔	✔	✔	✔	✘
Rosetta FIPS 140-2 Level 3 Smart Card Access	✘	✔	✘	✘	✔	✔	✘
Data Vault Encrypted Compartment Option	✔	✔	✔	✔	✔	✔	✘
OS Malware Protection - Read Only Option	✔	✔	✔	✔	✔	✔	✔
32/64/128/256, 512GB & 1TB Capacities	✔	✔	✔	✔	✔	✔	✔
Support Boot from most Macintosh Computers	✔	✔	✔	✔	✔	✔	✔
Support Boot from Surface Pro 3/4	✔	✔	✔	✘	✔	✘	✔
MIL 810 Validated	✔	✔	✔	✔	✔	✔	✔
Up to 4 Cryptographically Separated Profiles	✘	✘	✘	✔	✘	✔	✔
Device Management Option (Enable, Disable, Password Reset, BitLocker Mgmt, "Kill Pill")	✔	✔	✔	✔	✔	✔	✔
Made In America	✔	✔	✔	✔	✔	✔	✔

SPYRUS®

At a cost significantly less than arguing the reasonability of your processes and taking the chance of becoming out of contract compliance, an end to end security solution that includes hardware roots of trust offer the only data protection assurance that similarly priced software solutions are UNABLE to achieve. The only way to protect against the ambiguity of "reasonable" is to protect your customer's and your brand beyond reasonable. Each component in your ecosystem can be managed with enterprise driven policy that enforce data protection controls, removing the ability for users and administrators to 'work-around' data protection security controls, maliciously or in error.

Important Discriminating Features

Operating system bootable live drives, hardware encrypted devices, and Trusted Flash® ensure, at the highest levels, protection of data at rest; protection of seeding, seeds and key generation.

Embedded Hardware Security Modules (HSMs) with smartcard and PKI support ensure, at the highest levels of protection, that only authorized users and/ or devices obtain data access and protect data in motion.

Secure identity-based encrypted data sharing and storage applications, leveraging a hardware root of trust to ensure, at the highest levels of protection, that data sharing is only allowed between authorized personnel on authorized devices.

The SPYRUS Enterprise Management System for HSM management, either on premise or hosted provides management, auditability, accountability and control of the enterprise's Hardware Roots of Trust, electronically enforcing enterprise control.

Made in USA, the SPYRUS products include industry's most extensive lineup of Windows To Go and Linux2Go bootable live drives, hardware encrypted PocketVault P-3X USB 3.0, and Rosetta® Trusted Flash® microSDHC data storage.

Each hardware product includes an embedded Rosetta HSM with smartcard and PKI support. A Microsoft [NASDAQ: MSFT] Gold Partner, SPYRUS supports the widest selection of certified Windows To Go products to meet different customer requirements with capacities up to 1 TB.

Additionally, the NcryptNshare secure sharing and storage applications combined with the SPYRUS Enterprise Management System™ (SEMS) provides enterprise management, auditability, and control of the entire family of SPYRUS security products. If used with the secure USB storage device, the PocketVault P-3X, SEMS can also track the meta data that is stored on the device, meaning you will always know what data was on the device if it was lost or stolen, an extremely important feature for audit compliance.

Contact SPYRUS at info@spyrus.com to obtain information on availability and pricing on the SPYRUS Hardware Security Modules and Software solutions.

Developers may access the SPYRUS Developers Portal at developer.spyrus.com and request a login to access detailed descriptions of typical applications and purchase prototyping quantities of SPYRUS HSMs.

Corporate Headquarters
103 Bonaventura Drive
San Jose, CA 95134
+1 (408) 392-9131 phone
+1 (408) 392-0319 fax
info@SPYRUS.com

East Coast Office
+1 (732) 329-6006 phone
+1 (732) 832-0123 fax

UK Office
+44 (0) 113 8800494

Australia Office
Level 7, 333 Adelaide Street
Brisbane QLD 4000, Australia
+61 7 3220-1133 phone
+61 7 3220-2233 fax
www.spyrus.com.au

Document number 402-000004-01