SPYRUS®

103 Bonaventura Drive | San Jose, CA 95134
USA +1-408-392-9131 | FAX +1-392-0782
https://www.SPYRUS.com

Cybersecurity Maturity Model Certification (CMMC)

SPYRUS Solution Addresses 60 controls to Safeguard Covered Defense Information and Cyber Incident Reporting for Contractors and Subcontractors

Secured Access, Data Protection & Endpoint Management

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.

OUSD(A&S) is working with DoD stakeholders to build upon DFARS 252.204-7012 by adding a verification component with respect to cybersecurity requirements. The Cybersecurity Maturity Model Certification (CMMC) initiative will include certified independent third-party organizations to conduct audits and inform risks across the Defense Industrial Base.

SPYRUS Solution

SPYRUS solutions enable any organization to immediately meet the DFARS Clause 252.204-7012 deadline for Safeguarding Covered Defense Information and Cyber Incident Reporting—and be ready for a CMMC audit that will be necessary to do business with the DoD. 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 provides 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. Each component in the SPYRUS solution can be managed with enterprise driven policy that enforces data protection controls, removing the ability for users and administrators to 'work-around' data protection security controls, whether maliciously or in error:

- Our family of bootable live drives, hardware encrypted devices, and TrustedFlash® ensure, at the highest levels, protection of data at rest;
- Our NcryptNshare secure sharing and storage applications leverage the SPYRUS hardware root of trust to ensure, at the highest levels of protection, that data sharing is only allowed between authorized personnel on authorized devices; and,
- The SEMS platform provides on premise or SEMSaaS hosted enterprise management, auditability, accountability and control of the entire family of SPYRUS security solutions, electronically enforcing enterprise controls.

103 Bonaventura Drive | San Jose, CA 95134
USA +1-408-392-9131 | FAX +1-392-0782
https://www.SPYRUS.com

SPYRUS PocketVault USB Secure Storage

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.

PocketVault USB Secure Storage and Live Drives

- Multi Factor Authentication (MFA) & PKI SmartCard services (keys generated on chip, never exported)
- AES (Advanced Encryption Standard) -128/192/256 (ECB, CBC, CTR) SHA-224/256/384/512
- ECDSA (Elliptic Curve Digital Signature Algorithm) P-256/384/521
- ECDH (Elliptic-curve Diffie–Hellman)
- RSA (Rivest–Shamir–Adleman), 3DES, SHA-1 & 2
- RNG (random-number generator) SP800-90 & FIPS 186-2
- Elliptic Curve Cryptography & RSA Algorithms
- High-entropy RNG
- Extensive Security Fault alarms
- Cryptographic Data Firewall
- Anti-cloning
- Split Knowledge Algorithm
- Secure Key Backup & Recovery Options
- Signal Radiation Masking
- Tamper-Protected Zeroization
- FIPS 140-2 Level 3
- MIL STD 810 validated – Shake, Rattle and Roll/Temperature, EMI, Waterproof, X-Ray & Magnet
- Common Criteria 5+ Components

Live Drives

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.

103 Bonaventura Drive | San Jose, CA 95134
USA +1-408-392-9131 | FAX +1-392-0782
https://www.SPYRUS.com

SPYRUS NcryptNshare

Securely sharing information from remote locations is made easy and secure with the **SPYRUS Rosetta® NcryptNshare™ 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. These 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.

SPYRUS Enterprise Management Systems (SEMS) Platform

At the heart of SPYRUS solutions is our SPYRUS Enterprise Management System™ (SEMS) platform. SEMS extends a true end-to-end security approach to manage user access, to protect data at rest; in transit. We enable the enterprise to comply with all applicable law and regulation. With SEMS user/device management, enterprise administrators can centrally register, block/unblock, revoke, set policies, integrate 3rd party applications for secured access, audit, and

"kill" the SPYRUS services and hardware encrypted devices. SEMS provides a high security and productivity solution for any organization deploying SPYRUS encrypting secure storage drives and/or our Microsoft certified bootable Windows To Go Live Drives. While these drives provide the strongest Authentication encrypted access, Data-at-Rest protection when used by the mobile workforce, organizations are faced with another challenge that is the management, audit and policy enforcement of these high capacity, small form factor devices.

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.

Meeting CMMC Requirements

The SPYRUS security solution addresses 60 controls required by NIST 800-171 & CMMC.

Access Control

1. Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).
2. Control the flow of CUI in accordance with approved authorizations.
3. Separate the duties of individuals to reduce the risk of malevolent activity without collusion.
4. Employ the principle of least privilege, including for specific security functions and privileged accounts.
5. Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.
6. Limit unsuccessful logon attempts.
7. Monitor and control remote access sessions.
8. Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.

Asset Management

9. Visibility into the hardware devices, to include removable media, operating on the network.
10. Discover/ prohibit new/ unauthorized devices that connect to the network.
11. Identify all devices actually present.
12. Address whether the device is authorized on the network.
13. Address whether someone is assigned to manage the device.
14. Prevent entry of malicious or compromised hardware from being installed on the system.
15. Reduce the number of easy-to-compromise devices that are not actively administered.
16. Prevent unauthorized hardware from being used for data exfiltration.

SPYRUS®

103 Bonaventura Drive | San Jose, CA 95134
USA +1-408-392-9131 | FAX +1-392-0782
https://www.SPYRUS.com

Audit and Accountability

17. Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.
18. Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.
19. Review and update logged events.
20. Alert in the event of an audit logging process failure.
21. Protect audit information and audit logging tools from unauthorized access, modification, and deletion.
22. Limit management of audit logging functionality to a subset of privileged users.

Identification and Authentication

23. Identify system users, processes acting on behalf of users, and devices.
24. Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.
25. Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.
26. Employ replay-resistant authentication mechanisms for network access to privileged and non- privileged accounts.
27. Prevent reuse of identifiers for a defined period.
28. Enforce a minimum password complexity and change of characters when new passwords are created.
29. Prohibit password reuse for a specified number of generations.
30. Store and transmit only cryptographically-protected passwords.
31. Obscure feedback of authentication information.

Personnel Security

32. Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.

Media Protection

33. Protect (i.e., physically control and securely store) system media containing CUI.
34. Limit access to CUI on system media to authorized users.
35. Sanitize or destroy system media containing CUI before disposal or release for reuse.
36. Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.
37. Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.
38. Control the use of removable media on system components.
39. Prohibit the use of portable storage devices when such devices have no identifiable owner.
40. Protect the confidentiality of backup CUI at storage locations.

Recovery

41. Actions taken to render data written on media unrecoverable by both ordinary and, for some forms of sanitization, extraordinary means.
42. Process to remove information from media such that data recovery is not possible. It includes removing all classified labels, markings, and activity logs.

Situational Awareness

43. Confidence in the protection of identity and encryption keys to safeguard sensitive data, sustain fundamental operations, and protect enterprise infrastructure would be under this.

System and Communications Protection

44. Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.
45. Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.
46. Separate user functionality from system management functionality.
47. Prevent unauthorized and unintended information transfer via shared system resources.

103 Bonaventura Drive | San Jose, CA 95134
USA +1-408-392-9131 | FAX +1-392-0782
https://www.SPYRUS.com

48. Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).
49. Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling).
50. Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.
51. Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.
52. Establish and manage cryptographic keys for cryptography employed in organizational systems.
53. Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.
54. Prohibit remote activation 27 of collaborative computing devices and provide indication of devices in use to users present at the device.
55. Protect the authenticity of communications sessions.
56. Protect the confidentiality of CUI at rest.

System and Information Integrity Provide

57. protection from malicious code at designated locations within organizational systems.
58. Monitor system security alerts and advisories and take action in response.
59. Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.
60. Identify unauthorized use of organizational systems.

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, 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.

About SPYRUS

SPYRUS develops and deploys cryptographic operating systems in innovative ways, providing the strongest protection for data in motion, data at rest and data in process. For more than 20 years, SPYRUS has delivered encryption, authentication, and digital content security products to government, financial, and healthcare enterprises. SPYRUS solutions enable customers to meet stringent regulatory requirements for data protections across industries.