SecurityFirst™
Data-Centric Cyber Solutions

WHITE PAPER

Keeping-up with Government Requirements

Defense Department Contractor Data Protection Mandate

As a contractor doing business with the Department of Defense (DoD), your needs for data protection are exploding. Recent updates to Defense Federal Acquisition Regulations (DFARS) now mandate that even unclassified DoD information residing on a contractor's internal information systems must be safeguarded from cybersecurity incidents. Furthermore, the requirements in DFARS clause 252.204-7012 must be implemented when Covered Defense Information (CDI) is processed, stored, or transits through an information system that is owned or operated by the contractor, or when performance of the contract involves operationally critical support. That doesn't leave a lot out.

The quickest and easiest way to comply with these updated regulations is to apply data encryption and access controls to everything stored or processed by your information technology (IT) systems, and today's advanced solutions make that plausible. In most cases, gone are the days when processing overhead would bog-down encryption and decryption activities causing a noticeable slowing of your application systems. Also, encryption key management can be a simplified activity whether you choose a software solution or integrate a Hardware Security Module (HSM) thanks in part to the Key Management Interoperability Protocol (KMIP).

New Requirements

Companies, organizations, and contractors that provide services to the DoD are required to fully comply with the Defense Federal Acquisition Regulations (DFARS) specifying requirements for contracts, foreign acquisitions, bonds, insurance, taxes, labor laws, materials content, etc. Cybersecurity requirements and compliance mandates for IT systems are specified in DFARS 252.204-7008 and 7012 respectively, with the National Institute of Standards (NIST) Special Publication 800-171 serving as the governing publication.

Deciphering even the clear-text descriptions in these publications is a bit of an art form in itself, but what they specify is a pronounced need for data protection. These entities have long since been required to protect information carrying a restricted classification (Confidential, Secret, etc.), but as of last year are also now required to protect data and information deemed "sensitive but unclassified." This significantly expands the amount of data that needs to be protected and controlled in order to enforce authorized access and use.

The incremental information that must be protected per DFARS 252.204-7012 includes:
a. Contractor attributional or proprietary information
b. Controlled technical information
c. Covered defense information
i. Marked or identified
ii. Collected, developed, etc.
d. Technical information

The regulation also outlines precise measures regarding what these organizations must do for compliance. They must implement NIST SP 800-171, and adhere to the further guidance provided in DFARS 252.204-7008. Compliance can be achieved through security solutions, processes, or a combination of the two, and organizations must use their best judgment to reasonably determine associated data that may need to be protected. However, the regulation is not totally inflexible; it allows the use of cloud environments, as long as they conform to the FedRAMP Moderate Baseline definitions.

Are You Compliant?

Some have estimated the amount of data that must be protected resulting from these updates has increased by 10-fold or more. Accordingly, this expanded protection mandate has potentially created large gaps in accepted and existing data security practices, requiring that all organizations doing business with the DoD reassess their information technology systems, operations, processes, and data classifications. Oh joy.

As a result, many organizations--especially lower-tier contractors and small businesses--will suddenly find themselves out of compliance and will suffer dire consequences if they fail to address the new requirements. An expanded use of encryption, access controls, and monitoring technologies is almost a given, but choosing the wrong technology can simply make matters worse. Imagine telling the board that yes, your data was encrypted, but even your IT experts can no longer retrieve the original data.

New Complexity

DoD contractors will now need to introduce additional complexity into their existing environments. The variety of data sets and the associated workflows can present a difficult problem when expanding current data protection practices. For example, many applications that use this newly defined “unclassified but sensitive data” will require customizations to maintain proper functions. New point products will likely need to be introduced into the IT environment creating bottlenecks and scalability issues. Access control solutions must also be reviewed and adjusted. Finally, these new products and processes will need to be integrated into a security information and event management (SEIM) environment.

Potential Consequences

Failure to comply with the new mandate has very clear implications for every organization. The four primary consequence types are:

- Criminal
- Civil
- Administrative
- Contractual

Facing any of these can trigger remedial actions through federal, state, and local law, including penalties such as fines, monetary damages, and more. Civil actions for damages and other appropriate remedies could also be adjudicated. Non-compliance often results in a breach: the exposure of data to unauthorized third parties that can then exploit it for improper or illegal activity. Statistics suggest that any organization doing business online can expect to fall victim to at least one successful cybersecurity attack every 36 months, and DoD contractors are a favorite hacker target.

The cost of a successful data breach can be staggering. Survey data suggests the average to be $3.62M (Ponemon Cost of a Data Breach 2017). Even when covered by cyber insurance, such costs can decimate any contractor equity and frequently put them out of business.

The Way Forward

Getting compliant with the new mandate may seem overwhelming, but there is a proven strategy available to develop an effective data security posture, regain control, and achieve compliance.

Here are three integrated vectors to pursue:

1. Federated and unified data protection (primarily focused on encryption)
2. Policy-based access control (with separation of duties and least-user privileges)
3. Detection and response to incidents (through SIEM and analytics tools)

Federated data security is the ability to use a single data encryption tool across the enterprise. It is characterized by a central management capability to expand as the data environment grows, scaling the security perimeter without creating new attack avenues or risks. Policy-based access control works in conjunction with the federated encryption to provide complete control of data access, eliminating the Insider Threat through the use of stringent and monitored separation of duties and default least user privilege. Additionally, the unified encryption and access control capability delivers a minimized attack surface and compartmentalized damage control, significantly reducing exposure and risk to the data environment in the event of a successful breach.

Achieving compliance is essential, but doing so cost-effectively is just as important. Reducing the complexity is vital, contractors should consider outsourcing this new solution set to providers skilled in both security and DOD compliance. Outsourcing allows a contractor to stay focused on its core skills and services without adding complexity to its IT environment or expanding staff. Finally, using an MSP or CSP with FedRAMP approved facilities eliminates capital expenditures and provides access to expert services for delivering expedient and cost-effective compliance.

DataKeep™ – The Solution

DataKeep is an advanced data-centric software solution that protects sensitive and personal data from being exposed in the event of a breach, while ensuring compliance with regulatory requirements and data privacy mandates.

Security teams can define and log access policies by job role, while blocking privileged user access, securely encrypting at the source and transparently managing encryption keys. DataKeep technology protects data on Windows and Linux, physical and virtual servers and encrypts at volume-level or file-level for additional granularity. Powered by secure SPxCore technology, DataKeep combines AES-256 encryption with cryptographic splitting and internal key management certified by the NIST to be FIPS 140-2 compliant.

The need for data protection is clear. The public is demanding data privacy, and network perimeter controls alone aren't enough. Data must be protected at its core to provide protection and as a last line of defense.

About SecurityFirst

SecurityFirst™ delivers data-centric solutions that address the high-profile cyber threats facing organizations today, such as data breaches, ransomware and cloud security. We emphasize protection of the data itself to serve as your last line of defense. Data is always protected no matter where it resides and recoverable in the event of an unexpected failure or malicious attack such as malware or ransomware. As organizations and governments mandate stricter requirements for data privacy, SecurityFirst helps protect data from compromise and exposure.

About DataKeep

DataKeep™ secures critical data at its core to deliver unrivaled protection, control and resiliency. Customer-defined access policies, strong encryption and event logging combine with native secure backup/restore capabilities to address your data privacy, compliance and recovery needs.

Security teams can define and log access policies by job role and manage privileged and superuser access to block insider and external threats. DataKeep securely protects data at the source no matter where data resides, encrypting data at the volume or file level for attached storage or before sending to object storage. Native backup and restore commands can be leveraged to enable prompt recovery of archived data in the event of a ransomware attack.

DataKeep's ability to support M of N distributed shares allows companies to encrypt, split and distribute data across multiple object store locations or vendors for business continuity and operational efficiency. Organizations can utilize the backup and restore capabilities with object storage for secure cloud backup and archiving to improve resiliency.
Secure your most valuable assets – your data, your brand and your reputation – with Datakeep.