Supporting DFARS 7012 NIST SP 800-171 Regulatory Compliance Requirements with Spirion

For covered contractor information systems that are not part of an IT service or system operated on behalf of the Government, the following security requirements apply:

> *The covered contractor information system shall be subject to the security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations…. The Contractor shall implement NIST SP 800-171, as soon as practical, but not later than December 31, 2017.*
>
> *~ Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012*

About the DFARS 252.204-7012

The Department of Defense (DoD), General Services Administration (GSA), and National Aeronautics and Space Administration (NASA) published a rule that requires federal government contractors, grantees, or those with cooperative agreements to apply cybersecurity controls to protect corporate information systems effective June 15, 2016. The systems are to be protected with control requirements based on security requirements published in NIST 800-171, “Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations.”

The scope of this requirement is limited to systems that store Covered Defense Information (CDI), which in this case is defined to include any information related to “the performance of the contract" that DoD provides to the contractor— pretty much anything. This also includes data the contractor accumulates in support of the contract— pretty much everything. As a result, DFARS 252.204-7012 is an expansive requirement and will have a dramatic impact on the number of systems that must be considered in-scope of a gap assessment. System information covered under this rule falls into four categories:

- Controlled Technical Information (CTI), which is defined as "technical information” with military or space application that is subject to controls or everything the government has provided or asked for already.
- OpSec information about intentions, capabilities, and activities that an adversary could use to guarantee failure or unacceptable consequences.
- Export-controlled information, such as "dual-use" technologies like nuclear or biochemical information.
- Any additional information specifically identified in the contract, which is pretty much whatever the government has not asked for yet.

The new rule also flows down to subcontractors, but only applies if subcontractors meet the same applicability definitions described above. The new rule also notes that compliance with basic safeguarding requirements will not remove any other regulatory or existing contractual requirements related to safeguarding government information in covered contractor information systems.

NIST SP 800-171

NIST SP 800-171 outlines the basic safeguarding requirements that applicable contractors must implement. The publication includes 14 families of security requirements, comprising 109 individual controls.

The following pages detail how Spirion helps organizations align with the controls families.

Function: Identify

Category: Access Management (ID.AM)	Subcategory:	Spirion's Features:
The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried.	Spirion's Remote Network discovery can scan any number of user defined IP address ranges facilitating the identification of systems on the network and locate and inventorying of all sensitive data on those systems.
	ID.AM-4: External information systems are catalogued.	Spirion can search any location, including third-party service providers data sources and accurately locate an inventory all sensitive data.
	ID.AM-3: Organizational communication and data flows are mapped.	Spirion watches user's document usage and can classify, quarantine, shred, redact execute scripts, or modify permissions based on workflow rules. Spirion can accurately locate, classify, monitor and report where sensitive data is found—on anything it can connect to across an organization's network and cloud environments. Spirion working with network data loss prevention (DLP) solutions can control data movement using Spirion Classifications written to the file's metadata.
	ID.AM-5: Resources (e.g., hardware, devices, data, time, and software) are prioritized based on their classification, criticality, and business value.	Spirion can locate, identify and classify both structured, unstructured and user-defined sensitive data using real-time, on-demand or scheduled scans.
	ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established.	Spirion facilitates Role Based Access Controls and secure Profiles for data stakeholders and data stewards.
Category: Governance (ID.GV)	**Subcategory:**	**Spirion's Features:**
The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	**ID.GV-3:** Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed.	Spirion can assist organizations in managing their sensitive data for legal and regulatory requirements through customizable automated data classifications and automated monitoring and reporting. Spirion can manage sensitive data to ensure it resides in approved locations using automated workflow rules.
	ID.GV-4: Governance and risk management processes address cybersecurity risks.	Spirion can assist organizations in managing their risk for legal and regulatory requirements through automated audit scanning and automatic reporting. Spirion can be used as a risk mitigation strategy using automated workflows to quarantine, redact or shred and encrypt files based on workflow rules.
Category Business Environment (ID.BE)	**Subcategory:**	**Spirion's Features:**
The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	**ID.BE-5:** Resilience requirements to support delivery of critical services are established.	Spirion's discovery process locates sensitive data (PII, PCI, PHI or confidential data or intellectual property unique to the organization) which facilitates the creation of data classification rules based on sensitivity of data defined by the organizational business rules. This permits identification of critical systems and prioritization of the data that needs attention.

Risk Assessment (ID.RA)	Subcategory:	Spirion's Features:
The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	**ID.RA-1:** Asset vulnerabilities are identified and documented.	Spirion's discovery process inventories the location of all sensitive data which includes the device, data steward (owner), and many other attributes. This process is automated and can send alerts.
	ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed.	Spirion provides a proactive process which inventories all sensitive data and its location. This proactive and prudent step provides a cyber awareness of the security footprint. Identifying the devices with large amounts of confidential and/or sensitive data enables organizations to make informed decisions to harden or remove those devices containing.
	ID.GV-4: Governance and risk management processes address cybersecurity risks.	Spirion's AnyFind™ definitions in addition to the Sensitive Data Engine™ facilitates location of all sensitive data. Using these results facilitates the ability to make informed decisions around the management of sensitive data and assess cybersecurity risk next best steps.
	ID.BE-5: Resilience requirements to support delivery of critical services are established.	Spirion provides resilient processes and an architecture to deliver enterprise operations. The services are low impact and all operations highly configurable thus reducing risk to ongoing business process.
Category: Risk Management (ID.RA)	**Subcategory:**	**Spirion's Features:**
The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	**ID.RA-1:** Asset vulnerabilities are identified and documented.	Spirion can assist organization in their risk assessment and monitoring efforts through identifying where sensitive data is located using automated scanning and reporting, ensuring compliance to vulnerability mitigation procedures.
	ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk.	Using previous system scans and reports organizations can better access, identify and manage risk based on complete visibility of sensitive data in the organization.
	ID.RA-6: Risk responses are identified and prioritized.	Spirion allows organizations to prioritize their responses based on knowing what systems contain classified data and the amount of that data.

Function: Protect

Category: Access Control (PR.AC)	Subcategory:	Spirion's Features:
Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	**PR.AC-4:** Access permissions are managed, incorporating the principles of least privilege and separation of duties.	Spirion's Role Based Access Controls (RBAC) limit authorized users and operations to granular permissions for Console activities. This approach incorporates the principle of least privileges (POLP) and separation of duties.
Category: Awareness and Training (PR.AT)	**Subcategory:**	**Spirion's Features:**
The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	**PR.AT-1:** All users are informed and trained.	Spirion can be used as a training aid by showing users what sensitive data has been found on their system and provide them an opportunity to remediate the data themselves. Tags added to the data are reflected in metadata, icon overlays and application integrations.
	PR.AT-2: Privileged users understand roles & responsibilities.	Spirion provides on-demand contextual links from within the Spirion application console and client documentation for end-users and privileged IT professionals. This documentation promotes application policy and security awareness and responsibilities in the role. Documentation and training aids are also available on the Spirion consumer portal, user guides and through Technical Support.
Category Description: Data Security (PR.DS)	**Subcategory:**	**Spirion's Features:**
Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	**PR.DS-1:** Data-at-rest is protected.	Spirion can constantly monitor systems to ensure sensitive data is only stored in approved locations and quarantine, shred or redact data based on workflow rules.
	PR.DS-2: Data-in-transit is protected.	Spirion classifications can be used by network DLP solutions to manage and control data movement.
	PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition.	Spirion workflows and actions are formally defined and managed by definitions applicable to the business data handling process for the organization. This remediation process provides options to move data to appropriate locations (quarantine), delete (shred), redact, encrypt, and the removal off over permissive data. The accountability of these processes assure that the definitions created by the organization are appropriate and consistent with the organizations technical strategy. Needs to be repeatable and defensible to ensure data security.
	PR.DS-5: Protections against data leaks are implemented.	Spirion classifications can be used by network DLP solutions to manage and prevent data exfiltration. Spirion can scan and monitor removable media.
	PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity.	Spirion can verify information integrity though file hash scanning.

Category: Information Protection Processes and Procedures (PR.IP)	Subcategory:	Spirion's Features:
Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	**PR.IP-1:** A baseline configuration of information technology / industrial control systems is created and maintained.	Spirion provides a discovery engine in addition to AnyFind definitions that provide a baseline set of templates to locate data types. Accurate data discovery and automated persistent data classification is the first line of defense and the foundation to an effective cybersecurity program.
	PR.IP-6: Data is destroyed according to policy.	Spirion can employ automated sanitization of sensitive data based on location, classification and/or data types using user configurable DoD standards shredding.
	PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties.	Spirion's customizable reporting engine can generate reports automatically or when specific workflow rules are executed and can be automatically distributed to appropriate parties to assist in monitoring the effectiveness of their data protection strategies. Spirion Sensitive Data Watcher™ monitors the file system and automatically detects, classifies and reports on confidential data in real-time as files are created, modified or moved. Alerting, automated notifications, assignment and remediation are performed according to customized workflow processes. Risk exposure can be visualized in real time with Spirion Spyglass™.
Category: Protective Technology (PR.PT)	**Subcategory:**	**Spirion's Features:**
Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	**PR.PT-1:** Audit / log records are determined, documented, implemented, and reviewed in accordance with policy.	Spirion includes User and Event audit and logging processes. This event configuration ensures that security integrity is maintained through documented and implemented process facilitating reviews in accordance with organizational audit and security policy.
	PR.PT-2: Removable media is protected and its use restricted according to policy.	Spirion can scan and monitor removable media and can quarantine, shred or redact data based on workflow rules.
	PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality.	Spirion applies the principle of least privileges. System process use the most restrictive system account process. Access to Spirion is controlled using Role Based Application Control (RBAC) and Active Directory integrations consistent with security industry best practices. This process is consistent and well documented.

Function: Detect

Category: Anomalies and Events (DE.AE)	Subcategory:	Spirion's Features:
Anomalous activity is detected in a timely manner and the potential impact of events is understood.	**DE.AE-3:** Event data are aggregated and correlated from multiple sources and sensors.	Spirion can watch systems in real-time as users create and edit documents. As sensitive information is detected Spirion can take automated actions and report the data and actions taken back to the console server and/or alert appropriate personnel. The visualization tool SpyGlass™ is incorporated within the Spirion console to quickly understand discovery, remediation and risk exposure over an historical time line.
	DE.AE-5: Incident alert thresholds are established.	Spirion can be configured to alert at user-defined levels for user defined events and take predetermined actions including alerting personnel.
Category: Security Continuous Monitoring (DE.CM)	**Subcategory:**	**Spirion's Features:**
The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	**DE.CM-1:** The network is monitored to detect potential cybersecurity events.	Using Spirion's ability to classify sensitive data and 3rd party network DLP solutions' ability to read those classifications, data movement can alert personnel to cybersecurity events.
	DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events.	Spirion provides granular event and user event logging (monitoring) as events occur. Spirion monitors and captures data real-time using Sensitive Data Watcher™ for numerous types of data repositories. Spirion system Event and User logging provides audit level to detect potential cybersecurity events.

Function: Respond

Category: Response Planning (RS.RP)	Subcategory:	Spirion's Features:
Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.	**RS.RP-1:** Response plan is executed during or after an event.	Spirion processes, such as workflow and remediation, provide security response processes executed in a repeatable and maintained process to ensure timely response to data events. This functionality provides action as part of the response plan for the event(s).
Category: Communications (RS.CO)	**Subcategory:**	**Spirion's Features:**
Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.	**RS.CO-3:** Information is shared consistent with response plans.	Spirion provides SIEM integration, SNMP Trap and e-mail notifications providing coordinated and consistent response with stakeholders as deemed appropriate. Access is granted through RBAC controls.
Category: Analysis (RS.AN)	**Subcategory:**	**Spirion's Features:**
Analysis is conducted to ensure adequate response and support recovery activities.	**RS.AN-2:** The impact of the incident is understood.	Using Spirion's previous system scans, the types of sensitive data, amounts of sensitive data and the classifications of that data are instantly known and can be used to guide incident response.
	RS.AN-3: Forensics are performed.	Spirion can be used in a forensics capability to determine what data existed on the system at the time of the security incident.
	RS.AN-4: Incidents are categorized consistent with response plans.	Using both historical data and current information the severity of the incidents can be better assessed and proper response plans implemented.
Mitigation (RS.MI)	**Subcategory:**	**Spirion's Features:**
Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.	**RS.MI-1:** Incidents are contained.	Spirion's automated scans and reporting can quickly assist organizations in containing incidents.
	RS.MI-2: Incidents are mitigated.	Spirion's automated scans and reporting can assist organization in protecting vital systems and mitigate data loss.

About Spirion

Spirion, headquartered in Saint Petersburg, Florida, is the leader in the rapid discovery and classification for protection of sensitive data across your network and public cloud. Spirion provides enterprise data management software to help businesses reduce their sensitive data footprint and proactively minimize the risks, costs and reputational damage of successful cyberattacks.

Spirion helps organizations avoid costly data breaches by discovering, classifying, monitoring and protecting personal information, medical records, credit card numbers, and intellectual property stored across the enterprise, within e-mail, and in the cloud. Spirion specializes in the high-precision search and automated classification of unstructured data using its AnyFind engine's unparalleled accuracy when analyzing human-generated text and images. Spirion has thousands of customers among leading firms in the healthcare, public sector, retail, education, financial services, energy, industrial, and entertainment markets. To learn more, please visit spirion.com.

Contact Us

Spirion, LLC
+1 (646) 863-8301
info@spirion.com
www.spirion.com