VECTRA®

How Cognito supports the Defense Federal Acquisition Regulation Supplement (DFARS) and NIST framework

To protect Covered Defense Information (CDI) – unclassified data categorized as sensitive because it was provided by or generated for the U.S. government and not intended for public release – comes DFARS 252.204-7012 and rules pertaining to "Safeguarding Covered Defense Information and Cyber Incident Reporting."

The DFARS supplement applies to all U.S. Department of Defense (DoD) solicitations other than procurements for "commercial off-the-shelf items."

If a company has contracts with the DoD, or is a subcontractor to a prime contractor with DoD contracts, that organization has until Dec. 31, 2017 to implement NIST SP 800-171. This is a requirement that is stipulated in the DFARS 252.204-7012.

The DFARS cyber clause must be flowed down to all suppliers or subcontractors that will store, process and/or generate CDI as part of contract performance.

CDI includes unclassified controlled technical information or other information, as described in the Controlled Unclassified Information (CUI) Registry at http://www.archives.gov/cui/registry/category-list.html. It requires safeguarding or dissemination controls pursuant to and consistent with law, regulations and government-wide policies, and is:

1. Marked or otherwise identified in the contract, task order, or delivery order and provided to the contractor by or on behalf of DoD in support of the performance of the contract; or
2. Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract.

Controlled technical information means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination.

Controlled technical information would meet the criteria, if disseminated, for distribution statements B through F using the criteria set forth in DoD Instruction 5230.24, Distribution Statements on Technical Documents. The term does not include information that is lawfully publicly available without restrictions.

The good news is NIST 800-171 has a mapping table (Appendix D) to map controls from NIST 800-53 to NIST 800-171. NIST 800-53 is the federal framework for securing critical infrastructure, a widely used standard for mapping process and maturity of a security program.

The sections below highlight key components of the NIST framework and provide details about how the Cognito™ cybersecurity platform from Vectra® provides DoD contractors and subcontractors with continuous, automated threat detection and response across enterprise networks – from cloud and data center workloads to user and IoT devices.

Using artificial intelligence, Cognito condenses weeks or months of work into minutes, enabling security operations teams to take swift action to prevent theft or damage from cyber-attacks. The categories described by NIST 800-171 that are supported by Cognito are detailed in the following tables.

3.4 CONFIGURATION MANAGEMENT

Subcategory	Cognito capability
Basic security requirements	
3.4.1 – Establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	Cognito continuously monitors and analyzes internal network traffic, internet-bound traffic and data center traffic, including traffic between virtual workloads in the data center to establish baselines of system behaviors and to identify unapproved activity.
3.4.2 – Establish and enforce security configuration settings for information technology products employed in organizational information systems.	Cognito continuously monitors and analyzes internal network traffic, internet-bound traffic and data center traffic, including traffic between virtual workloads in the data center to establish baselines of system behaviors and to identify unapproved activity.
Derived security requirements	
3.4.3 – Track, review, approve/disapprove, and audit changes to information systems.	Cognito tracks the internal Kerberos infrastructure to understand normal usage behaviors and detect when trusted user credentials are compromised by attackers, including the misuse of administrative credentials and abuse of administrative protocols, such as IPMI.
3.4.4 – Analyze the security impact of changes prior to implementation.	Cognito provides multiple early-warning opportunities to detect ransomware, other malware variants, and malicious activity that precedes an attack on any network device, including devices that do not run antivirus software.
3.4.5 – Define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system.	Cognito continuously monitors and analyzes all network traffic, including internal traffic between physical and virtual hosts with an IP address, such as laptops, smartphones, BYOD and IoT devices, regardless of the operating system or application.
3.4.6 – Employ the principle of least functionality by configuring the information system to provide only essential capabilities.	A combination of supervised and unsupervised machine learning applied to the local network develops the baseline of appropriate and approved behavior from which to identify unapproved behavior of personnel, connections, devices, and software.
3.4.7 – Restrict, disable, and prevent the use of nonessential functions, ports, protocols, and services.	A combination of supervised and unsupervised machine learning applied to the local network develops the baseline of appropriate and approved behavior from which to identify unapproved behavior of personnel, connections, devices, and software.
3.4.8 – Apply deny-by-exception (blacklist) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.	A combination of supervised and unsupervised machine learning applied to the local network develops the baseline of appropriate and approved behavior from which to identify unapproved behavior of personnel, connections, devices and software.

3.6 INCIDENT RESPONSE

Subcategory	Cognito capability
Basic security requirements	
3.6.1 – Establish an operational incident-handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities.	Metadata is analyzed with behavioral detection algorithms to identify hidden and unknown attackers. For example, supervised machine learning lets Cognito find the hidden traits that all threats have in common, while unsupervised machine learning reveals attack patterns. Cognito condenses thousands of events and network traits to a single detection using machine learning techniques that automatically expose attackers based on the characteristics of network traffic.
3.6.2 – Track, document, and report incidents to appropriate organizational officials and/or authorities.	Automated scoring of hosts reveals the overall risk to the network based on threat and certainty. The Threat Certainty Index™ from Vectra scores all threats and prioritizes attacks that pose the biggest risk. The scoring of compromised hosts by the Threat Certainty Index allows security teams to define threshold levels based on combined scoring (e.g., critical > 50/50).

VECTRA®
Security that thinks®

Email info@vectra.ai **Phone** +1 408-326-2020
vectra.ai