NIST 800-171 Compliance Reports

Simplify NIST 800-171 Compliance with AWN CyberSOC™

Today, federal departments and agencies are increasingly digitized and subcontracted. This has led to an explosion of government data held in the information systems of subcontractors who work with sensitive or confidential data related to agriculture, finance, military and other areas that fall under federal regulations.

To keep this information secure, Executive Order 13556 established the Controlled Unclassified Information (CUI) program to standardize the way federal contractors handle unclassified information that requires protection, such as personally identifiable information, or sensitive government assets.

This program has issued final guidelines for protecting this data, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations", known as the NIST 800-171 standard. The US Department of Defense has issued the Defense Federal Acquisition Regulation Supplement (DFARS) cybersecurity requirement. This rule requires defense contractors to meet the NIST 800-171 standard or risk losing their contracts.

Arctic Wolf's security operations center (SOC)-as-a-service enables defense contractors and other government contractors to meet many of the NIST 800-171 compliance requirements using the industry-leading cloud-based AWN CyberSOC. Arctic Wolf simplifies compliance reporting with the help of our dedicated Concierge Security Engineers who are assigned to your account.

NIST 800-171 Compliance Requirements

Controlled Unclassified Information (CUI) can be stored in a variety of repositories, such as file servers, databases, access logs and other types of unstructured and structured data repositories. Safeguarding access to CUI and defending it from outside attack requires diligent administration and close cooperation between the IT teams and the many business units that need access to the data.

Finding the right balance between the tasks supported by your IT organization and the checks to be automated through Arctic Wolf's SOC-as-a-service enables you to streamline NIST 800-171 compliance and reduce costs.

AWN CyberSOC

- Best managed threat detection and response
- Dedicated security expertise for your IT team
- 24/7 monitoring with unlimited log sources

Benefits

- Simplifies NIST 800-171 compliance with customized reporting
- Protects CUI by monitoring all communications and traffic for malicious activity
- Supports incident response and risk-assessment exercises
- Enables compliance with DFARS cybersecurity requirements

Arctic Wolf validates several primary requirements of NIST 800-171, including basic and derived security requirements in the following areas:

Section	Requirement:
Sec. 3.1	Access Control
Sec. 3.3	Audit and Accountability
Sec. 3.5	Identification and Authentication
Sec. 3.6	Incident Response
Sec. 3.11	Risk Assessment
Sec. 3.13	System and Communication Protection
Sec. 3.14	Workstation Security

A full list of NIST 800-171 requirements is available from the National Institute of Standards website.

Arctic Wolf Compliance Solution for NIST 800-171

Arctic Wolf's AWN CyberSOC™ monitors activity in on-premises IT infrastructure and in cloud applications using physical/virtual Arctic Wolf sensors. AWN CyberSOC continuously monitors network flows and ingests log records from an unlimited number of log sources, and uses human-assisted machine learning to accurately detect and respond to advanced attacks.

Arctic Wolf's Concierge Security Engineer™ (CSE) dedicated to each customer account extends your IT staff with security expertise, hunts down advanced zero-day attacks, and provides customized compliance reports to meet your NIST requirements. The table below shows how the AWN CyberSOC enables you to address and provide evidence for several key areas of NIST requirements.

	Requirement	Arctic Wolf Solution
Sec. 3.1: Access Control	**3.1.20:** Verify and control/limit connections to and use of external information systems.	The AWN CyberSOC service receives firewall logs, which can be used to demonstrate requirement compliance.
Sec. 3.3: Audit and Accountability	**3.3.5:** Use automated mechanisms to integrate and correlate audit review, analysis, and reporting processes for investigation and response to indications of inappropriate, suspicious or unusual activity.	AWN CyberSOC delivers this service via automated tools and adds a Concierge Security Engineer to reduce false positives and provide additional context and actionable intelligence.
	3.3.6: Provide audit reduction and report generation to support on-demand analysis and reporting.	Arctic Wolf has many standard reports and can create custom reports on an ad-hoc or weekly schedule. We also support our customers in the event of an audit or external investigation including exporting of event/log data or real-time discovery via screen sharing with your assigned CSE.
	3.3.8: Protect audit information and audit tools from unauthorized access, modification and deletion.	Arctic Wolf has strict security policies in place to prevent unauthorized access to SOC tools. Log data is encrypted in transit and at rest.

	Requirement	Arctic Wolf Solution
Sec. 3.5: Identification and Authentication	**3.3.5:** Use automated mechanisms to integrate and correlate audit review, analysis, and reporting processes for investigation and response to indications of inappropriate, suspicious or unusual activity.	AWN CyberSOC™ delivers this service via automated tools and adds a Concierge Security Engineer™ to reduce false positives and provide additional context and actionable intelligence.
	3.5.3: Use multifactor authentication (MFA) for local and network access to privileged accounts and for network access to non-privileged accounts.	Arctic Wolf can provide log data from MFA systems used, such as Okta or DUO, to comply with this requirement.
Sec. 3.6: Incident Response	**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.	Arctic Wolf can provide closed ticketed incidents as evidence of an operational handling capability.
	3.6.3: Test the organizational incident response capability.	Arctic Wolf can help validate your incident response plan by performing a tabletop IR exercise.
Sec. 3.11: Risk Assessment	**3.11.2:** Periodically scan for vulnerabilities in information systems and applications, as well as when new vulnerabilities affecting the system are identified.	This is a core function of the Arctic Wolf service for externally exposed systems.
Sec. 3.13: System and Communication Protection	**3.13.1:** Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	The Arctic Wolf sensor generates net flow data at egress points to the public internet, and can also work off span/mirror ports for key internal subnet/VLANs and provide monitoring and alerting based on the net flow data.
	3.13.5: Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	Arctic Wolf can provide firewall log data from servers or systems installed in the separated zones.
	3.13.14: Control and monitor the use of voice over Internet protocol (VoIP) technologies.	VoIP traffic can be monitored by an Arctic Wolf sensor using an internal tap or span/mirror configuration. If the central server (call manager etc.) is providing logs via syslog, that can be used for additional context and alerting.
Sec. 3.14: System and Information Integrity	**3.14.6:** Monitor information systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	This is a core function of the AWN CyberSOC service, and is conducted through a sensor appliance that acts as a managed intrusion detection system.

ARCTIC WOLF

AICPA SOC

SOC2 Type II Certified

Contact us

arcticwolf.com
1.888.272.8429
info@arcticwolf.com