SOLUTION BRIEF

NIST 800-171 Compliance

Simplify NIST 800-171 Compliance with Arctic Wolft

Government business is now increasingly digitized and subcontracted. This has led to an explosion of government data held in the information systems of subcontractors, including sensitive or confidential data related to agriculture, finance, military, and other areas regulated by federal government agencies.

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.

The program issued final guidelines for protecting this data in "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations," known as the NIST 800-171 standard. The US Department of Defense announced that its contractors must meet this standard or risk losing their contracts.

Arctic Wolf® enables defense contractors and other government contractors to meet many of the NIST 800-171 compliance requirements using the industry-leading Arctic Wolf® Managed Detection and Response, and Arctic Wolf® Managed Risk offerings. Arctic Wolf simplifies compliance and compliance reporting with the help of a dedicated Concierge Security® Team of engineers 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 IT teams and the many business units that need to access the data.

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

Arctic Wolf Security Operations

- Superior managed threat detection and response
- Continuous risk assessment and vulnerability management
- Dedicated security expertise for your IT-team
- 24x7 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

> "Arctic Wolf security operations include everything Sparks needs for a comprehensive security operations function. We looked at alternatives from some of the largest IT security vendors and went with Arctic Wolf because it was easy to purchase and deploy, and was priced in a predictable way. To build the equivalent of the service internally would cost at least 10 times more."
>
> — Steve Davidek, IT Manager, City of Sparks, Nevada

City of Sparks

IDENTIFY
PROTECT
DETECT
RESPOND
RECOVER
NIST

NIST Frameworks for Data Security

NIST 800-53

- Helps federal agencies implement proper controls required under FISMA
- Applies to federal agencies

NIST 800-171

- Used to demonstrate compliance with DFARs for handling Controlled Unclassified Information (CUI), a subset of NIST 800-53
- Applies to organizations that work with US government entities or handle sensitive government data

Cybersecurity Framework (CSF)

- Outlines standards, guidelines, and best practices to manage cybersecurity-related risk
- A voluntary framework useful to any organization

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. 3.4	Configuration Management
Sec. 3.5	Identification and Authentication
Sec. 3.6	Incident Response
Sec. 3.7	Maintenance
Sec. 3.8	Media Protection
Sec. 3.11	Risk Assessment
Sec. 3.12	Security Assessment
Sec. 3.13	System and Communication Protection
Sec. 3.14	System and Information Integrity

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 Managed Detection and Response (MDR) monitors activity in on-premises IT infrastructure and in cloud applications using Arctic Wolf sensors. Arctic Wolf MDR 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 monitors on-premises environments as well as cloud environments, including infrastructure-as-a-service (AWS, Azure) and software-as-a-service (Microsoft 365, G Suite, Box, Salesforce, etc.).

The Arctic Wolf Managed Risk solution is a vulnerability assessment service managed by security experts. The solution enables you to continuously scan your networks and endpoints, as well as quantify risk-based vulnerabilities.

The Arctic Wolf Concierge Security Team (CST) 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 Arctic Wolf enables you to address and provide evidence for several key areas of NIST requirements.

Requirement	Arctic Wolf Solution
Sec. 3.1: Access Control	
3.1.1: Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	Arctic Wolf provides you with role-based access control for audit logging/alerts/reports, account management or changes, as well as mechanisms to centrally review access activities.
3.1.2: Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	Arctic Wolf provides you with role-based access control for audit logging/alerts/reports, account management or changes.
3.1.3: Control the flow of CUI in accordance with approved authorizations.	Arctic Wolf provides you with monitoring activities for file and application access, USB monitoring, and email metadata analysis.
3.1.4: Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	Arctic Wolf provides reporting and alerting on attempts to cross role boundaries, and also on changes to configuration that affect separation of duties.
3.1.5: Employ the principle of least privilege, including for specific security functions and privileged accounts.	Arctic Wolf provides network connection monitoring, application execution, and records and monitors system logon activities.
3.1.6: Use non-privileged accounts or roles when accessing non-security functions.	Arctic Wolf provides process execution, application installs, and command execution, which are reported dependent on OS/application auditing.
3.1.7: Prevent non-privileged users from executing privileged functions and audit the execution of such functions.	Arctic Wolf can capture the event logs that Windows creates when privilege/administrative functions are carried out, such as DNS changes and changes to system files.
3.1.8: Limit unsuccessful logon attempts.	Arctic Wolf provides the capability to alert and report on login failures. Access to the Arctic Wolf customer portal is linked to the Active Directory (AD) with password controls that are generally a function of AD.
3.1.9: Provide privacy and security notices consistent with applicable CUI rules.	Arctic Wolf can provide baseline configuration checks that determine non-compliant systems.
3.1.10: Use session lock with pattern-hiding displays to prevent access/viewing of data after period of inactivity.	Arctic Wolf connection sessions time out after a period of inactivity, which is generally a function of AD. A screensaver hides contents from being viewed.
3.1.11: Terminate (automatically) a user session after a defined condition.	Arctic Wolf sessions time out after a period of inactivity.

NIST 800-171 Compliance (Continued) >

NIST 800-171 Compliance (Continued)

3.1.12: Monitor and control remote access sessions.	This control is related to remote access. Arctic Wolf captures and reports on remote desktop sessions and VPN logs. Arctic Wolf reporting can identify users and times of remote access sessions.
3.1.13: Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	SSL is used for remote access by the Arctic Wolf Concierge Security Team (CST). Your CST monitors for connection type such as SSL/TCP.
3.1.14: Route remote access via managed access control points.	Arctic Wolf provides contextual data on activities from remote access control points for designated systems and produces alerts/reports.
3.1.15: Authorize remote execution of privileged commands and remote access to security-relevant information.	Arctic Wolf provides contextual data on activities, and monitors where, when, “who did what?”, and “who tried to do what?”. Role-based access restricts access to privileged functions.
3.1.17: Protect wireless access using authentication and encryption.	Arctic Wolf® Agent detects the wireless configuration used by a workstation, and will report on the settings of that access point.
3.1.20: Verify and control/limit connections to and use of external information systems.	Arctic Wolf Managed Detection and Response can monitor based on network connections and firewall rules, and provides contextual data on the use of external systems.
3.1.21: Limit use of organizational portable storage devices on external information systems.	Arctic Wolf Agent provides visibility on endpoints for all user activities pertaining to USB devices such as connect/eject and files copied, and provides the ability to block personal thumb drives.
Sec. 3.3: Audit and Accountability	
3.3.1: Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity.	Arctic Wolf Managed Detection and Response fully supports tracking, reporting, and alerting on all audit events generated by host systems. Audit events are those that are significant and relevant to the security of information systems. Arctic Wolf provides a complete package of predefined reports and alerts based on systems/applications in use. This information is useful for incident response and demonstrating compliance activities.
3.3.2: Ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.	Arctic Wolf supports tracking, reporting, and alerting on all audit events generated by host systems. Audit events are events that are significant and relevant to the security of information systems. Host systems audit records generally contain all the information, including timestamp, login id, and status. Arctic Wolf provides a complete package of predefined reports and alerts based on systems/ applications in use. This information is useful in incident response and demonstrating compliance activities.

NIST 800-171 Compliance (Continued) >

NIST 800-171 Compliance (Continued)

3.3.3: Review and update audited events.	The Arctic Wolf Concierge Security Team conducts weekly analysis, and performs monthly and quarterly security and risk reviews.
3.3.4: Alert in the event of an audit process failure.	Arctic Wolf Concierge Security Team alerts/reports when audit logs have been received.
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.	Arctic Wolf Managed Detection and Response delivers this service via automated tools, and adds the Concierge Security Team to reduce false positives and provide additional context and actionable intelligence. For vulnerability assessment and risk management, the Arctic Wolf Managed Risk solution supports hundreds of different manufacturer log feeds to provide organization-wide risk awareness across business, information systems, and security. The Arctic Wolf Concierge Security Team provides expertise, discipline, and accountability for analyzing and prioritizing indications of compromise.
3.3.6: Provide audit reduction and report generation to support on-demand analysis and reporting.	Arctic Wolf provides many standard reports and can create custom reports on an ad-hoc basis. Arctic Wolf also supports 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 CST. Additionally, Arctic Wolf provides log filtering and reporting capabilities.
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. Logs are cryptographically hashed upon archiving, and Arctic Wolf Agent-based logs are encrypted by default in transit and at rest.
3.3.9: Limit management of audit functionality to a subset of privileged users.	The Arctic Wolf customer portal supports role-based, granular access to users based on administrative policies.
Sec. 3.4: Configuration Management	
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.	Arctic Wolf provides baseline configuration reports for Windows systems, and detects and reports on changes. However, this is one part of configuration management. Baselines may be maintained for each system and deviations from baselines will be documented in the Arctic Wolf customer support portal. Arctic Wolf maintains a classification and categorization register of all assets configured in the IT environment.

NIST 800-171 Compliance (Continued) >

NIST 800-171 Compliance (Continued)

3.4.2: Establish and enforce security configuration settings for information technology products employed in organizational information systems.	Arctic Wolf can report on changes to settings dependent upon the type of logs received. The internal vulnerability assessment and configuration management capabilities of Arctic Wolf Managed Risk are required for configuration assessments. Additionally, Arctic Wolf Agent runs pre-defined security controls benchmarks and reports on those benchmarks.
3.4.3: Track, review, approve/disapprove, and audit changes to information systems.	Audit events and changes can be monitored by the Arctic Wolf Concierge Security Team (CST) depending on the log data received. In addition, the CST provides a daily snapshot of changes to Windows systems.
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.	Arctic Wolf Agent provides operational telemetry to categorize and inventory installed hardware and software, and alerts on non-whitelisted applications, suspicious processes, unpatched devices, vulnerabilities, and more.
3.4.9: Control and monitor user-installed software.	Arctic Wolf Agent provides operational telemetry to categorize and inventory installed hardware and software to control and monitor endpoints for user-installed software, applications, suspicious processes, unpatched devices, vulnerabilities, and more.
Sec. 3.5: Identification and Authentication	
3.5.1: Identify information system users, processes acting on behalf of users, or devices.	Arctic Wolf Agent monitors endpoints for active processes on workstations and servers. The Arctic Wolf Concierge Security Team can set alerts based on a custom set of variables.
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, such as Okta or DUO.
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.	The Arctic Wolf Concierge Security Team works with you to closely define your organizational objectives, establish alert and ticketing methodologies, provide monthly and quarterly analysis of your security posture, monthly and quarterly analysis of vulnerabilities and your risk posture with Arctic Wolf Managed Risk, as well as incident response activities and containment actions with Arctic Wolf Managed Detection and Response and Arctic Wolf Agent.
3.6.2: Track, document and report incidents to appropriate officials and/or authorities both internal and external to the organization.	The Arctic Wolf Managed Detection and Response solution notifies you of any relevant security incidents.

NIST 800-171 Compliance (Continued) >

NIST 800-171 Compliance (Continued)

Sec. 3.7: Maintenance	
3.7.1: Perform maintenance on organizational information systems.	The Arctic Wolf Managed Risk solution monitors systems for out-of-date software and configurations, and provides reports and analysis with trends and graphs to track progress.
Sec. 3.8: Media Protection	
3.8.2: Limit access to CUI on information system media to authorized users.	Using Arctic Wolf Agent to monitor Active Directory and access logs of workstations and servers, The Arctic Wolf Concierge Security Team monitors events 24/7 and provides alerts where unauthorized users have attempted to access CUI on information system media.
3.8.8: Prohibit the use of portable storage devices when such devices have no identifiable owner.	The Arctic Wolf Agent can whitelist specific USB devices, and alert on non-approved device serial numbers when these are connected to endpoints (workstation, or server).
Sec. 3.11: Risk Assessment	
3.11.1: Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of CUI.	The Arctic Wolf Managed Risk solution provides continuous scanning of your internal and external networks and endpoints for vulnerabilities and risks. Your risk posture is monitored 24/7 by the Arctic Wolf Concierge Security team, with monthly and quarterly risk reports reviewed with your IT team.
3.11.2: Periodically scan for vulnerabilities in information systems and applications and when new vulnerabilities affecting the system are identified.	Arctic Wolf Managed Risk continually scans internal and external systems for vulnerabilities. Arctic Wolf MDR scans externally exposed systems for vulnerabilities. The Arctic Wolf Agent leverages security controls benchmarking to provide a view into globally-accepted configurations, and provide analysis of your risk posture.
3.11.3: Remediate vulnerabilities in accordance with assessments of risk.	The Arctic Wolf Concierge Security Team works with you to prioritize critical vulnerabilities, and assist with severity assessment and triage of vulnerabilities.
Sec. 3.12: Security Assessment	
3.12.1: Periodically assess the security controls in organizational information systems to determine if the controls are effective in their application.	Arctic Wolf Agent conducts internal vulnerability assessments, and completes host-based scans looking for potential vulnerabilities through security controls benchmarking and recommended configurations.
3.12.3: Monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.	Arctic Wolf Agent provides for continuous monitoring of security controls on endpoints such as workstations and servers through security controls benchmarking.

NIST 800-171 Compliance (Continued) >

NIST 800-171 Compliance (Continued)

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 Managed Detection and Response provides firewall log data from servers and 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 the Arctic Wolf Managed Detection and Response solution 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	
3.14.1: Identify, report, and correct information and information system flaws in a timely manner.	Detailed technical information on identified vulnerabilities and recommendations are provided by the Arctic Wolf Managed Risk solution to remediate the vulnerability. Reports of vulnerabilities, including those that relate to specific compliance requirements, are created with the Arctic Wolf Concierge Security Team.
3.14.3: Monitor information system security alerts and advisories, and take appropriate actions in response.	The Arctic Wolf Managed Detection and Response solution ingests alerts from other security tools, such as antivirus and firewalls, etc. Additional user context is layered onto the alert, helping you make informed decisions faster.
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 Arctic Wolf Managed Detection and Response solution, and is conducted through a sensor appliance that acts as a managed intrusion detection system.

About Arctic Wolf: Arctic Wolf® is the market leader in security operations. Using the cloud-native Arctic Wolf® Platform, we provide security operations as a concierge service. Highly trained Concierge Security® experts work as an extension of your team to provide 24x7 monitoring, detection, and response, as well as ongoing risk management to proactively protect systems and data while continually strengthening your security posture. For more information about Arctic Wolf, visit arcticwolf.com.

ARCTIC WOLF