FORESCOUT

Implement NIST 800-171 Quickly and Effectively with Device Visibility and Device Compliance

> **“Cybersecurity is, you know, probably going to be what we call the ‘fourth critical measurement.’ We’ve got quality, cost, schedule, but security is one of those measures that we need to hold people accountable for[1]”**
>
> — Patrick Shanahan, Deputy Secretary of Defense

Federal contractors provide a valuable service to the country by supplying the Department of Defense (DoD) with goods and services. The recent mandate issued through the Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-Supply Chain. NIST 800-171 contains over 100 controls which, when implemented effectively, can provide defense contractors with a solid security program.

Now that the mandate has been in effect for several months, ask yourself: How compliant are you? Are you ready to defend your systems against an attack? Are you sure you can see all the devices that enter or leave your network? Do you know all the systems that contain Controlled Unclassified Information (CUI) data? How complete is your System Security Plan (SSP)? Forescout can help you to reduce the impact of compliance on your budget by simplifying and effectively implementing NIST 800-171 controls.

Simplifying Compliance Through Visibility™

The first step to implementing NIST 800-171 is knowing the devices on your network, the access rights they have, when they connect and which data and applications these devices are allowed to access. Organizations need proof that mechanisms on these devices for securing CUI data, such as encryption agents, are operational. They also need visibility into the applications that access CUI data. Given the huge proliferation of devices, organizations need a different approach. Traditional agent-based security solutions do not provide a complete solution. An organization’s security tools must work in an agentless manner to see all devices, regardless of type, and ensure compliance with corporate policies as well as with NIST 800-171.

Quickly Comply with 800-171 with These Seven Tips:

1. **Conduct internal review to identify CUI (2) (1)** The first and most basic step toward compliance is developing a keen understanding of where CUI resides and who uses it. The proliferation of devices on a daily basis makes it challenging to identify and segment those that could contain sensitive data and ensure that they are compliant with corporate policies for patching, encryption and authentication.

   Solution: Forescout can provide visibility of every device from mobile to IoT to data center devices, Forescout gathers asset intelligence continuously upon connection and integrates with your current vulnerability management systems.

2. **Establish cui environment and migrate data (3)** Shrinking the footprint for CUI data not only limits overall risk exposure, but it reduces the cost of protecting it. For this reason, it is important to create a separate environment on the network to store all CUI data.

   Solution: Install (or configure existing) a firewall and create a CUI network segment or segments. Shrinking the footprint for CUI data not only limits overall risk exposure, but it reduces the cost of protecting it. Forescout can help with the network segmentation strategy which incorporates control in your campus, data center and cloud environments to ensure the entire application ecosystem that handles your CUI data is segmented.

3. **Implement technical controls (4) (5) (6)** The technical controls represent challenges. Allowing sufficient time to evaluate, select, and implement solutions is a must. Some of these are:

   A. **Security/file integrity monitoring**
   Logs from devices that reside on the CUI environment are collected and evaluated by a security monitoring technology to identify anomalies in system and file access. Encryption and other strategies can be deployed.

   B. **Vulnerability scanning**
   All devices on the CUI environment (including the firewall) must be scanned on a frequent basis to identify security gaps (vulnerabilities) in software and operating systems. Equally important to collecting vulnerability data is the process of repairing (applying patches) to remediate the gaps. Ensure that maintenance activities are scheduled in similar frequency to the vulnerability scanning process.

   Solution: Forescout can be leveraged by extending continuous monitoring and security controls across your entire environment—from campus to data center to the cloud—to ease compliance. Use an advanced network visibility solution to discover noncompliant devices and trigger/enforce updates.

   C. **Multifactor authentication**
   Any employee that needs access to CUI data will be required to utilize multifactor authentication to access the segmented CUI environment.

   Solution: Forescout can be leveraged as an agentless solution to gain visibility of accounts on all types of managed and unmanaged devices, including IoT devices. Next, automate policy-based access control and enforcement of these devices based on their security posture and behavior. Developing a baseline will help you articulate any current control gaps

4. **Develop policies and conduct awareness training** Policies are a critical factor in achieving NIST 800-171 compliance as they provide both process and technical guidelines on how CUI data will be managed.er

   Solution: Leverage Forescout to mandate that IT Security has been completed before your moved into a production computing environment. Orient the written policy with the segmentation strategy that enforces the training and awareness of your CUI environment via validation that you have completed training. Forescout can confirm that training is current and complete by referencing a 3rd party database that stores the appropriate access list.

5. **Conduct security and risk assessments (7)** These assessments are designed to help the organization understand what controls are required to effectively protect CUI data and then evaluate their effectiveness at protecting it.

   Solution: Forescout is the heterogeneous security solution that works across campus, data center and cloud environments—allowing you to manage a large number of endpoints with a single console for quicker response and efficiency. Add in an advanced SIEM to close the full circle of an IOC to more efficiently protect and automate responses in near real time. Cyber incidents must be reported to the DoD within 72 hours.

6. **Develop and publish an incident response plan (7)** An incident response plan serves as the focal point for handling elevated threats to CUI information. Both technical controls (Step 4) and process controls (Steps 5 and 6) are evaluated and documented to identify thresholds of risk that require notification/involvement from organization stakeholders to sufficiently investigate and resolve.

   Solution: Leverage Forescout to avoid breaches of CUI data. Orchestrate security information sharing and workflows across your current SIEM, ATD and other security and IT management tools to get the most from your investments and accelerate and automate incident response through Forescout.

7. **Develop and publish a system security plan (the tool)** A System Security Plan summarizes identified risks and describes how the organization addresses (or plans to address) the NIST 800-171 requirements. It defines the environment in which the system operates and how the security requirements are implemented.

   Solution: Leverage Forescout as the integral solution tool for your system security plan. Forescout can be leveraged across multiple applications, flows, across the campus, data center and cloud environments and crossed boundaries in multiple areas of your security groups. Each of the policies within Forescout can be pointed to as the solution across all these areas to comply sooner.

Learn More

- Accelerate and Maintain NIST Compliance Solution Brief
- Campus Compliance Solution Brief
- Forescout Compliance Guide

Learn more at
www.Forescout.com

FORESCOUT

Forescout Technologies, Inc.
190 West Tasman Drive
San Jose, CA 95134, USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support 1-708-237-6591

[1] Aaron Mehta, Fifth Domain, September, 2018, “Shanahan: cybersecurity will become new measure for industry” - https://www.fifthdomain.com/digital-show-dailies/air-force-association/2018/09/19/shanahan-cyber-security-will-become-fourth-critical-measurement-for-industry/?utm_source=Sailthru&utm_medium=email&utm_campaign=ebb%2009.20.18&utm_term=Editorial%20-

[2] DFARS CyberReporting Requirement: DFARS 252.204-7012(c)(1)(iii)

© 2019 Forescout Technologies, Inc. All rights reserved. Forescout Technologies, Inc. is a Delaware corporation. A list of our trademarks and patents can be found at https://www.forescout.com/company/legal/intellectual-property-patents-trademarks. Other brands, products, or service names may be trademarks or service marks of their respective owners. **Version 06_19**