Business Challenges

- Protect Controlled Unclassified Information
- Avoid data breaches that result in loss of public trust, and which can lead to losing contracts and grants
- Improve overall network security
- Demonstrate and maintain DFARS compliance
- Ensure subcontractor compliance with DFARS

Technical Challenges

- Keep targeted attacks from stealing CUI data or forcing network downtime
- Discover connected devices and identify their level of compliance
- Prevent infected or non-compliant devices from spreading malware
- Measure effectiveness of security controls and demonstrate compliance with NIST 800-171
- Orchestrate unified, automated device remediation and threat-response capabilities

ForeScout Can Help You Accelerate and Maintain NIST 800-171 Compliance

We secure federal assets today. We can help you keep your contracts and grants by helping you to accelerate and maintain NIST 800-171 compliance!

Supply-chain vulnerabilities can result in breaches in national security. Several U.S. government contractors have experienced a publicly disclosable data breach in the past two years.[1] Contractors must implement NIST 800-171 and report deficiencies within 30 days of contract award. ForeScout provides support for approximately 87 percent of the technical NIST 800-171 controls,[2] simplifying compliance and disclosing gaps.

The Challenge

The Department of Defense (DoD) requires all contractors that process, store or transmit Controlled Unclassified Information (CUI) to have met the Defense Federal Acquisition Regulation Supplement (DFARS) minimum security standards by December 31, 2017 or risk losing their DoD contracts.[3]

NIST 800-171 provides a framework for all companies that conduct business with the DoD to protect CUI. Whether you represent a prime contractor, subcontractor, research university, chemicals/pharma manufacturer—or you have other business interests with the DoD—you are required to implement the controls and comply with 800-171 to continue to do business with the DoD.

The ForeScout platform helps with 800-171 preparedness by automating and accelerating your path to compliance, reducing overall risk and maintaining and demonstrating ongoing compliance.

Ask Yourself:

- Is your staff equipped to interpret and apply all 110 controls of 800-171?
- Can you afford the time to devote potentially billable resources to creating and enforcing policies, as well as monitoring compliance to this framework?
- If you're manually monitoring compliance today, can you effectively demonstrate immediate responsiveness to a breach so as to report it within 72 hours?
- Have you identified every device that is responsible for using/transferring/handling CUI data?

Critical DFARS 252.204.7012 Requirements for Contractors:[3]

- **Adequate security** (7012-b): Provide adequate security on all covered contractor information systems.
- **Subject to NIST 800-171** (7012-b(2)(i)): 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"
- Be compliant as of **December 31, 2017** and notify DoD CIO within 30 days of contract award if not compliant ((7012-b(2)(ii)(A))
- **Have a System Security Plan (SSP) and other measures for non-standard devices.** Apply other measures especially for non-standard devices (7012-b(3)): Apply other information systems security measures when the Contractor reasonably determines that information systems security measures, in addition to those identified in paragraphs (b)(1) and (2) of this clause, may be required to provide adequate security in a dynamic environment or to accommodate special circumstances (for example, medical devices) and any individual, isolated, or temporary deficiencies based on an assessed risk or vulnerability.
- **Rapidly report all cybersecurity breaches within 72 hours:** ((7012-c (1)(ii))
- **Require all of the above from subcontractors** (7012-m(1): Include this clause…in subcontracts, or similar contractual instruments, for operationally critical support, or for which subcontract performance will involve covered defense information.

How ForeScout helped a defense contractor satisfy DFARS requirements:

Before ForeScout

A defense contractor that works directly with the U.S. DoD had a challenge with DFARS NIST 800-171 compliance, specifically, gaining real-time visibility into devices connected to the network and the ability to identify and take action on rogue devices. ForeScout conducted a trial that found a high percentage of machines that were not managed, out of compliance, had broken agents or were not accessible. The analysis showed the company that they were dealing with an acute level of risk. Reports revealed that 64 percent of their Windows machines had critical patches missing and 62 percent had no antivirus running.

How ForeScout helped

ForeScout installed rapidly on a production network and immediately started collecting data. The company's SecOps personnel quickly observed when new devices joined the network, and created policies to quarantine or block unauthorized devices. The company was able to choose not to use 802.1X and provide support for a heterogeneous infrastructure without adding additional agents to an already "agent-heavy" environment.

Why ForeScout for 800-171 compliance?

By providing visibility into devices connected to the network, ForeScout offers direct component support for over 50 of the 109 NIST 800-171 controls as well as supplemental support across over 90 controls. The ForeScout platform agentlessly detects devices as they connect to the network, automates simple and repeatable tasks, and infuses those elements into existing IT security and management services. As a result, it can illuminate blind spots and improve process workflow automation. The following table shows key use cases for protecting CUI data in contractor networks.

Use Case	NIST 800-171 Control[4]	How ForeScout Helps
Configuration Management Recent research by BitSight showed that nearly one in five Technology and Aerospace/Defense contractors use an outdated Internet browser in the workplace, increasing exposure to compromise.[1]	NIST 800-171 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.	You can leverage the ForeScout platform to help enhance and ensure your CMDB is up to date in real time with the latest versions of software found on the devices. You can manage other data points of your devices for other requirements. The benefit of this integration is that the CMDB is a real-time rather than point-in-time database.

Remote Access Many prime contractors allow remote access to their networks to the sub-contractors with whom they work.	NIST 800-171 3.1.12: Monitor and control remote access sessions.	Use ForeScout to monitor and control remote access, including VPN, WLC and MDM integrations. The ForeScout platform helps organizations ensure connections are appropriate and configured for compliant communications. ForeScout can take remediation action to address connection issues, including sending pop-up messages to users, alerting operations, or quarantining the device, to name a few. This helps ensure remote connections are compliant and secure at all times.
Incident Response Campus Security Operations Centers must not only provide safeguards that ensure inappropriate access to campus networks can be swiftly identified but must remediate and report breaches within 72 hours.	DFARS ((7012-c (1)(ii)) NIST 800-171 3.6.1 and 3.6.2: Establish an operational incident-handling capability for organizational systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities, and provides mapping to the relevant security controls that address incident handling, monitoring and reporting techniques.	You can automate responses to breaches and notify personnel across multiple teams through the ForeScout platform's ability to detect changes on devices and anomalous behavior in real time. This data is provided to your SIEM or integrated with your applications.

ForeScout helps government agencies at the federal, state and municipal levels meet their numerous access control and continuous device compliance requirements with an agentless, easy-to-deploy and scalable solution. The product provides these groups with continuous visibility and compliance. Government agencies use the ForeScout platform today to protect their critical network infrastructure and sensitive data, improve their risk posture, measure compliance with security policies and improve operational efficiency.

The ForeScout platform helps to protect many of the network infrastructures of the DoD as well as those of its military contractors and suppliers. ForeScout CounterACT® is NIAP Common Criteria – Protection Profile Compliant. It is included in the DoD's Defense Information Systems Agency (DISA) Unified Capabilities Approved Products List (UC APL) of those that have completed Interoperability (IO) and Information Assurance (IA) certification, demonstrating that it meets the government's high standards for security, ease of use and deployment, low end-user impact and interoperability with existing remediation solutions and infrastructure-agnostic requirements.

See The ForeScout platform offers the unique ability to see devices the instant they connect to your networks without requiring software agents or prior knowledge of the device. It sees devices other products simply can't, such as smartphones, tablets, laptops and other agency-owned and personal mobile devices as well as Internet of Things (IoT) devices, and even detects stealthy sniffer devices that do not utilize an IP address.

Control Unlike systems that tag violations and send alerts to IT and security staff, the ForeScout platform actually enforces network access control, endpoint compliance, mobile device security and threat control in one automated system. As a result, citizens, contractors and government employees can access networks without compromising security. In addition, this visibility and control platform continuously monitors devices on your network and improves the effectiveness of your security policies so you can demonstrate compliance with regulations.

Orchestrate The ForeScout platform integrates with more than 70 network, security, mobility and IT management products.* This ability to orchestrate information sharing and operation among myriad security tools allows you to:

- Share contextual insights with IT, security and management systems
- Automate common workflows, IT tasks and security processes across systems
- Accelerate system-wide threat response to quickly mitigate risks and data breaches

Network access control to protect CUI data

ForeScout offers comprehensive NAC capabilities and more based on real-time visibility of devices the instant they access the network. Our platform continuously scans the network and monitors the activity of known, company-owned devices as well as unknown devices such as personally owned and rogue endpoints. And it lets you automate and enforce policy-based network access control, endpoint compliance and mobile device security. In fact, the ForeScout platform provides an extensive range of automated controls that preserve the user experience and keep business operations running to the maximum extent possible.

Continuous firewall and device monitoring

ForeScout Extended Modules for Next-Generation Firewalls (NGFWs) enable IT teams to orchestrate dynamic network segmentation and create context-aware security policies within next-generation firewalls based on continuous device monitoring and extensive endpoint insight from the ForeScout platform. Combined solutions from ForeScout and Palo Alto Networks® or Check Point® Software are designed to detect advanced persistent threats (APTs) and indicators of compromise (IOCs). The Extended Modules feed user ID information into the NGFWs as well as exact classifications of actual devices for automated policy enforcement and threat response.

Automated compliance and assessments

ForeScout's Advanced Compliance Module automates on-connect and continuous device configuration assessment to comply with security benchmarks. It lets you leverage standards-based security benchmarks and content published in the SCAP format to:

1. Improve device hygiene for greater device security.
2. Verify system configuration settings and increase compliance against 800-171, DFARS and many other regulatory requirements.
3. Reduce usage of outdated application versions.
4. Gather and aggregate assessment results for audit preparation.
5. Streamline existing processes and automate compliance and remediation workflows.

Learn More

Government Solutions Brief

Campus Compliance Solution Brief

Continuous Compliance White Paper

ForeScout Technologies is transforming security through visibility, providing Global 2000 enterprises and government agencies with agentless visibility and control of traditional endpoints, IoT devices and operational technologies the instant they connect to the network. Our technology continuously assesses, remediates and monitors devices and works with disparate security tools to help accelerate incident response, break down silos, automate workflows and optimize existing investments. As of December 31, 2017 more than 2,700 customers in over 80 countries improve their network security and compliance posture with ForeScout solutions. See devices. Control them. Orchestrate system-wide threat response.

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

*As of December 31, 2017

[1] Beyond Uncle Sam/Analyzing the Security Posture of U.S. Government Contractors and Subcontractors https://cdn2.hubspot.net/hubfs/277648/Insights/BitSight_Insights_Analyzing_Security_Federal_Contractors.pdf?t=1518627701354&utm_campaign=Q117%20BitSight%20Insights&utm_source=hs_automation&utm_medium=email&utm_content=60575255&_hsenc=p2ANqtz-_0z9olHk3qpgNnQhxOlNyQPmlLIiMiQTPr6Ks3LCU-fr6vdfnLGhVyB-ryJQlZuqazl9cvjhhhS1wl6_Qo9VomXiw2mA&_hsmi=60575255

[2] ForeScout addresses these controls fully or partially depending on architecture, applications and dependencies. For a complete list of controls supported by ForeScout, please contact your account team.

[3] Text of DFARS 252.204-7012: Safeguarding Covered Defense Information and Cyber Incident Reporting: https://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm#252.204-7012

[4] Text of NIST 800-171 rev 1: https://csrc.nist.gov/publications/detail/sp/800-171/rev-1/final

[5] As of March 31, 2018