FORCEPOINT Supply Chain Compliance

PROTECTING CONTROLLED UNCLASSIFIED INFORMATION

FORCEPOINT
POWERED BY Raytheon

Protecting the human point.

Supply Chain Compliance Overview

All federal contractors routinely create, process, store and receive sensitive information that must be protected. In October of 2016, the U.S. Commerce Department's National Institute of Standards and Technology (NIST) released NIST SP 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations." By the end of 2017, U.S. Federal Government agencies will be required to ensure the security of Controlled Unclassified Information (CUI) in non-Federal Government systems.

The Government has developed a program designed to address deficiencies in managing and protecting CUI information by standardizing best practices for security technology and procedures. This program applies to components of nonfederal information systems and organizations that create, process, store or transmit CUI, or that provide security protection for such components. The program is critical to supporting Government missions; in particular, the missions of the war fighters who defend our nation and the tools and systems they rely on.

As a government supplier, you understand the impact of SP 800-171, and the U.S. Government's requirement to implement security technology and processes beyond standard password controls. The deadline for implementing the controls defined by NIST SP 800-171 is **December 31, 2017**.

WHY COMPLIANCE IS IMPORTANT

Many U.S. Government contractors are in the process of analyzing their current technology, to identity deficiencies and gaps with the published regulations to meet this deadline. Proper security technology and procedures are critical to companies (of any size) that seek to protect against network outages, malware/ransomware attacks and data exfiltration. Cybersecurity goes beyond protecting the information within your walls; it includes what happens during transport and while data resides with other customers or suppliers.

Meeting the requirement is not only vital to the security of our nation, but can enhance the security of your company's valuable assets and data. It helps protect your critical data on and off your network, or while transferring between networks, and can also give your company a competitive advantage over competitors who are not yet compliant.

Forcepoint Products

Forcepoint is a market leader in multiple cybersecurity categories including Web and Email Security, Next-Generation Firewall (NGFW) technology, and Data Loss Prevention (DLP) solutions. Forcepoint's unique mix of integrated solutions can help government contractors meet the NIST SP 800-171 requirements by the December 31st, 2017 deadline.

Forcepoint NGFW

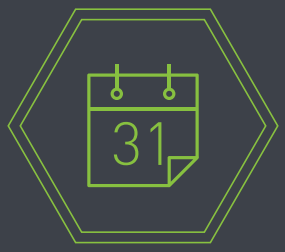
Forcepoint NGFWs connect and protect people and the CUI data they use throughout their offices, branches and the cloud—doing so with the greatest level of efficiency, availability and security. With Forcepoint NGFW, you can deploy, monitor and update thousands of firewalls, VPNs and IPSs from a single console.

Providing security without compromise, Forcepoint is a pioneer in Advanced Evasion Technique (AET) defenses and proxy technologies for mission-critical applications. Forcepoint NGFW is designed to provide maximum protection while eliminating costly network downtime, blocking sophisticated attacks and managing encrypted traffic, without hurting performance.

Forcepoint Endpoint DLP

Forcepoint Endpoint DLP protects our customers' most critical CUI data. As the #1 analyst-rated security company protecting endpoint data, Forcepoint provides your company the industry's most mature endpoint agent and fingerprinting capabilities for both Windows and Mac users.

Forcepoint Endpoint DLP protects against advanced threats by identifying encryption designed to evade DLP analysis, detects the illegitimate transmission of user credentials, as well as Drip DLP techniques that exfiltrate small amounts of data over extended periods of time. Advanced functionality allows the monitoring, blocking or forced encryption of data sent to USB storage devices.



- **NIST SP 800-171 specifies security and process controls required to protect CUI in non-federal systems.**
- **The deadline for compliance is December 31, 2017.**
- **Forcepoint can help accelerate your compliance timeline.**

The Forcepoint Solution

All of Forcepoint's cybersecurity products are designed to minimize the disruption to your corporate network both during and after installation. The Forcepoint solution includes out-of-the box, preconfigured policies to help ensure a quick and easy setup.

We offer government contractors (of any size) an affordable, preconfigured package of hardware and software tools, enabling you to quickly deploy a technical platform that will assist in addressing most of the technology controls defined by NIST SP 800-171.

Visit www.forcepoint.com/NIST800-171 for more details or call 1-800-929-0490 or email NIST800-171@forcepoint.com today to speak with a Forcepoint specialist.

ABOUT FORCEPOINT

Forcepoint is transforming cybersecurity by focusing on what matters most: understanding people's intent as they interact with critical data and intellectual property wherever it resides. Our uncompromising systems enable companies to empower employees with unobstructed access to confidential data while protecting intellectual property and simplifying compliance. Based in Austin, Texas, Forcepoint supports more than 20,000 organizations worldwide. For more about Forcepoint, visit www.forcepoint.com and follow us on Twitter at @ForcepointSec.

CONTACT

www.forcepoint.com/contact

[BROCHURE_SUPPLY CHAIN COMPLIANCE_EN] 400020.071417