

Attestation of Non-Applicability of UCR CORE Requirements to Xerox Multi-Function Devices (MFDs)

Version 1.0 (March 2026)



©2026 Xerox Corporation. All rights reserved.

Xerox®, AltaLink®, Xerox Extensible Interface Platform® are trademarks of Xerox Corporation in the United States and/or other countries. BR38616

Document Version: 1.0 (March 2026).

Contents

- 1. Introduction 4**
 - Purpose..... 4
 - Target Audience 4
 - Disclaimer 4
- 2. Attestation Letter 5**
- 3. Basis for Non-Applicability of UCR-CORE 6**
- 4. Cybersecurity Compliance is STIG-Based, NOT UCR-CORE 7**
- 5. Fax Hardware Isolation Further Supports Non-Applicability 8**
- 6. Summary Attestation 9**
- 7. Additional Information and Resources 10**
 - Security @ Xerox® 10
 - Responses to Known Vulnerabilities..... 10
 - Additional Resources 10

1. Introduction

Purpose

The DoD Unified Capabilities Requirements (UCR) 2008, Change 3 applies to all DoD-owned or controlled information systems and technologies that transmit voice, video, or data over DoD networks, including secure communication devices. It ensures interoperability, security, and performance standards for products connected to the Defense Information System Network (DISN).

Target Audience

The target audience for this document is Xerox manufacturing partners and customers concerned with IT security.

Disclaimer

The content of this document is provided for information purposes only. The performance of the products referenced herein is exclusively subject to the applicable Xerox Corporation terms and conditions of sale and/or lease. Nothing stated in this document constitutes the establishment of any additional agreement or binding obligations between Xerox Corporation and any third party.

2. Attestation Letter

Xerox® Corporation

Subject: Attestation of Non-Applicability of UCR-CORE Requirements to Xerox Multi-Function Devices (MFDs).

This letter serves as a formal attestation that Xerox® Multi-Function Devices (MFDs), are not subject to Unified Capabilities Requirements (UCR-CORE) applicability.

Place of Issue: Xerox Corporation
Address: 800 Phillips Road Webster, NY 14580
Issued by: Xerox Cybersecurity
Date of Issue: 8/04/26

Signature Authority:  Justin R Denton
Director of Governance, Risk, and Compliance

3. Basis for Non-Applicability of UCR-CORE

Following the Department of Defense (DoD) announcement of the sunset of the DoDIN APL program on September 30, 2025, with all APL testing concluding by December 31, 2025, DISA confirmed that interoperability validation is transitioning to UCR CORE only for Unified Capabilities (UC) systems, with enforcement beginning in FY 2026.

UCR CORE applies specifically to Unified Capabilities systems—voice, video, conferencing, messaging, and other real time communications technologies.

Xerox® MFDs do not provide UC services and therefore fall *outside* the scope of UCR CORE enforcement requirements.

Accordingly:

Xerox® MFDs are categorically not Unified Capabilities (UC) products and therefore are not subject to UCR CORE interoperability requirements.

4. Cybersecurity Compliance is STIG-Based, NOT UCR-CORE

DISA's APL Sunset Notice confirms that cybersecurity validation now transitions to the DISA Vendor STIG program, replacing the APL cybersecurity certification process.

As such:

- Xerox® MFD deployments map to the Multifunction Device & Network Printer STIG (or relevant SRGs).
- Xerox® will provide the STIG mapping and required security artifacts as part of the RMF package.

5. Fax Hardware Isolation Further Supports Non-Applicability

Many Xerox® MFDs include optional analog fax modules.

These modules:

- Operate on physically and electrically isolated circuitry
- Have no interaction with the IP based print/scan network functions
- Do not process, generate, or terminate UC voice/video signaling

Because the fax subsystem is a wholly separate, analog switched component, it cannot participate in IP based UC functions that UCR CORE governs.

Therefore:

The presence of an analog fax card does not introduce any UCR-CORE relevant functionality and does not alter the device's non-UC classification.

6. Summary Attestation

Based on the DoD CIO and DISA guidance:

- UCR-CORE applies only to Unified Capabilities systems.
- Xerox MFDs are not UC systems.
- Xerox MFDs remain outside the scope of UCR-CORE interoperability requirements.
- Cybersecurity compliance is satisfied through Vendor STIG requirements, not APL or UCR-CORE.

Thus, we formally attest:

Xerox® Multi-Function Devices are not impacted by UCR-CORE requirements and require no UCR-CORE testing, evaluation, or contractual interoperability validation.

7. Additional Information and Resources

Security @ Xerox®

Xerox maintains an evergreen public web page that contains the latest security information pertaining to its products. Please see <https://www.xerox.com/security>

Responses to Known Vulnerabilities

Xerox has created a document which details the Xerox Vulnerability Management and Disclosure Policy used in discovery and remediation of vulnerabilities in Xerox software and hardware. It can be downloaded from this page: <https://www.xerox.com/information-security/information-security-articles-whitepapers/enus.html>

Additional Resources

Below are additional resources.

Security Resource	URL
Frequently Asked Security Questions	https://www.xerox.com/en-us/information-security/frequently-asked-questions
Common Criteria Certified Products	https://security.business.xerox.com/en-us/documents/common-criteria/
Current Software Release Quick Lookup Table	https://www.xerox.com/security
Bulletins, Advisories, and Security Updates	https://www.xerox.com/security
Security News Archive	https://security.business.xerox.com/en-us/news/
Xerox Zero Trust Security	https://www.xerox.com/en-us/about/security-solutions/zero-trust-security