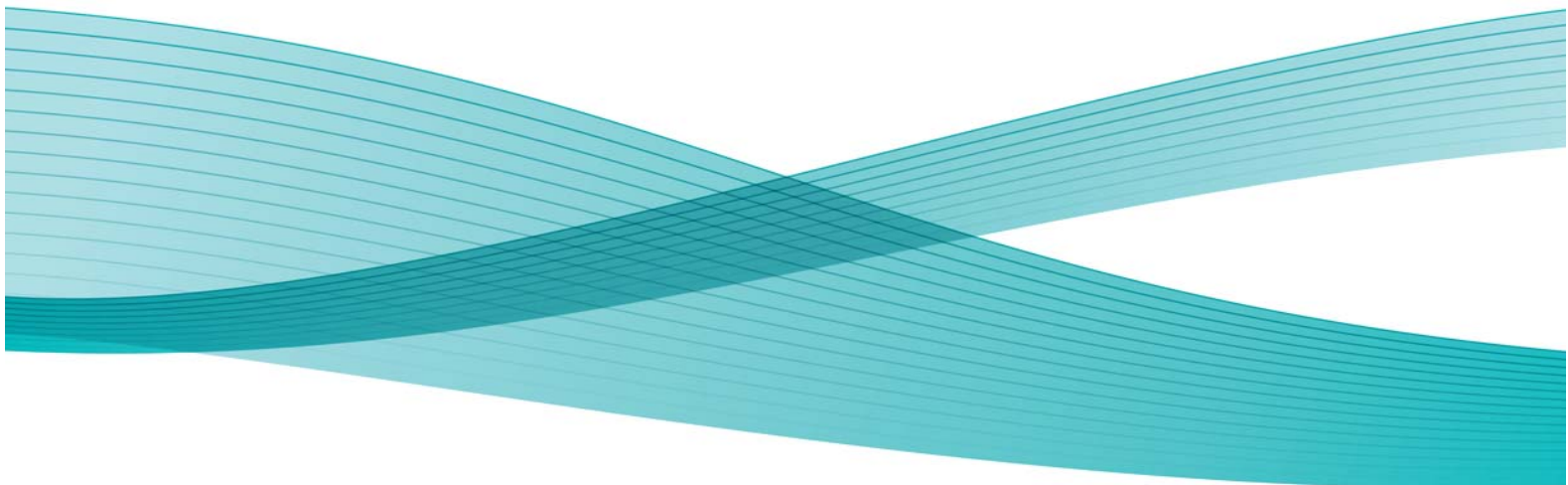


# Delivering Security for the Print Environment

Holly Turner, PMP  
Certified Lean Six Sigma Black Belt



This page intentionally blank

## The Challenge

A major US government customer needed to refresh their print environment. Seventeen (17) campus locations across the United States from Florida to California needed coverage. The customer maintains a high-security deployment environment with several unique constraints, including:

- Campuses are co-located on military bases
- Ongoing attempts at infiltration by agents of foreign governments to obtain technology secrets
- Facility access restricted to US citizens
- Continuous audit for compliance to security policy
- Atlantic hurricanes pose a physical threat

The user community asked for new capabilities for copy, print, fax, and scan supported by multi-function devices (MFD). Color printing was also needed. Management looked for a turnkey solution to offload responsibility for the printers and reduce costs. A number of vendors were competing for the contract, but the winner would need to demonstrate capability to delivery services securely.

The customer asked for a Security Plan. The security plan needed to be comprehensive covering all technology, processes, and personnel that Xerox would provide as part of a managed services solution.

## The Solution

Xerox has a multi-pronged approach to security comprehending people, standards and technology.

### The People

First, a professional team is assembled:

- A dedicated Security Analyst to be the single-point-of-contact for the customer and responsible for maintaining services security
- Certified Information System Security Professionals (CISSP) to review security requirements in many disciplines such as physical, encryption, network, and business recovery.
- Certified Security + technicians to execute security tasks including configuring device and tool settings to harden them for network installation
- Certified Lean Six Sigma Black Belt to analyze and deliver solutions for any security barriers identified

### The Standards

Best Practice methodologies are followed. Xerox Security is based on the ISO27001 Code of Practice for Security. The customer was using NIST SP 800-53 standards. The two standards were mapped line-by-line to ensure that operations would comply with the customer standard. Documentation for all field services processes was assembled for a security review.

## The Technology

Xerox selected devices which were certified for ISO15408 (Common Criteria) and supported many security features:

- Fax/Network Separation
- Network Authentication
- Secure LDAP, SSL, IPSec, SNMPv3
- Image Overwrite
- Disk Encryption
- Internal Firewall
- Auditing
- Two-factor Common Access Card (CAC) support

The team initially focused on identifying and documenting all of the security requirements of the customer. In addition to review of the NIST standards, internal procedure requirements had to be considered. Each campus location had unique security requirements depending on activities at that location. Workshops at each location engaged the print manager, local security officer, contract officer, and often the IT managers and administrators. Xerox has many years of experience working with Federal customers, the military, and defense contractors and can 'speak the language' of these critical stakeholders.

## The Plan

Xerox customized a Security Plan for this customer based on the ISO27001 standard. The plan considered all components of onsite security including annual policy review, asset management, HR regulations, physical and environmental considerations, communications and operations management, maintenance, incident management, business continuity, and compliance. The Security Plan needed to be in place before the first Xerox equipment was delivered and installed. One key element of the plan was the definition of the secure state for each device model hardening it for installation on the customer network.

## Deployment

The Plan was reviewed with customer stakeholders and Xerox field resources. A Project Plan was built to identify all the delivery tasks required by the variety of customer environments.

- Assignment of a dedicated Xerox Security Analyst
- Device checklists to 'harden' configuration settings for the network
- Document the planned secure state for each device
- Technician training on secure procedures for each campus
- Xerox tools for remote management (e.g., password resets, software upgrade)
- Audit plan for controls

## Deployment (continued)

Like most projects, once the plan was in place the actual on-site installations proceeded smoothly. Progress was monitored and coordinated with the customer through weekly meetings with the Xerox Security Analyst in attendance.

After a few months, the account reached steady-state. Did the Security Analyst exit?

No, Xerox is on board to provide security for the life of the contract. The Security Analyst continues to meet with the team each week to address any security concerns or incidents.

## The Results

- All security audits passed to date
- 95% of devices in secure state
- No violations of customer facility policies
- No security incidents resulting in the loss or compromise of data

The Xerox Security Analyst continues to serve as the customer Single Point of Contact for security concerns. The Security Plan is reviewed on an annual basis which includes documenting and mitigating any new risks. Secure operational processes are followed for device install, upgrade, service and disposal. Training materials are in place to ensure continuity as Xerox and customer resources transition over time. Xerox collaborates with the customer to assess risk, mitigate, and update the Security Plan as needed over the life of the contract.

## The Standards

**ISO27001 - ISO/IEC 27001:2005** - Information technology - Security techniques - Information security management systems. an information security management system (ISMS) standard published in October 2005 by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

**NIST SP 800-53** - The National Institute of Standards and Technology Special Publication (NIST SP) 800-53 Revision 2 provides guidelines for securing information systems within the federal government by selecting and specifying security controls.

**ISO15408** - The Common Criteria for Information Technology Security Evaluation (abbreviated as Common Criteria or CC) is an international standard (ISO/IEC 15408) for computer security certification. It is currently in version 3.1. Common Criteria provides assurance that the process of specification, implementation and evaluation of a computer security product has been conducted in a rigorous and standard manner.