SECURING THE PUBLIC TRUST:

A LAYERED APPROACH TO DEVICE AND DOCUMENT SECURITY IN THE GOVERNMENT LANDSCAPE

The modern government landscape is defined by complex networks of connected people, processes, and technology. As advanced persistent threats continue to evolve and cyberattacks increase at an alarming rate, the public sector remains a prime target for malicious actors.

While IT departments invest heavily in securing traditional network perimeters, networked endpoints—such as multifunction printers (MFPs) and scanners—can become vulnerabilities if not properly hardened. Because these devices process and transmit sensitive, classified, or personally identifiable information, breaches involving paper or digital documents can be just as damaging as traditional electronic data theft.

Developing an effective security posture requires a holistic approach that balances human factors, enforceable policies, and advanced technology. For government agencies at the federal, state, and local levels, this means adopting a layered defense strategy that rigorously aligns with strict statutory mandates while addressing the resource constraints of public sector IT teams.

NAVIGATING GOVERNMENT MANDATES AND REQUIREMENTS

Public sector IT environments operate under strict regulatory and statutory compliance frameworks designed to help protect national security and citizen data. Establishing a secure infrastructure requires adherence to several critical mandates:

Homeland Security Presidential Directive 12 (HSPD-12): HSPD-12 requires a standard, secure, and reliable form of identification for federal employees accessing federally controlled facilities and information systems. For networked endpoints, this necessitates two-factor authentication solutions, such as the use of Common Access Cards (CAC) or Personal Identity Verification (PIV) cards. By implementing embedded, serverless authentication applications, agencies can help ensure that device functions remain locked until a user inserts their government-issued card and enters their PIN. This actively verifies their identity and security classification against a Public Key Infrastructure (PKI) and Active Directory, helping to satisfy stringent Department of Defense and civilian agency requirements.

Hardcopy Device Protection Profile (HCD-PP) and Common Criteria: The Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408) is an internationally recognized standard for evaluating IT security. Within this framework, the HCD-PP (Hardcopy Device Protection Profile) serves as the standard procurement requirement for the U.S. and Japanese governments when acquiring digital multi-function devices. HCD-PP rigorously evaluates cryptographic key management and helps secure that generated random numbers possess sufficient entropy to help provide a critical security baseline for device procurement.

FIPS 140-3 Validation: The Federal Information Processing Standards (FIPS) outline the requirements for cryptographic modules protecting sensitive information. Government devices must utilize hardware and software cryptographic engines that comply with the FIPS 140-3 Level 2 standard. This helps ensure that data at rest and data in transit—including digitally signed emails, encrypted file attachments, and solid-state drives—are protected by robust, government-validated cryptographic algorithms.

THE CRUCIAL ROLE OF FEDRAMP AUTHORIZATION IN CLOUD WORKFLOWS

As government agencies increasingly adopt cloud-based workflows and managed print services, ensuring the security of these cloud environments is critical. The Federal Risk and Authorization Management Program (FedRAMP) promotes the adoption of secure cloud services across the U.S. government by providing a standardized approach to security assessments for cloud service offerings. Built on the guiding principle of "do once, use many times," FedRAMP helps save agencies significant time, money, and effort by eliminating redundant security assessments.

When evaluating cloud-based print management and device management services, agencies should mandate solutions that have achieved FedRAMP authorization at the Moderate impact level. The Moderate impact level accounts for the majority of authorized cloud service offerings and is required for systems where the loss of confidentiality, integrity, or availability would result in serious adverse effects on an agency's operations, assets, or individuals. Utilizing a FedRAMP-authorized service means the system has met all continuous monitoring requirements and is already validated against a known set of rigorous security standards.

Furthermore, government document workflows often require secure integration with third-party cloud storage. Agencies must ensure that their networked endpoints allow users to securely scan documents directly to FedRAMP-authorized cloud destinations. For the most sensitive data, it is critical that these services explicitly support scanning to and printing from the Government Community Cloud (GCC) High environment—including platforms like Microsoft's SharePoint Online, OneDrive, and Exchange Online.

AUGMENTING DEFENSE WITH MANAGED SECURITY SERVICES

Even with stringent mandates and secure cloud workflows in place, government IT departments frequently face budget limitations and personnel shortages. Securing an organization can be a complex task that requires professional subject matter experts, stakeholders from different lines of business, and an exhaustive risk assessment. To bridge this gap, public sector organizations can benefit from leveraging Managed Security Services to evaluate readiness, mitigate vulnerabilities, and respond to incidents.

Consulting and Vulnerability Management
Agencies can confer with expert consultants who help evaluate the organization's readiness to mitigate data breaches, prepare for compliance audits, and qualify for cybersecurity insurance policies. Beyond policy consulting, organizations should utilize Managed Vulnerability Services to perform comprehensive internal and external assessments, systematically scanning the entire infrastructure to identify gaps in the security posture.

Penetration Testing
To validate host and network configurations, proactive penetration testing is vital. Managed security experts can conduct internal and external testing designed to exploit existing vulnerabilities, assessing the true resilience of an agency's email systems, firewalls, routers, VPN tunnels, web servers, and networked endpoints.

Comprehensive IT and Security Suites
For a truly holistic approach, agencies can deploy complete managed IT and security suites. These managed services extend beyond basic monitoring to provide Account Management and Governance, Next-gen Antivirus, and Extended Detection and Response capabilities (including SIEM and SOAR). Crucially, they also incorporate Dark Web Monitoring, Automated Threat Response, and human-centric defenses such as continuous Security Awareness Training and Phishing Testing Programs to help ensure that employees remain the strongest line of defense.

THE CIA TRIAD AND THE SHIFT TO SERVERLESS ARCHITECTURE

An effective government security posture is founded on the CIA Triad formulated by the National Institute of Standards and Technology: **Confidentiality** (preventing unauthorized disclosure), **Integrity** (ensuring data is not tampered with), and **Availability** (ensuring timely access to authorized users).

To operationalize these principles efficiently, many agencies are moving toward serverless document distribution. Shifting hosting, processing, and storage directly onto a single, embedded multifunction device helps eliminate the need to invest in and support costly dedicated application servers. From a security standpoint, serverless technology is highly beneficial: it helps remove a potential point of failure, ensure high availability for mission-critical workflows, and significantly reduce the network attack surface that adversaries could otherwise target.

BEST PRACTICES FOR HARDENING THE INFRASTRUCTURE

To defend against highly motivated adversaries, agencies must secure every stage of the document lifecycle—from the initial print or scan command to the final network transmission.

1. Device Security and Hardware Resilience
Endpoints must be fundamentally hardened against malware intrusion and firmware tampering. Best practices include:

- **Verify System at Startup:** Utilizing the hardware as a "Root of Trust" to automatically verify that the boot process, operating system, firmware, and embedded applications have not been altered by malicious third parties before the device initializes.
- **Platform Firmware Resilience:** Implementing automatic recovery mechanisms that can restore a device using a secure backup program if an unauthorized modification is detected.
- **Application Whitelisting:** Utilizing dynamic embedded controls to help ensure that only authorized, known programs contained in a dynamic whitelist can execute. This is designed to block malware, spyware, and unauthorized rewriting of software modules.

2. Secure Document Distribution and Information Control
Controlling how users transmit, receive, and retain information is paramount. Agencies must implement stringent controls:

- **Advanced Authentication Protocols:** In addition to CAC/PIV, agencies should support multi-factor authentication like RSA SecurID Tokens and One Time Passwords (OTP). This requires users to enter an RSA passcode alongside their Active Directory credentials, providing an additional level of security for scanning and sending critical information.
- **Restricted Scan Workflows:** To help prevent misdirected information, organizations can lock down scanning capabilities so that authenticated users can only send documents to pre-approved destinations or strictly to their own email address ("Send to Myself").
- **Document Sanitization and Preview:** Before transmission, users should be required to preview scans and utilize automated blank-page removal to help ensure that only the intended, accurate information is distributed.
- **Universal Design without Compromising Security:** Security mandates must not hinder productivity for visually impaired employees. Implementing voice-operated assistant applications with security features allows users to perform basic copy, print, and scan workflows via voice commands while remaining within the authenticated environment.

3. Network Communication and Continuous Auditing
A zero-trust mindset dictates that no endpoint is inherently trusted. Network communications must be protected by robust protocols such as IEEE 802.1X, which establishes a closed point-to-point connection only after authenticating the network device, preventing unmanaged systems from connecting to the infrastructure.

Furthermore, data exchanges should be safeguarded using IPSec to encrypt inbound and outbound traffic at the network level, and TLS 1.3 to help prevent data tampering during transit.

Finally, continuous monitoring and auditing are foundational to government compliance. Organizations must configure endpoints to capture detailed audit logs—including user authentication status, document transmission records, and IPSec failures. By integrating these endpoints with external Security Information and Event Management (SIEM) systems via standard Syslog protocols (RFC 5424), IT security analysts can gain real-time visibility into their environment. This integration enables the rapid detection of anomalies, root cause analysis of incidents, and proof of compliance during regulatory audits.

CONCLUSION

In the public sector, securing the workplace is a constant practice of due care and due diligence. There is no such thing as "security through obscurity". By adopting a layered defense strategy that prioritizes Managed Security Services, FedRAMP-authorized cloud platforms, serverless distribution, robust identity management, cryptographic standards, and continuous auditing, government agencies can successfully protect their physical and digital assets.

Ultimately, compliance with federal mandates is not just a regulatory checkbox—it is a foundational requirement for securing the public trust.

Canon

1-844-50-CANON | usa.canon.com/business

06/26-0888-15631