Business white paper

Managing security risks

Information security for defense agencies: secure your printing assets to protect sensitive and private data

Table of contents

It is becoming increasingly essential for IT professionals to keep ahead of the changing nature of the information security landscape. One threat vector in particular that is often overlooked is the potential for unauthorized access to the network of printing and imaging devices found throughout defense agencies.

Introduction

The advancement and proliferation of information technology, Web 2.0 and social media, and an "instant-on, always-on" digital world have created an explosion in the amount of personal and non-personal information stored, processed, shared, and transmitted. The growth in information is mind-boggling, according to several sources. IDC estimates that from 2005 to 2020, the digital universe will grow by a factor of 300, from 130 exabytes to 40,000 exabytes, or 40 trillion gigabytes (more than 5,200 gigabytes for every man, woman, and child in 2020). From now until 2020, the digital universe will about double every two years.[1] Governments' ability to appropriately regulate and protect sensitive and private data increases in difficulty almost day over day due to this accelerated proliferation in the volume and breadth of communication channels.

Defense agencies in particular feel this strain. Even as the demand for increased mastery of the information explosion is accelerating, the resources with which to develop effective processes are shrinking. Budgets and staffing are affected by the global economic crisis. Agencies must still meet the new demands of complex missions all over the world, provide rapid response to a widening scope of military and political actions, deploy technologically advanced tools such as shared and cloud services, and acquire the skills to use those services. It is a daunting task for those charged with securing government information technology infrastructure: repelling attacks, protecting data, preserving privacy—while ensuring that the policies necessary to do so are understood and practiced by all employees—and it takes unprecedented vigilance. All of this must be done while simultaneously demonstrating the efficiency of the processes to constituent and budget panels overseeing each agency.

The intent of this white paper is to assist government defense agencies that are prime targets for infiltration and attack through an increased understanding of the changing nature of the threat landscape. One threat vector in particular that is often overlooked is the potential for unauthorized access to the network of printing and imaging devices found throughout these agencies. Often misunderstood, today's modern printer fleets are powerful, network-connected devices with computing capabilities on a par with servers and personal computers. If left unprotected, printers and imaging devices, their network infrastructure, and the sensitive data passing through them are vulnerable to attack or theft by any number of means, including cyber terrorists, hacktivists, criminal syndicates, and even disgruntled insiders with a counter-agency agenda in mind.

This paper will expose six major security risks within printers and printing networks, and demonstrate how these devices can be secured using greater automation and secure information workflow technology. By addressing these six areas of exposure, today's overtaxed agency IT resources can contribute to the overall security of the agency even in the climate of today's unparalleled information explosion.

[1] IDC Digital Universe Study, sponsored by EMC, December 2012.

Defense agencies must balance openness with security to manage risks

The U.S. Government Accountability Office (GAO) report found a 650% rise in information security incidents over the past five years, including infections from malicious code; violations of use policies; unauthorized access into networks, applications, and data; and scams, probes, and attempted access. Ongoing weaknesses in information security policies and practices were found in all 24 major U.S. federal agencies.[2] Defense agencies are obvious targets as they harbor vast amounts of sensitive and confidential military and national security intelligence. But despite the strong alignment of people, processes, and technology to safeguard information assets, the attackers continue to make the headlines:

- "European Union under cyber attack as major summit begins," by Per Nyberg, CNNWorld, March 24, 2011
- "Over 24,000 sensitive military files were stolen by foreign intruders, Pentagon admits"—Infosecurity, July 24, 2011
- "China suffered a half million cyberattacks last year, says government"—Infosecurity, August 10, 2011

The insider threat

Organizations face significant consequences from internal incidents, including financial implications, reputation damage, and/or theft of sensitive or confidential information. Yet, insider fraud remains a high risk for organizations, mostly because they fail to implement sufficient resources to prevent or quickly detect insider fraud:[3]

- More than 75 percent of the respondents indicated that privileged users within their own institutions had or were likely to turn off or alter application controls to change sensitive information—and then reset the controls to cover their tracks.
- Eighty-one percent replied that individuals at their institutions either had used or were likely to use someone else's credentials to gain elevated rights or bypass separation of duty controls.
- On average, respondents noted that their organizations experienced more than one incident of employee-related fraud per week—about 53 in a year's time. Twenty-four percent of respondents indicated that their organizations experienced more than 100 incidents in the past 12 months.
- Once an incident has occurred, it takes organizations an average of 89 days to discover it and an additional 96 days to uncover the root cause and determine the consequences to the organization.
- A majority of respondents—or 62 percent—were unable or unsure of their ability to assess the financial impact and true costs of fraud.
- Approximately two-thirds of internal fraud investigations do not result in actionable evidence against the perpetrators, meaning a majority of the incidents go unpunished and leave organizations vulnerable to additional incidents.

On the heels of the Wikileaks Cablegate scandal in 2010, the White House issued an executive order to issue sweeping new cybersecurity policies to protect classified information.[4] New interagency governing bodies were formed to oversee the protection of classified information across federal agencies and departments, and balance the needs of federal users that have permission to access it.

For sensitive information to be fully secure, it needs to be proactively managed throughout its entire lifecycle. This includes not only how data files are protected at rest as they reside on servers or personal computers or are in motion as they transfer within a network, but also how information is managed during the scanning and printing process—in the "on-ramp" and "off-ramp" endpoints. Even if an agency has the right processes and technology in place for the other stages of the lifecycle, safe policies and procedures must be in place for these devices as well, where critical access and, therefore, exposure resides in the interaction with employees. For IT security professionals, employees can be either the greatest asset or biggest liability in pursuit of managing information risks. So, reasonable caution must be taken to block preventable exposures.

[2] "Information Security: Weaknesses Continue Amid New Federal Efforts to Implement Requirements," United States Government Accountability Office Report to Congressional Committees, October 2011.

[3] Attachmate Corp. and Ponemon Institute, "New Ponemon Research: Insider Fraud is Common and Often Flies Under Corporate Radar," September 2011 (attachmate.com/Press/PressReleases/sep-22-2011.htm).

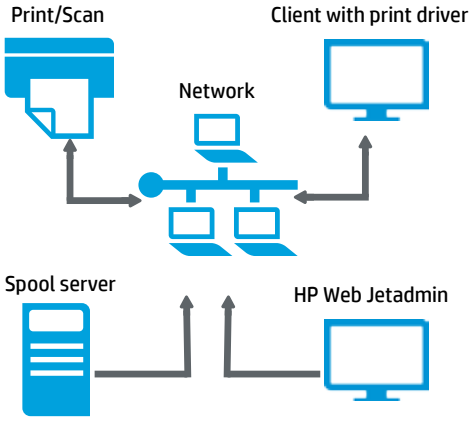
[4] InformationWeek, "Feds Tighten Cybersecurity Policies to Stop Insider Threats," by Elizabeth Montalbano, October 7, 2011.

Securing an imaging and printing infrastructure is impacted by technological innovations

Traditional security

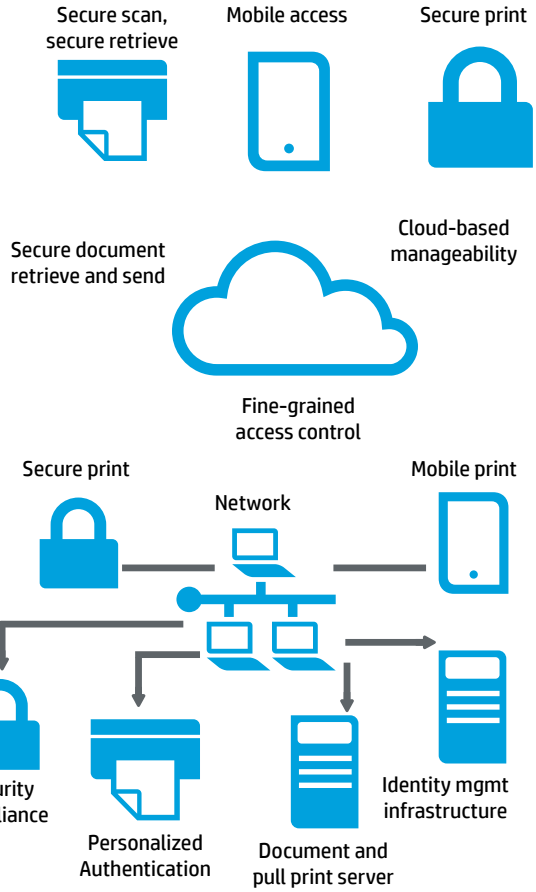
- Isolation approach
- Device- and user-centric security

Very limited outside access to protect assets



Security and the cloud

- Ubiquitous, secure access to government assets in enterprise and cloud
- Web-powered—new document workflow models
- Document-centric security



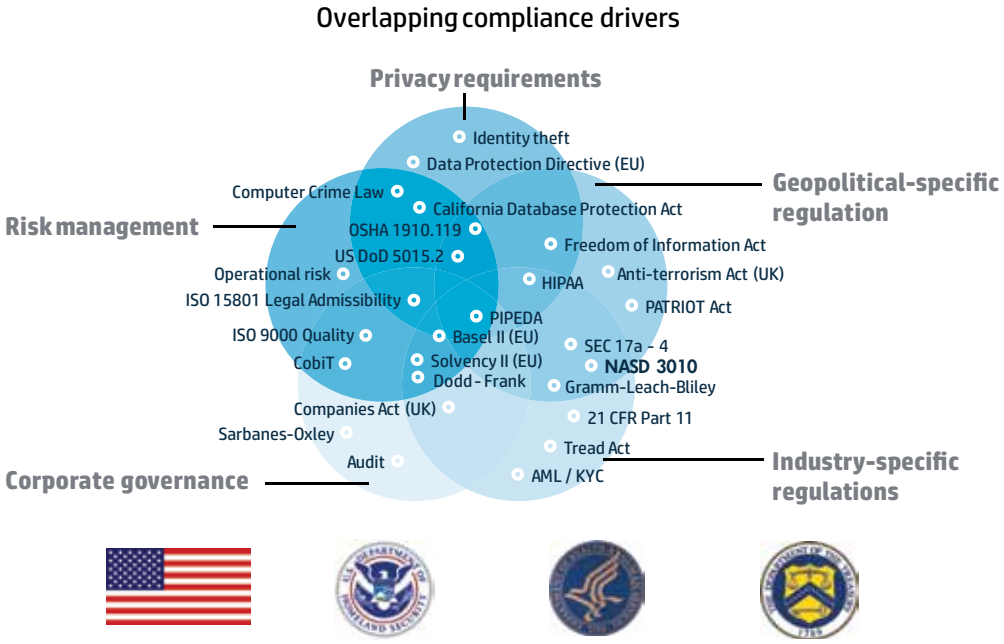
Defense in depth: layering security throughout the information lifecycle

Virtually all government installations use a "defense-in-depth" model where multiple security countermeasures or multiple layers are used to protect the integrity of information assets. "Defense in depth" minimizes the probability that a cyber attack will succeed. Plus, it provides redundancy should a control fail or should vulnerability be exploited, so it can cover aspects of personnel, procedural, technical, and physical measures. These mechanisms, procedures, and policies are intended to increase the dependability of an IT system and buy time to detect and respond to an attack.

This approach starts with physical security such as door locks, smartcard and ID badge validations, metal detectors, surveillance systems, and even the presence of security guards. The next step is to lockdown networks, servers, and endpoint devices with security solutions such as firewalls, intrusion detection and prevention, and antivirus software; this will prevent or minimize damage from malicious or accidental intrusions at various points of vulnerability. The approach then applies security on the application and data file level to help ensure another level of protection.

As seen in the diagram above, securing the printing infrastructure is impacted as much by technological trends as is the rest of the network. Layering security is even more critical as organizations adopt cloud and virtualized environments.

Understanding compliance is crucial to making the right information security decisions. But with upwards of 20,000 compliance requirements globally, and many overlapping, this is no small task.



How many print jobs are currently sitting at the printer? Have you ever sent a job to a printer and then forgotten to pick it up—or mistakenly picked up a previous print job that wasn't yours? How many times have you noticed a printed document at the printer with either confidential or personal, non-business-related material?

Six inherent risks with printing and imaging devices

According to a Government Technology survey, 81 percent of respondents reported having an IT security plan in place. Of these respondents, 68 percent claimed printers as part of their planning, but 60 percent on average could not identify how printing devices were actually secured.[5] It appears that a large gap exists between perceived and actual security of printers and other imaging devices. Researchers found that many of those surveyed believed their printers were as secure as their own PCs. It was also determined, however, that most office workers did not realize the inherent risks and vulnerabilities of either their network-connected printing devices or their printing process and, in most cases, they were unaware of both.

In May 2009, realizing that printers and imaging devices are at risk of attack and abuse, the IEEE Standard for a Protection Profile in Operating Environment A, or P2600, was ratified. This standard established a protection profile for hard-copy devices such as printers, multi-function printers (MFPs), scanners, and fax machines, among others.

Moreover, despite broad participation by manufacturers to establish baseline security for their devices, it appears government agencies with much to lose are not heeding the call. Failure to protect network-connected devices against an escalating war with cyber terrorists and malicious insiders is an extremely risky proposition. Following are six major risks and exposures with printers and other imaging devices that warrant close inspection:

Risk #1—Printed hard copies

One of the most common printing security risks involves printed hard copies where an employee will request a print job and delay or forget to pick it up. A document containing sensitive or confidential information that sits idly in the paper tray or elsewhere for any length of time is a security risk. Spying on a printed document can be inadvertent or deliberate. That same document also can be taken by an employee or a visiting contractor or guest, who can then easily transport it out of the office.

[5] "Understanding the Risks: Government Technology IT Security Survey," Government Technology, August 2011.

Is there sensitive information stored on your printers' hard drives? Do you ever send your printers or MFPs out for repairs? When a printer is retired, do you know how each printer's hard drive is sanitized or disposed of? Do you have a certificate of verification of each device disposition for future audits?

Do you know if all or part of the data in your print jobs is encrypted? Is it possible for you to intercept or re-route a print job as it travels over the network to a printer? What is a man-in-the-middle attack, and should you care?

Example: A city in the United Kingdom distributed personal information accidentally after a print job mix-up. A document with personal information was inadvertently mixed in with other documentation. Both documents were printed on the same shared printer, and the documents were not checked before being mailed.—Infosecurity, "City…falls foul of data protection act following printer mix-up," April 5, 2011 (first published in Computer Weekly).

Risk #2—Data on printer hard disks

Unknown by many, today's modern printers and MFPs contain hard disks similar to servers or personal computers. Printer hard disks store material such as passwords, routing information, address books, identification data, and confidential information as well as thousands of print jobs that can be stored for years. Although layered security policies apply to all network-connected devices, printers are often overlooked. A malicious attack could just as easily target an unprotected printing device as a PC or server and compromise data. To exacerbate the risk, printers can be removed to an offsite location for repair, resale, or demolition—with the hard disk intact and data exposed to whomever accesses the device.

Example: A healthcare insurance provider suffered a data breach in 2009 that involved the theft of 57 hard drives. Initially, it was unclear what was on the drives. It turned out that almost one million customer records with sensitive data were included. Over the last two years, the insurer spent approximately $6M to encrypt 885 terabytes of mass data storage equivalent to almost 35,000 single-layer Blu-ray discs, and locked down over 1,000 Windows®, AIX, SQL, VMware, and Xen server hard drives and approximately 6,000 additional workstation and removable drives and nearly 136,000 volumes of backup tape.
—InformationWeek, "[Insurer] Encrypts All Its Data" by Neil Versel, August 1, 2011.

Risk #3—Print jobs sent over the network

Print jobs are usually sent from a computer to the printer via the network. Layered security ensures the network is secured with firewalls and other security software to protect communications between servers and endpoint computers. But what about the data communications between a computer and a printer? Many organizations do not apply encryption to print jobs, making it easy to snag a print job as it travels over the network to a printer. Sniffer tools easily obtained through the Internet are used to intercept print jobs. A man-in-the-middle attack can re-route print job information to a laptop first before it continues on to a printer, thus allowing a perpetrator to view the data before it goes to the printer. All communications on an agency's network need to be encrypted—inclusive of print jobs.

Example: Since a cyber attack in August 2011, an industrial manufacturer in Japan acknowledged that data on defense equipment may have been leaked. A statement confirmed the "unintended transfer of some information on the company's products and technologies between servers within the company." Previous news reports cited 83 servers and computers across 10 facilities were infected with a virus and indications that data on defense equipment and nuclear power plants had been compromised and data transmitted to external destinations. It's possible an email with an infected attachment automatically connected a recipient's computer to a U.S. website involved in the attack.—"[Manufacturer] acknowledges possible defense data leak," Asahi Shimbun, October 26, 2011 and "Cyber attack probe centers on defense industry group," Asahi Shimbun, October 17, 2011.

Does your printing system reliably arbitrate the access to print jobs based on user roles and device limits? Does your agency have set guidelines in regards to what employees can and cannot access? Are printers monitored both physically and/or by video?

Are your office printers used for highly sensitive jobs such as logistical and troop deployment plans, troop movements, or administrative functions such as check printing or filling prescriptions? Do you know who controls special papers and media? Would you be able to find out whether a document has been forged or altered?

Do you know how many printers, MFPs, servers, scanners, and computers make up your office printing system? Do you know your agency's policy or guidelines in regards to how printers are controlled and maintained? Are the printers placed in locations that are acceptable for printing all levels of classification?

Risk #4—Controls and access to printers

Today, there is no such thing as a "dumb" printer or MFP such as was found in the days of "dumb" terminals. Today's imaging and printing devices are incredibly sophisticated with intelligence, memory, and operating power on a par with a computer. Yet access to the printers and their control settings is rarely restricted. In most offices, employees and even outside contractors are free to walk right up to an MFP and print, fax, email, or copy any document they choose. If any controls are enacted, it's for charge-back capability, not security. With some devices they can even access network servers, exposing still further data upstream. A disgruntled insider with the right technical acumen can enter their own email and "spoof" the printer device, which opens up the possibility of a virus-laden email to appear as a legitimate company communication to the recipient.

Example: A Chinese scientist pleaded guilty to economic espionage in connection with the theft of trade secrets via print devices at his former employer to benefit a university in China. "[The former employee] used his insider status at two of America's largest agricultural companies to steal valuable trade secrets for use in his native China," said the U.S. Attorney General. Financial losses are estimated at $7 million USD. A spokesperson said the company would be strengthening security measures to protect its technology. The former employee faces a maximum prison sentence of 25 years.—"...Scientist Admits to Economic Espionage, U.S. says," by Andrew Harris, Bloomberg News, October 18, 2011.

Risk #5—Tampering and fraudulent activity

As stated above, printing systems are at risk from the tampering and fraud of insiders. In-office printing systems are often used for special print jobs such as check printing, prescriptions, patient wristbands, and other special-purpose activities. An unprotected printer makes it too easy for an insider to commit a fraudulent act. An employee with a grudge and access to special paper and media can print forged checks, write new prescriptions, or alter them with new names, quantities, or dosages. They can make changes to other sensitive documents right on one of the official internal printers.

Example: An insider at a major bank sold customer data to a criminal crime ring that used the information to commit fraud. Names, addresses, Social Security numbers, phone numbers, bank account numbers, driver's license numbers, birth dates, email addresses, and the like were stolen. Security filters like mothers' maiden names, PINs, and account balances were among the data given to outsiders.—Computerworld, "Insider data theft costs...$10 million," by Robert McMillan, May 25, 2011.

Risk #6—Fleets of printers, networks, and users elevate risk

In the real world of a government agency, there isn't just a handful of individual printers, but a fleet of hundreds and even thousands of printers, MFPs, servers, computers, scanners, and fax machines that comprise the organization-wide printing system. The risks are compounded many times over if printer security and management is not applied. Although a large fleet is best controlled and managed centrally, many organizations have not implemented this. It is also likely that these same organizations are not maintaining records or audit trails of printer activity, nor do they have a clear way to identify security threats across their printer fleet.

Example: A celebrated police service experienced a "major network issue" that prevented staff from using a number of services, including print services and system access for some staff and officers. With a portion of the computer system offline, some checks were hindered. "Information leakage" by certain print servers is suspected as the cause for the outage, and not a deliberate attack.—"...Police confirms ICT outage but plays down attack fears: Two weeks of IT woe for cop staff," by Paul Kunert, The A Register, June 20, 2011.

HP print security solutions and best practices

HP has been studying the print security challenge for many years. As the world's largest IT company with the largest security practice that is NIST certified, HP Imaging and Printing also has #1 market share in virtually every printing category it's in, and is a trusted partner to approximately 300 government agencies in more than 30 countries. With more than four decades of unsurpassed domain expertise and experience, HP print solutions are adapted to the specific needs of individual government agencies so that agencies can safely and affordably share information and reduce security risks. Here's how HP printer solutions are designed to address the six major printer security risks:

Employee authentication and pull printing: addressing risk #1—printed hard copies

HP pull printing solutions consist of an employee verification system designed to keep printed hard copies from falling into the wrong hands. When an employee sends a print job to a printer, the job is not immediately printed, but instead it is stored on the server until the employee authenticates him- or herself successfully to the device. The security module is connected to, or embedded in, the printer. The print job is then "pulled" from the server. Any number of HP authentication options can be used that leverage an agency's preference:

- Personal identification numbers (PINs)
- Proximity ID badges
- Smartcards or magnetic cards

A special feature of the modular HP pull printing system is HP Access Control (HPAC) authentication. HPAC allows agencies to incorporate authorization, authentication, audit, and job accounting processes into the printing infrastructure, supporting information security across the organization for all print-related procedures.

For greater accessibility, HP Managed Print Solutions allow the ordered print job to be pulled from the HP Output Server, where it's encrypted, and then sent to any connected printer. No matter where the job originates from or where it is finally executed, security is assured during transmission by the encryption protocol. Pull printing also reduces the waste from printed documents that are never picked up. If an employee sends a print job to a printer and it never is pulled down to print, the print job expires, it is never stored locally on the printer, and the paper and ink for that print job are saved. There are many HP LaserJet MFP and printer options that support HP Output Server.

Securing printer and MFP hard disks: addressing risk #2—data on printer hard disks

The first step to securing the hard disk is to encrypt its data, preventing unauthorized users from reading its contents. HP LaserJet solutions offer the option of HP High-Performance Secure Hard Disks that encrypt all data sent to and stored on the printer. HP Secure File Erase facilitates the systematic clean erasing of data after a document has been printed to prevent the data from being unnecessarily stored and potentially accessed. It can flexibly allow the erasing of certain files or the sanitizing of an entire hard drive, which is critical when sending a printer out for repair or when decommissioning the device. HP complies with the encryption of user data as recognized with standards such as FIPS 140-2, NIST 800-88 for in-drive Secure Erase command and degaussing, and NIST 800-88 4 for data sanitization.

The "Four A's of Security"

Control types

Authentication

Authorization

Access

Audit

The "Four A's of Security" is a simplified descriptor that communicates the essential keys to securing information technology, including individual controls on devices.[6] The 4A's are:

- **Authentication** is the process of attempting to verify the digital identity of the sender of a communication such as a request to log in. The sender being authenticated may be a person using a computer, a computer itself, or a computer program. A blind credential, in contrast, does not establish identity at all, but only a narrow right or status of the user or program.

- **Authorization** protects computer resources by only allowing those resources to be used by resource consumers that have been granted authority to use them. Resources include individual files or items data, computer programs, computer devices, and functionality provided by computer applications. Examples of consumers are computer users, computer programs, and other devices on the computer.

- **Access** refers to the practice of restricting use of a resource by controlling the ability to interact with that resource. This can be achieved through either physical or logical means such as locks, keys, access control lists, etc.

- **Audit** refers to a series of controls that enable accountability through the use of records and logs to associate a subject with its actions.

The beauty of this model is that it allows for the strengthening of one control type to counterbalance a deficiency of another. By classifying controls by type and identifying their counterbalancing controls, it is possible to identify mitigation strategies as soon as a control failure or limitation is discovered.

Protecting data sent over the network: addressing risk #3—print jobs sent over the network

To help ensure data is safe over the network, an HP encryption solution can be implemented. Encryption can be all-inclusive or customized according to the users or devices involved. These solutions encrypt and help secure files, preventing them from being read if re-routed or intercepted. HP printers can read reencrypted files sent using an HP encryption solution, such as:

- IPsec/IPv6 to encrypt network packets
- Hardware encryption with special NCS and hardware KeyManagement
- HP Jetdirect
- Jetmobile SecureJet

Controlling printer access: addressing risk #4—controls and access to printers

Universal guidelines and best practices indicate that the goal of information security is to protect the confidentiality, integrity, and availability of information. Access to protected information must be restricted to people who are authorized to access that information.

[6] Secure Thinking, "The Four A's of Security," by Mark Trimmer, June 13, 2007.

By verifying printer users, you can control who uses which printers as well as who has access to IT and administrative print settings and who has access to faxing, color printing, and other features. HP can help agencies set up codes or proximity badges and card readers in order to restrict unauthorized access to devices' controls.

HP Secure Multiple Network Printing integrates existing network infrastructures, printers, and pull printing technology with HP security solutions. This enables users working on different networks and at different security levels to share a common print infrastructure that takes the classification of the highest connected network. The security-enforcing functionality is appropriate to the customer environment, using gateways built with data diodes to provide the highest level of separation where required, firewalls, or virtual networks at lower levels. This separation preserves data integrity and confidentiality while lessening the IT device management burden—and it provides seamless access for users.

Preventing tampering and fraud: addressing risk #5—tampering and fraudulent activity

To prevent tampering and fraud, many HP MFPs and printers can be equipped with secure paper input trays, so an unauthorized user cannot remove the special paper used to print checks or prescriptions. HP also provides cutting-edge fraud-proof ink and media technologies that show whether alterations have occurred and send an alert if sensitive documents are being removed. The secure micro-toner and other watermarks preserve the integrity of the document, and tamper-evident ink creates a stain on the document if someone has attempted to scrape or wash ink from a document.

Additionally, HP offers solutions that will track printing or use auditing codes that can be read by a machine to verify authenticity.

Managing and monitoring fleets of printers, networks, and users: addressing risk #6—fleets of printers, networks, and users elevate risk

The first step to securing your fleet is to take a complete inventory of printers, scanners, copiers, faxes, and multifunction printers, including device details, locations, access details, network connection, and the like. Next, you need to understand printer usage, such as:

- What type of content is printed, scanned, copied, and faxed
- Amount of paper used
- Levels of confidential or sensitive data printed
- How printers are set at the network level
- How devices are monitored remotely
- Individual access rights to printer functions
- How many print jobs are lost or forgotten at printer stations

If this seems like a daunting task, that's because it is, if one were to undertake such an analysis manually. HP has a tool called HP Web Jetadmin that is a centrally controlled software tool that lets you take inventory of all of your networked devices. It can even get limited insight into non-HP networked devices. This tool can vastly reduce the analysis burden to the IT team and help accelerate you to a known position.

HP Information Workflow Solutions

HP Information Workflow Solutions are a combination of hardware, software, services, and consulting that helps secure and automate document processes to meet charters and budgets.

HP Managed Print Services, for example, provide managed services, software, and supplies for imaging- and printing-related devices—with flexible procurement, transition, and management options that help increase security, cut costs, and free IT resources to focus on the core mission of the agency.

Next steps

Now that you understand your fleet in terms of usage and management, you can better secure it. You can self-assess your fleet against a checklist or you can use a best practice tool provided by HP. Optionally, HP offers comprehensive workshops that can include assessments for nearly every facet of your printing. HP consultants can help you identify the fleet-wide vulnerabilities and your opportunities to increase security while decreasing printing costs.

Then, once you have gained control of your fleet, HP can help you make the management of it simpler, more straightforward, and cost-efficient by:

- Implementing a one-stop management and monitoring solution through HP Web Jetadmin
- Tracking usage
- Auditing printer practices
- Setting printer defaults
- Controlling access to printers and other imaging devices
- Optimizing and managing your fleet through a Managed Print Services engagement

Partner with HP

HP is a trusted partner to more than 300 government agencies in more than 30 countries worldwide. Whether enabling millions of secure access cards across a defense agency's infrastructure, managing and securing the world's largest and most secure intranet, deploying the largest infrastructure project ever undertaken in Europe, or bringing legacy data into today's information workflows in any of a number of secure environments, HP is a vendor that agencies know they can count on to streamline the flow of documents and information to improve delivery on key missions.

HP also has a special expertise in the area of security. We employ more than 3,000 security and privacy professionals and hold more than 600 security patents. Worldwide, our Enterprise Security Solutions:

- Discover more critical application vulnerabilities than other solutions in the market combined
- Prevent hundreds of millions of junk mail and billions of spam messages from reaching users monthly
- Detect and quarantine millions of instances of malware annually
- Secure more than a million applications and billions of lines of code for clients
- Collect, store, and process billions of security events daily
- Support millions of smartcards, tokens, certificate authorities, and usernames and passwords around the world

Getting started

Governments around the world turn to HP for the mission-focused experience and expertise needed to reduce costs, streamline processes, and operate more efficiently, while improving the quality and value of the services they provide. Depending on the scope and size of your imaging and printing security needs, you can plan and execute a solution in a variety of ways. For example:

- Use a self-assessment checklist and tool, such as the HP Security Action Plan, to scope your fleet and determine your security requirements. You can then implement any built-in security features and/or procure and deploy specialty imaging and printing solutions using either vendor services or your own.

- Conduct a comprehensive workshop that includes assessments of your printing environment. Identify vulnerabilities of the types outlined here that may be putting your agency at risk. This will help you clarify your needs for any vendor conversations you pursue and bring you closer to solutions.

- Consider using an outsourced-service type of vendor engagement such as a managed print service engagement, which can include custom solutions or an engagement level that takes care of the imaging and printing security areas that you don't want to manage in-house.

You'll need to get from your supplier comprehensive documentation that covers system build and installation, verification testing and acceptance, customer-specific configuration, configuration backup, system diagnostics, and full system recovery. Your vendor should also include onsite installation, verification, and acceptance as part of your statement of work. It's also beneficial for defense agencies to work with a partner who is experienced with ad hoc printing arrangements in harsh environments, on ships, in tents in the desert, and using federated and loosely connected printer estates where special printing arrangements may be necessary.

HP provides all of these services and more. For more information, contact your HP sales representative or defense specialist Alan Saxton at HP.

To learn more, visit
hp.com/go/govworkflow

HP three-part approach

HP helps you better serve your constituents by accelerating results, improving the flow and use of information, and reducing costs. Working together, we assess, deploy, and manage your imaging and printing system—tailoring it for where and when work happens.

Optimize infrastructure

Balance your total digital and hard-copy communication costs with your need for convenient user access and productivity.

Manage environment

Maintain end-to-end visibility and control of devices, content and workflows.

Improve workflow

Capture, connect, and communicate information with smart process automation and dynamic content personalization.

Sign up for updates
hp.com/go/getupdated

Share with colleagues

Rate this document

4AA3-9188ENW, Rev. 1, May 2013