U.S. Department
of Transportation

Office of the Secretary
of Transportation

ORDER

DOT 1360.5C

SUBJECT: DOT Information Technology Policy and Administration of Print Services

1. PURPOSE. This document establishes a policy and assigns responsibilities for printers and associated printing products and services for the Department of Transportation. The policy is written to establish operational guidelines and procedures governing the administration of print services in the DOT and to ensure that all staff has sufficient access to print resources in a cost-effective, secure, and resource-efficient manner.

2. CANCELLATION. DOT 1360.5B, Departmental Printing, Duplicating/Copying, and Publications Distribution

3. REFERENCES.

   a. Government Printing and Binding Requirements, as published by the Joint Committee on Printing (JCP), Congress of the United States.

   b. United States Code, Title 44, Public Printing and Documents.

   c. Federal Acquisition Regulation (FAR) Subpart 8.8, "Acquisition of Printing and Related Supplies."

   d. Recommended Security Controls for Federal Information Systems and Organizations (SP 800-53 rev 3), as published by the National Institute of Standards and Technology, August 2009.

   e. Guidelines for Media Sanitization (Special Publication 800-88), as published by the National Institute of Standards and Technology.

   f. DOT Information and Information Assurance Policy #2006-22(rev 1).

   g. DOT Order #1351.14 (CIOP Chapter, Section 4.6).

   h. Protection of Sensitive Agency Information (M-06-16), as issued by the Office of Management and Budget, June 23, 2006.

4. BACKGROUND. In 2007 DOT relocated approximately 5,600 employees to its new headquarters (HQ) building at Southeast Federal Center (SFC). The New HQ Information Technology Infrastructure has provided for the configuration of centrally located printing devices along its workstation spines. Additionally, the DOT Digital Document Center is strategically located and equipped to address the needs of employees for high volume printing needs.

   DOT is continuing to implement strategic sourcing programs as part of a key mandate by the Office of Management and Budget (OMB). The Print Services program's goal aims to identify and pursue opportunities to reduce costs and services while continuing to meet mission requirements. Printing, copying, scanning and faxing devices and their associated services were identified as an opportunity area where costs can be reduced significantly through strategic sourcing and management.

   As part of this initiative, the Office of the Senior Procurement Executive conducted an enterprise-wide analysis which produced the following findings:

   a. DOT Headquarters printing costs are estimated at $4.3 million per year. These costs relate to local printers, network printers, satellite multi-function printers, and the Digital Document Center (DDC). This does not include FAA and contract printing outsourced to the Government Printing Office (GPO).

   b. Desktop printers have the highest cost per page printed at $0.11 per page. Network printers have a cost per page of $0.049 per page. Satellite multi-functional printers would have a cost of $0.040 per page, if they were fully utilized.

   c. A significant number of personal and satellite multi-functional printers are not networked and thus are under-utilized, resulting in a higher cost per page printed.

   d. There is an opportunity to reduce overall costs by limiting color printing.

5. DEFINITIONS.

   DDC – Digital Document Center – DOT's production print center.
   GPO – Government Printing Office – The government agency tasked with printing authority for all government agencies.
   JCP – Joint Committee on Printing – US Congressional Committee with broad authority to regulate printing and distribution of publications by Government agencies.
   MFPs – Multifunctional Printers – that copy, print, scan and fax
   NIST – National Institute of Standards and Technology
   FIPS – Federal Information Processing Standard
   OMB – Office of Management and Budget

6. SCOPE AND EFFECTIVENESS. This policy applies to all Operating Administrations. This policy is effective upon signature.

   a. Roles and Responsibilities.

      (1) Office of the Secretary of Transportation, Office of Information Services.

(a) Issues departmental policy and provide oversight and evaluation, methodology, and destination of all the printing, duplicating/copying, multifunctional printing services, and publications distribution program for ALL DOT Modes (FAA,FTA, PHSMA, FMCSA,OST,NHTSA,FHWA,RITA,FRA,MARAD,SLSDC,OIG).

(b) Ensures that all printing and duplicating/copying produced and procured by or for the Department is accomplished within the regulations and guidelines established by departmental policy and the Joint Committee on Printing (JCP).

(c) Establishes a Central Printing and Publications Management organization, as required by the regulations of the JCP to provide central printing and publications management services for DOT.

(d) Represents the Department with the JCP, other Government agencies and non-Government organizations on printing, duplicating/copying and publications distribution matters.

(e) Develops, implements and manages policies for all of the printing services, including printed products and multifunctional printers.

(f) Manages all external vendor relationships and service provisions for the DDC and MFPs including maintenance, supplies, services and end-user support and billing.

(2) Office of the Chief Information Officer.

(a) Develops, implements and manages technology policies for desktop and group networked printers and supporting systems.

(b) Develops, implements and manages policies pertaining to information assurance, cybersecurity, and privacy for all printers and supporting systems.

(c) Provides network and desktop connectivity and - Common Operating Environment Service Desk.

(3) Operating Administrators and Departmental Officers.

(a) Ensures that instructions to comply with this procedure are issued to all their staff and that checks and reviews are maintained and documented.

(b) Ensures the appropriate actions are taken for cyber security incidents, personally identifiable information and any cyber related tasks.

(c) Develops, distributes and implements policies to grant exceptions.

(d) Develops, implements and manages policies for printers in the case where exceptions were granted.

(e) Provides services for locally attached printers including maintenance, supplies, and services and end-user support, in the case where exceptions were granted.

(4) Printing Officer.

(a) Serves as the designated central printing authority and liaison with the Joint Committee on Printing (JCP) and the Government Printing Office (GPO) and contract printers.

(b) Determines vehicle to procure a printing job, i.e., using a GPO vehicle, completed in-house, or on a multi-functional device.

(c) Provides technical advice and assistance.

(d) Tracks product costs of printed jobs. Provides Operating Administrations with list of their printing orders annually, including costs.

(e) Manages multi-functional printers and DDC.

(5) DOT Employees. It is the role of every DOT employee to join in the effort to increase productivity, protect information appropriately, reduce costs, promote energy conservation and attend to environmental concerns. This policy is designed to support the accomplishment of these objectives as it relates to printing devices and services. Our goal is 100% compliance.

7. POLICY. It is the objective of DOT to provide secure and cost-effective printing solutions for its employee base, through a balanced deployment of output devices. We encourage the use of centrally located, multi-functional printers that copy, print, scan and fax – as opposed to standalone, single function devices.

a. Ratio of Employees to Devices. Multifunctional printers have been centrally placed throughout DOT's Headquarters building. Most are strategically located to allow for the greatest access by the largest number of DOT employees.

(1) To move closer toward achieving a better utilization ratio, the following guidelines should be applied when making decisions regarding future equipment acquisitions and product placements:

Site/Department Sizes & Expected Users	Recommended Ratio
Very small sites (< 10 users)	1 device per site
Medium Sites (26-99 users)	1:15
Large Sites (100-500 users)	1:20
X Large Sites (500+ users)	1:30

Actual configurations and ratios will also depend on the specific work being produced. i.e. special application documents, unique requirements of specific end users, etc. Actual usage of current equipment should also be taken into consideration.

b. Equipment Acquisitions. DOT is seeking to apply strategic sourcing best practices to reduce the acquisition and life-cycle costs of local and network printing devices. All requests to purchase, rent or otherwise acquire printers, copiers, scanners or fax machines must have written approval as indicated below. When budgeting for replacement devices, typical lifecycles of printers are expected to be within the 36-48 month range.

Devices	Approval Authority
Multifunctional printers	Office of Information Services
Scanners, fax machines, desktop printers	Office of the Chief Information Officer

(1) Written requests should provide the following:

(a) Estimated number of copies/pages per month.

(b) Type of work to be reproduced.

(c) Highest level of sensitivity and confidentiality of information to be processed.

(d) Number of employees who will use the device(s).

(e) Any special circumstances that necessitate the need for a new device.

(2) The sensitivity of information to be processed may be determined through consultation with the organizational Information Systems Security Officer (ISSO) or Information Systems Security Manager (ISSM). Requirements to support printing and reproduction of highly sensitive information such as personally identifiable information, security sensitive information, or classified information will result in the application of additional controls and security requirements.

(3) Individual DOT Departments are not authorized to own or operate Department printing facilities. All large volume jobs should be directed to DOT's Digital Document Center for cost effective printing as well as the wide variety of finishing solutions available.

c. Copiers/Multi-functional Devices. Cost effective copying/printing dictates that larger volume jobs be reproduced at the Digital Document Center (DDC), located on the concourse level of the headquarters facility. The following guidelines by specific job can be used when determining the best use of resource devices.

Type of Output Devices and Services	Number of Impressions* per Job
Desktop printers	1-20
Multifunctional printers	21 – 99
Digital Document Center	100 – 25,000

Visual Information and Printing	25,001 and up

*Impressions as calculated by multiplying the number of pages times the number of copies. Each job will be evaluated to determine the best device or service.

d. Printers. The Department seeks to reduce its overall printing output costs and improve the protection of information by using every opportunity to consolidate assets. A major objective would be to limit the acquisition of single function devices – scanners, fax machines, standalone copiers and local and network printers - shifting printing to more cost effective, multifunctional printers and the DDC. Where feasible, older printers, including inkjets and personal desktop printers which have high supply and maintenance costs, present cyber security vulnerabilities, and lack many of the options and features of more robust devices, should be retired.

DOT recognizes that there are valid user requirements where local printers are still the best option and these exceptions must be managed effectively. When seeking to determine effective deployment of personal printers, considerations should be given to the following: proximity of end users to centralized printing devices (i.e. more than 100 feet away) and privacy requirements (i.e. personnel records, reviews, etc.). In most cases consideration can be given to the use of secure print features on multifunctional devices, where a numeric password or PIN, or a DOT PIV (personal identification verification) card is required to release a secured document for printing.

(1) Practices Designed to Reduce Costs.

Color versus Black and White Copying/Printing

When making a determination as to whether or not to use color versus black and white copying/printing consider the following:

- Black and white output should be used for:
  - All document drafts
  - Email print-outs
  - Internal communications
- Color output should be used when there is a need for:
  - Mission critical highlights
  - Clarifying information
  - Calling special attention to specific areas, i.e. maps & technical diagrams, safety programs, etc.

Other Cost Saving Practices

Additional measures to save on document output costs include the following:

- Default all devices - double-sided printing.
- Default all devices - black and white output.
- Print document drafts - black and white, double-sided.
- Print drafts of presentation slides – multi-image per page.

- Don't immediately resend jobs not printed – check for available resources (i.e. paper, toner, etc.)
- Preferred communication and storage method is electronic.
- Eliminate banner sheets where feasible.
- Print only the pages you need.
- Preview document prior to printing
- "Think before you copy/print" – make sure you need all copies you're making
- Scan and send documents electronically, and encrypted where required
- Avoid printing or reproducing sensitive information unnecessarily – you could be exposing the information to unauthorized access or disclosure
- Widen paper margins to save paper.

e. Cybersecurity and Privacy. New statutory requirements, existing U.S. Government policies on information management and protection, and an increased volume of sensitive information and electronic records are driving changes in technology infrastructure and processes to ensure that information is protected, records managed appropriately, and that compliance requirements are properly implemented.

(1) Cybersecurity. Printers, MFPs and printing services inherit the risks, and the associated technical and management controls, associated with the technology infrastructure to which they are attached. At DOT Headquarters, the infrastructure has been determined to carry a mix of information (sensitive, security sensitive, privacy sensitive) that requires the highest level of controls required by National Institute of Standards and Technology (NIST) guidance and standards, which are most effectively implemented through centrally-managed policies and technical solutions. Key among these controls:

(a) Media marking: The term is used when referring to the application or use of human-readable security attributes to indicate distribution limitations, handling caveats, or other applicable security attributes. These marks may include, but not be limited to, "For Official Use Only", "Security Sensitive Information" or other Federally- or DOT-approved marks.

(b) Audit logging: For information that requires a higher level of protection, critical – such as printing – that transfers the information from one medium (electronic) to another (physical paper), to associate a user account with that activity, and to identify, where practicable, the type or categorization of the information that was transferred. This control is more effectively and efficiently implemented within a centralized service, and is subject to a lower risk of being disabled or compromised.

(c) Media sanitization: Systems that process information requiring a high level of protection must be able to ensure that when that information is deleted and no longer needed that it is permanently, and completely removed. Modern desktop, network, and MFP printing devices often contain local hard disks or memory for the temporary storage of information while it is being printed. In order to meet the media sanitization requirement, the devices used at DOT must be validated to perform correctly in clearing or purging un-needed information. Validation is most

cost-effective when the inventory of equipment to be validated is standardized, and can be centrally managed.

(d) Encryption. Systems that process information requiring a high level of protection must encrypt that information when at rest (stored in memory or on a disk) and when in transit (as when moving over a network). The encryption solution must meet Federal Information Processing Standard (FIPS) 140-2 requirements, and be certified, or be a compliant product that uses FIPS 140-2 certified technology. Network printers and MFPs that process sensitive information must implement a validated encryption capability. While not all printed information will need this level of protection, the ability to provide the capability is most cost-effective when centrally managed and provisioned, and a standardized implementation ensures that gaps are minimized that would otherwise expose sensitive information that should be protected.

(2) Privacy. Protection of personally identifiable information (PII) is a requirement under law, with specific requirements mandated by the Office of Management and Budget (OMB). Implementation of these requirements centrally provides for efficiencies and accountability when the requirements are implemented in a decentralized fashion. As there are financial consequences associated with the exposure of breach of PII, measures can be employed, such as those that can be implemented with MFPs and centrally-managed network printers, to reduce this risk and potential cost to DOT.

(a) Logging of data extracts. OMB directives require that machine-readable data extracts be logged. With contemporary technology the ability to treat even printed information on paper as machine readable, though slower than digital media, is feasible. In order to meet the requirement for systems that do not implement logging internally, or which are infrastructure systems that store and transmit PII as only one of many types of information that they process, being able to log all information printed is a means to address this requirement. This capability is most effective and auditable when implemented as part of a centrally managed and provisioned service offering as a mandatory feature.

(b) Media marking. A related component to the logging of data extracts is ensuring that the information is identified as PII, and the date that the information must be destroyed (within 90 days or when no longer needed). For systems that do not implement media marking internally or which are infrastructure systems as described above, the standardized marking of privacy information and the direction to destroy within 90 days or when no longer needed is a necessary control. This capability is most effective, and cost effective, when implemented via a centrally managed and provisioned infrastructure.

(c) Encryption. Encryption of PII at rest and in motion is required by OMB directive. The functional requirements are essentially the same as for other sensitive information that should be encrypted, as described above for cybersecurity controls.

f. Deployment of Print Management Software. DOT employees will benefit from a managed printing environment that is cost effective, sustainable and secure. It will

support employees in making responsible, cost-effective, and eco-friendly printing and copying choices. Easy-to-understand messages will communicate critical printing information to end users when they submit a print job. Managed print software helps create a culture of responsible printing by giving employees information and a choice of actions at the most opportune time – before their documents are sent to a printer.

8. MONITORING FOR POLICY COMPLIANCE. A process for tracking the deployment of local and networked printers, multifunctional and standalone copiers, fax machines and scanners will be implemented in support of this policy initiative. This will be a consolidated effort between the Office of the Administration and the Office of the CIO. The tracking system will also include identification of printer and toner purchases within DOT's procurement systems to allow spend analyses and management of output device purchasing.

9. POLICY EXCEPTION REQUIREMENTS. OAs will submit all policy exception requests directly to their OA CIO in accordance with established OA policies. DOT Departmental and OST offices will submit this request to the DOT IT Shared Services organization, ACIO for IT Shared Services. The DOT IT Shared Services organization will monitor all approved exceptions.

10. DISTRIBUTION. This policy is distributed to all Departmental Officers, Heads of Operating Administrations and Operating Administration Chief Information Officers.

11. INFORMATION DISCLOSURE. While implementing this policy, DOT may collect information that is protected under certain exemptions contained in the Freedom of Information Act (FOIA), 5 USC 552. The appropriate program office must review each request to determine if the information falls within the compulsory disclosure provisions of the FOIA.

12. CONTACT. If you have specific questions related to this policy please contact the Office of Information Services.

FOR THE SECRETARY OF TRANSPORTATION:

Brodi Fontenot
Acting Deputy Assistant Secretary for Administration