

A TROY Group, Inc. White Paper



Three Bryan Drive
Wheeling, WV 26003 USA
(800) 633-2266
www.troygroup.com

Laser Printing of Vital Records
Meeting the Mandate for Improved Security

Introduction

This document examines the risks associated with printing certificates of vital record and offers practical solutions for minimizing the risks.

The Need for Improved Security

The main purpose of the birth certificate is to register and maintain a record of a birth. An “original” record is stored securely in a central office within each state and authenticated “copies” are issued to relatives or other authorized individuals for personal use when requested. In addition, birth certificates have long been used as an identity document. In this capacity, the birth certificate is considered a “breeder document”, providing access to a social security card and, subsequently, a driver’s license or a passport. Through this chain of documents, an individual can obtain a bank account and establish a residency; in short a full identity.

NAPHSIS (National Association of Public Health Statistics and Information Systems) plays the key role in providing national leadership and advocacy for all 57 vital registration jurisdiction members. Through ongoing research NAPHSIS makes available a best practices document revealing new and relevant products, technologies and procedures that ensure quality, security, confidentiality and utility of vital records.

The events of September 11, 2001 brought the security of identity documents used in the United States to the forefront. Among other changes, Congress enacted the Intelligence Reform Act of 2004 which required minimum security features and controls to officially recognized identity documents, including the birth certificate. Section 7211 of the Act directly impacted all States by requiring:

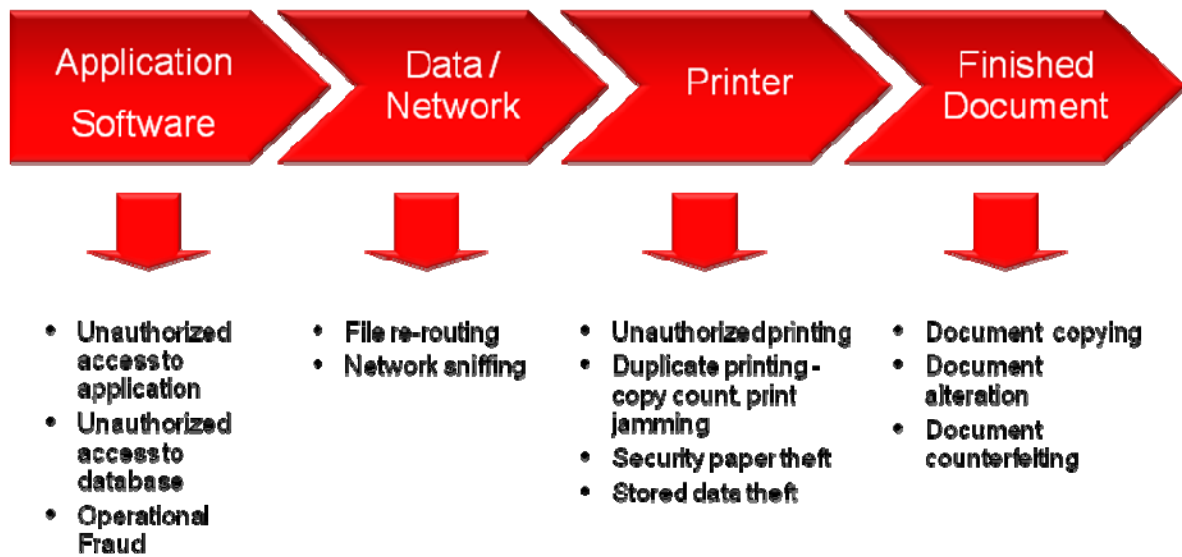
- State or local certification of issued birth certificates
- The use of “safety paper” or an alternative equally secure medium
- The display of the seal of the issuing custodian of record
- The addition of features designed to prevent document tampering, counterfeiting or duplication for fraudulent purposes.
- Proof and verification of identity as a condition of issuance
- Standards for processing of birth certificate applications to prevent fraud

The REAL ID Act of 2005 focused on creating uniform issuance and authentication procedures for driver licenses. The Act also impacted birth certificates by requiring States to verify source documents (like birth certificates) in the driver license issuance process. NAPHSIS has issued observations to its members in relation to State compliance. The compliance deadline is May 11, 2011.

Printing Process and Risks

Individual criminals or organized crime rings are methodical in their search for weak points in systems in their pursuit of criminal activities. In response, it is important to recognize all the areas of risk and use a redundant or “layered” method to counteract each area. Figure 1 provides a generalized model of the printing process and illustrates the potential risks at each stage.

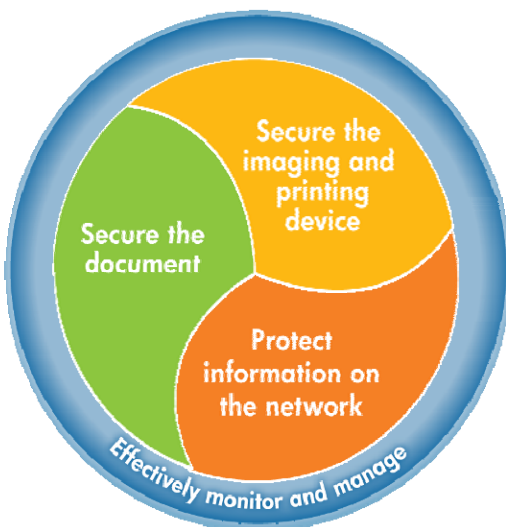
Figure 1 – Printing Process and Risks



Print Workflow Risk Management

Figure 2 shows the Security Printing Framework developed by HP. This Framework provides a model for organizations to proactively manage the risks in their print workflow. Within each of the four areas of the Framework technical solutions are available to help minimize risks.

Figure 2 – Security Printing Framework



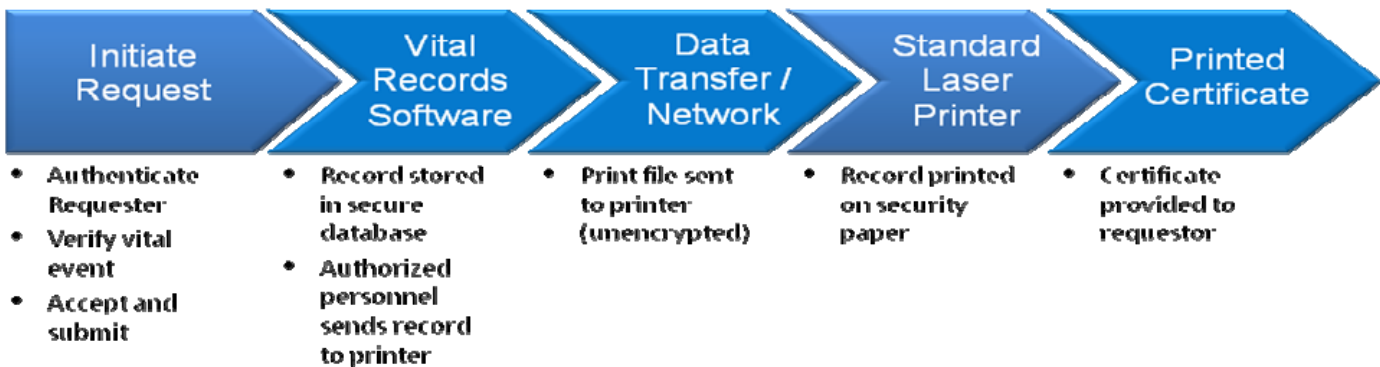
- **Protect information on the network**
 - All print data sent to the printer over a network from the application software should be encrypted.
 - Printers used for security documents should be configured so they are only visible to network administrators.
- **Secure the imaging and printing device**
 - Printers should be configured to accept encrypted data and decrypt the print file within the printer.
 - Printers should have firmware “over-rides” that prevent unauthorized duplicate printing using print panel settings or intentional jamming.
 - Paper trays should have locks and other devices to prevent unauthorized paper removal.
 - Internal memory and hard disks should be configured to erase stored data.
 - Users should authenticate themselves at the printer before the print job is released.

- **Secure the document**
 - Layered elements should be included that deter photocopying.
 - Security paper and specialty inks or toners should be used to deter alteration of printed information.
 - Multiple authentication features should be available for document examiners.
- **Effectively monitor and manage**
 - A print audit trail should be available in both the software and in the printer.

Laser Printed Certificate – Current Workflow & Risks

Figure 3 illustrates a common sequence of events leading to the printing of a vital record. The main security methods in practice are limited to the use of security certificate paper and operating procedures designed to protect the special certificate paper from theft. For example, it is common practice for the office to keep the paper in secure storage, log the paper out when it is needed, and immediately load it into the printer’s paper tray. Unused paper remaining at the end of the day is logged and returned to the secure storage area.

Figure 3 – Current Certificate Workflow



State vital records offices use a variety of printing systems. The most common technology in use today for printing authorized copies of birth and other official certificates is standard off-the-shelf laser printers. These printers lack the security safeguards defined in the Security Printing Framework and shown in the table below. Paper trays in off-the-shelf laser printers are not designed with security in mind, raising the potential for document theft. Among other weaknesses, these printers allow multiple copies, they can be tricked to print duplicates by taking advantage of the printer jam recovery feature, they do not support encrypted print workflows, they have no capability to maintain a print audit trail, and do not offer locking paper trays.

Table – Comparison of Standard and Secure Laser Printers

Category	Feature	Standard Laser Printers	Secure Laser Printers
Device Security	Copy Count Disable	Not available	Standard
	Jam Recovery Disable	Not available	Standard
	Paper Tray Locks	Accessory upgrade only	All trays available
	Secure Job Release	Limited	Configurable
Document Security	Security Fonts	Requires upgrade	Standard
	Anti-copy / Anti -Alteration	Requires upgrade	Standard
Information Security	Decryption	Requires upgrade	Standard
	Audit Trail	Requires upgrade	Standard

Figure 4 – Configured Secure Laser Printer



Figure 5 – Locking Paper Tray Accessory – Front and Rear view



Solutions for Managing Risk at the Printer

Full Featured Security Printers

Figure 4 shows a security laser printer configured with locking paper trays and printer-resident security software / firmware. These firmware security features are explained in the next section. Multiple tray configurations are available to provide users the ability to load and designate specific trays for specific uses, allowing the printer to remain secure in unsecure office environments.

Firmware Security Upgrading

Duplicate print prevention and copy count override are printer firmware features designed to prevent the printer from automatically reprinting when a document is intentionally jammed or instructed to print multiple copies. Some laser printers can be upgraded with add-on firmware modules that add these features as well as printer-based decryption, and in-printer audit trail.

Locking Trays Add-on Accessories

Key locking paper tray accessories (shown in Figure 5) can be added to standard, off-the-shelf laser printers. Tray locks prevent unauthorized access or removal of the secure paper tray and its contents. Added security is provided by incorporating heavy gauge steel shielding that prevents paper removal from the back of the printer. On select models steel shielding is added to the top of the accessory to assure the paper remains secured if the printer is separated from the add-on accessory.

Figure 6 – Printer Key Pad



Controlled Print Job Release

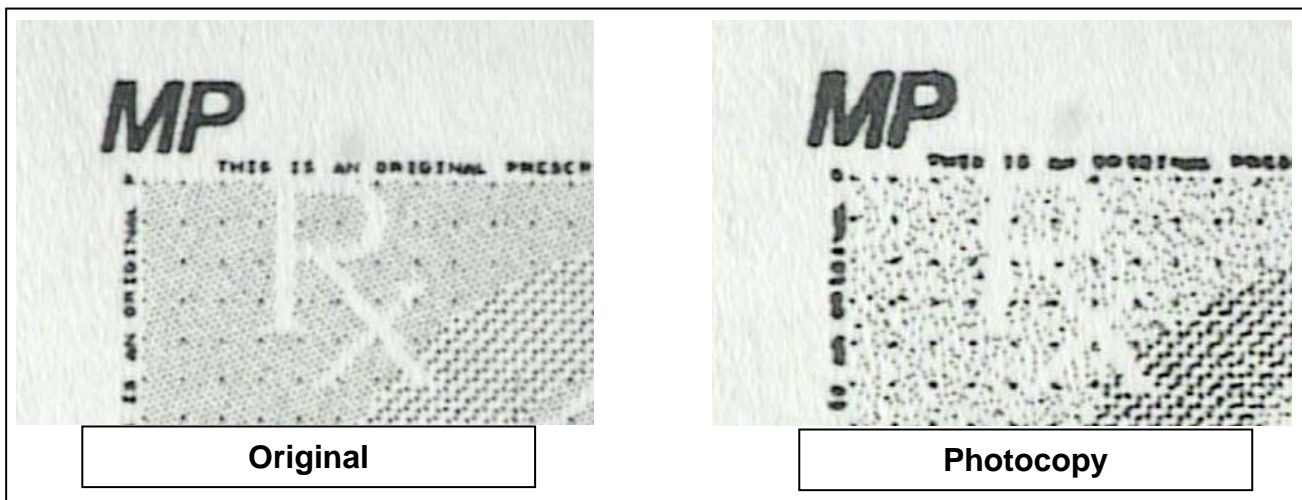
A laser printer keypad (Figure 6) provides added control for administrators. It can also be used for controlled print job release – holding print jobs until an authorized person arrives at the printer and keys in a security PIN code that releases the document for printing. This assures that only authorized individuals have access to the document in the print output bin. Security printers allow for greater flexibility on how controlled print job release is implemented.

Solutions for Managing Finished Document Risk – Using Printer Firmware Enhancements

Laser Microprinting

Microprinting is an anti-copy feature widely used on pre-printed forms. Microprint characters are so small, they degrade visibly when photocopied (see Figure 7). Until recently, micro printing could not be printed satisfactorily on a laser printer. Advances in print technology now make laser printed microprinting practical.

Figure 7 – Laser print Microprinting (magnified)



Laser printed microprint also allows for customized data to be printed, creating an even greater means of adding security to a document. Under magnification, microprint is also effective in verifying the authenticity of a document.

On-Demand Copy-Void Pantograph

Copy-void pantographs (Figure 8) reveal a hidden image or word when photo-copied and help to prevent unauthorized duplication. Like microprinting, this anti-copy technology was only available on pre-printed forms up until recently. Now, laser printed pantographs can be added cost-effectively at the time of laser printing.

Figure 8 - Laser Printed Document with a Copy Pantograph and VDW (on back)

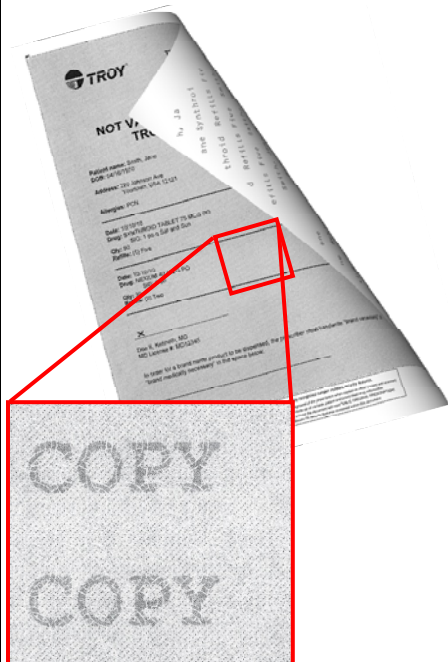


Figure 9 - Tamper Evident Security Toner



Figure 10 - Indelible Printing



VDW - Variable Data Watermarks

Security laser printers can be configured to capture select print data and print it in a repeating pattern on the front or back of a document. For example, the certificate number, child's name and date of birth can be captured from a print file and printed as a VDW. Figure 8 shows an example with a VDW on the back of document. This feature deters criminals from attempting to alter a document because the information targeted appears in multiple occurrences and locations. As a result, alteration attempts will create noticeable damage to the document.

Solutions for Managing Finished Document Risk – Using Specialty Toner

Tamper Evident Toner

Tamper evident security toner offers vital records offices an easy way to add security to all printed vital record documents. Security toner is a high adhesion laser toner formulated to release a bright red stain when chemical alteration is attempted. Security toner functions like other high quality toners and goes unnoticed until attempts are made to remove toner with a solvent. The bright red dye (Figure 9) is released by the solvent and can also serve as a simple and easy method of authenticating the document.

Bleed Through Document Security

Tamper evident security toner can also be used in combination with special paper coatings. When this is done, a “bleed through” effect (Figure 10) will occur in the areas of the document where the toner and the coating interact. Toner printed on uncoated areas of the document will not bleed through. This security feature is also known as indelible printing, because the dye creating the bleed-through image permeates the paper and cannot be removed without visibly damaging the document.

Solutions for Managing Finished Document Risk – Using Security Forms Paper

As previously mentioned, security paper is one of the most common security measures used by vital records offices in the printing and issuance of vital records. NAPHSIS estimates there are currently over 14,000 different designs of certified birth certificates on security paper in use today.

Security paper, also referred to as bank note or certificate paper, is subject to the federal government minimum standards as well as requirements regarding content, layout and security features that prevent tampering, counterfeiting or duplication.

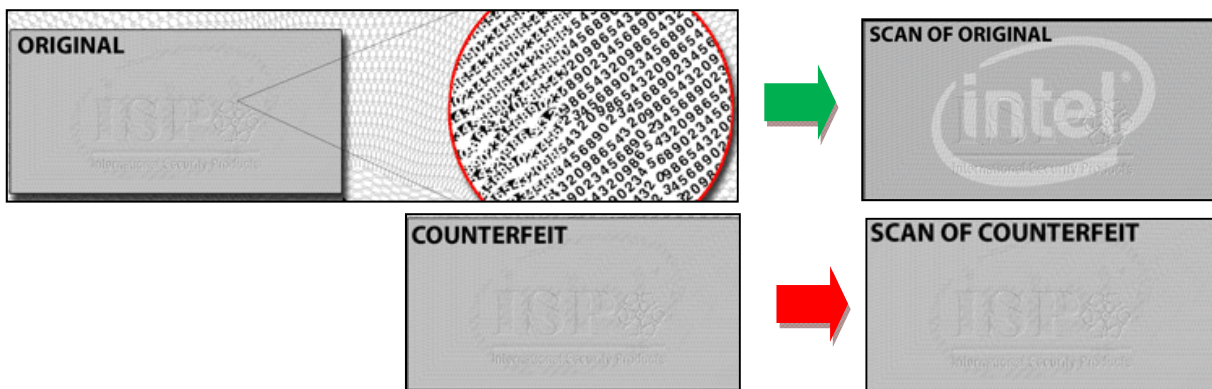
Well designed documents have a number of security features providing both overt and covert document validation as well as other more basic authentication methods including micro text, fluorescent fibers and thermo chromic inks to name a few. To protect against alteration and replication vital records administrators often require controlled security paper with a true watermark, full chemical protection, visible and invisible fibers and a number of other features designed.

This section is a summary of many of the most recent features introduced for use in security paper design.

Hidden Hi-Res Latent Images

This feature is comprised of a high resolution background pattern with a hidden message. The message can only be revealed when the document is scanned at specific scanner settings. This unique security feature provides a very effective method for authenticating high resolution counterfeits or photocopies because the latent image will not appear on copies or counterfeit documents.

Figure 11 - Hidden Latent Images



Hi-Res Micro-Latent Pantographs

Instead of dots or lines in traditional pantographs, the anti-copy micro-latent pantograph is produced with encrypted alpha numeric micro text (Figure 12) that is only visible with magnification. This new void pantograph adds significant new security to a document compared to traditional pantograph technology. Even the most current color copier or desktop imaging technology cannot replicate these patterns. In addition, it offers a very effective method of verifying authenticity.

Figure 12 - Micro-Latent Pantograph Technology

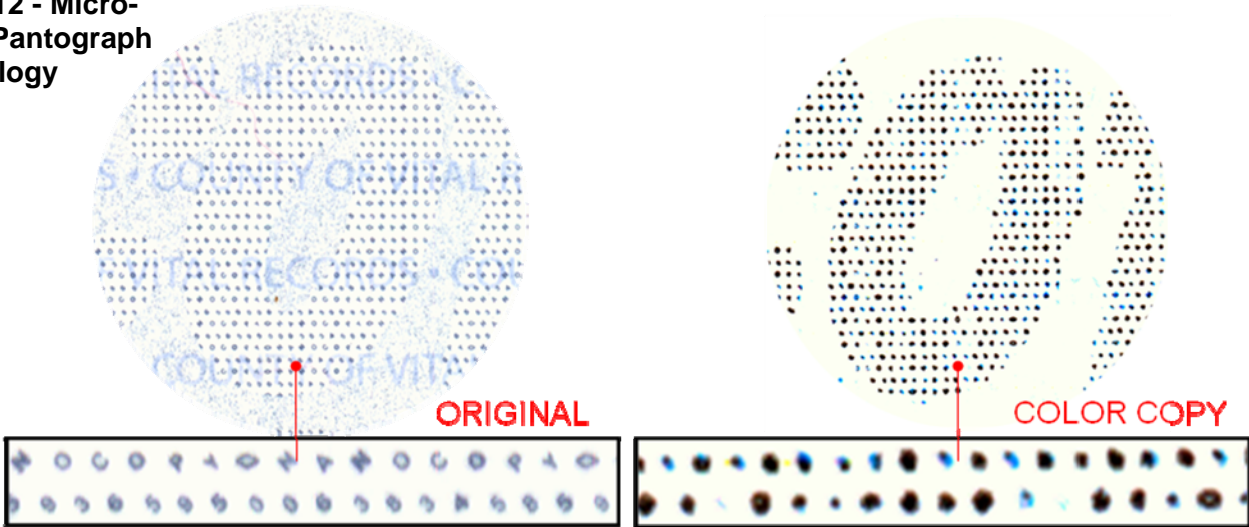


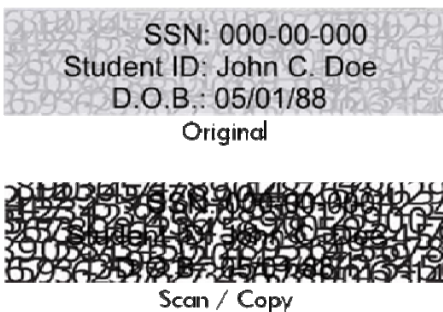
Figure 13 -Holographic Laminates



Engraved Holographic Laminates

Intaglio printing has been used on certificate paper for years and is the same printing process as used to print many currency notes. It provides the familiar tactile feel that is preferred by document examiners. The downside of producing certificate paper using the intaglio process is the high cost of production. Engraved holographic laminates (Figure 13) offer an effective alternative to Intaglio printing on certificate paper. To create the tactile feel, a steel engraved die is used at very high heat and pressure to embed a latent image within the holographic substrate. The added benefit of this feature is the multiple holographic images, which cannot be photocopied and can be used as a simple document authenticator.

**Figure 14
Optical Variable Devices**



Optical Variable Devices (OVDs)

Highly reflective images or numbers become obscured when copied or scanned. This principle is used to create an anti-copy feature in an OVD. The scrambled character pattern surrounding the OVD can be printed with an iron oxide ink so that the document can be easily authenticated with a commercial money detector.

Summary

Standard laser printer technology is in wide use for printing of Vital Records. However, these printers present multiple fraud risks that need to be addressed to meet the fraud prevention mandate for birth certificate printing. Security designed laser printers, specialty toner and the latest advancements in Security Forms paper offer cost-effective solutions to these printing risks.

TROY would like to thank International Security Products for the use of the images illustrating the features in the Security Forms Paper section of this document.

Suggestions for Further Research

- DSA Report March 2009, Report to the Nation, "An Analysis of National Document Security Vulnerability"
- Report on Security and Internal Controls: Office of Vital Records, Bureau of Vital Statistics. New York City Department of Health and Mental Hygiene. Bureau of Audit Services, June 4, 2009
- Perspective. James A Weed, PhD. April 30th, 2008
- The United States Vital Statistics System: The Role of State and Local Health Departments. Steven Schwartz, PhD, Registrar & Assistant Commissioner, Bureau of Vital Statistics, NYC Dept. of Health and Mental Hygiene April 23rd, 2008
- CRS Report for Congress "Intelligence Reform and Terrorism Prevention Act of 2004: National Standards for Drivers' Licenses, Social Security Cards and Birth Certificates" January 6, 2005

About TROY Group, Inc.



- TROY Group Inc. is a Corporate Member of NAPHSIS and an active member of the Document Security Alliance (DSA). Working in collaboration with Hewlett Packard and other leading security document providers, TROY is in a leading role in the ongoing fight against document fraud. TROY solutions are used by Government and Business organizations throughout the world to help protect their important documents.
- TROY Group, Inc. is a 17 year member of the HP Solutions Business Partner Program and the only member that is authorized by HP to enhance HP printers and toner cartridges for use in security printing applications. HP named TROY the 2008 HP World Wide Partner of the Year and the 2009 Outstanding Partner. All TROY HP-based solutions are Tested and Certified by HP.
- TROY solutions can be purchased from TROY or HP. HP fully supports TROY solutions under warranty and service agreements.
- TROY Group, Inc. maintains the highest standard in solution development and manufacturing, producing all TROY solutions in its ISO 9001:2000 certified facility located in Wheeling, West Virginia.

TROY Group, Inc.
Three Bryan Drive
Wheeling, WV 26003

800-332-6427
www.troygroup.com