

A PUBLICATION OF THE INSPECTORS GENERAL OF THE UNITED STATES

*The Journal of Public Inquiry*



SPRING/SUMMER

2007

PRESIDENTS COUNCIL ON  
INTEGRITY AND EFFICIENCY

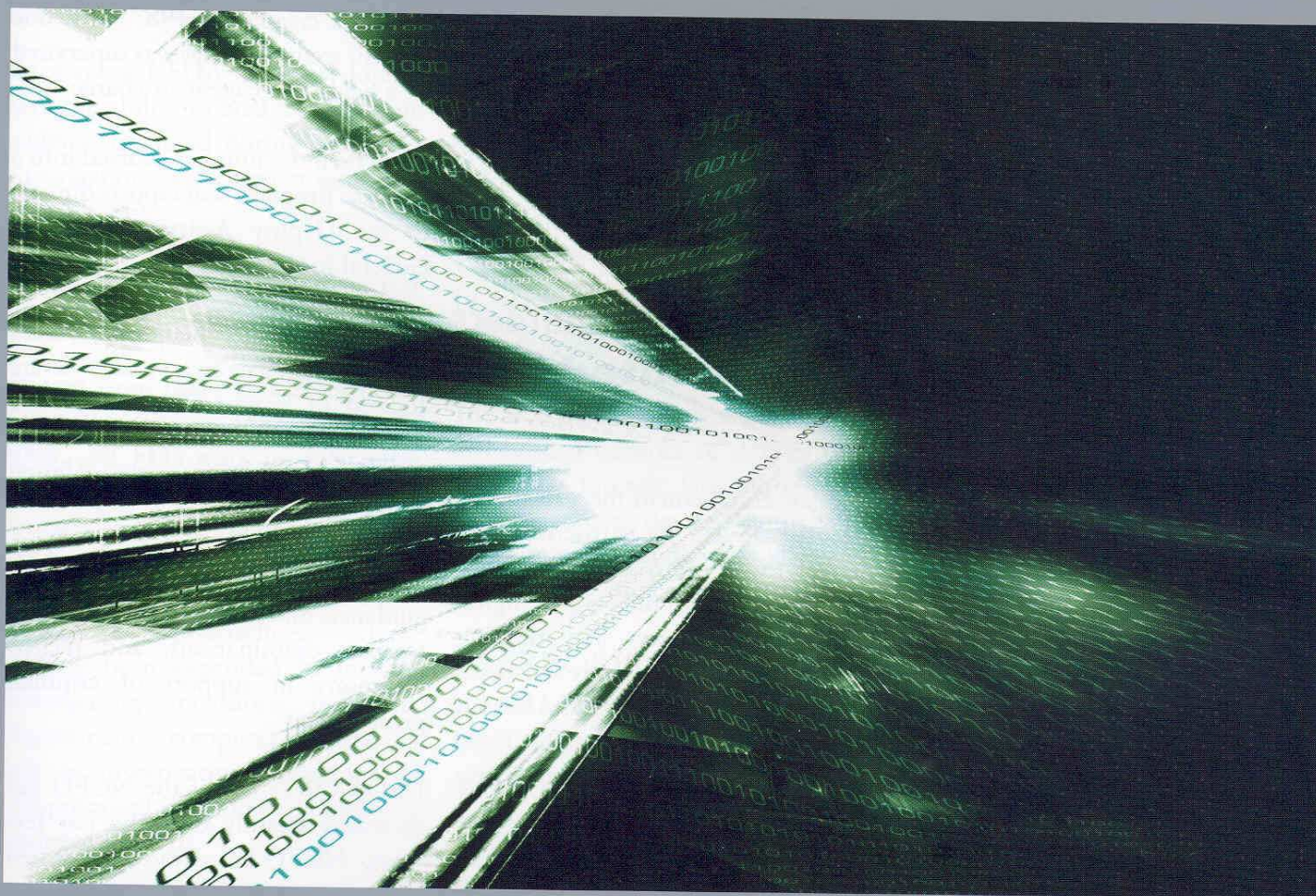
EXECUTIVE COUNCIL ON  
INTEGRITY AND EFFICIENCY



# DIGITAL FORENSICS

BY CRAIG M. GOSCHA AND EILEEN M. SANCHEZ REHRIG

6



THE VALUE OF PARTNERSHIP IN SUPPORT OF  
CRIMINAL INVESTIGATIONS



## INTRODUCTION

E-mail, the Internet, laptops, USBs, MP3 players, cell phones, PDAs, video equipment – today, nearly every crime has the potential to leave digital fingerprints. A scan of the headlines is evidence of this. Everything from white collar crimes to murders has been successfully prosecuted using digital forensics. As crimes become increasingly sophisticated, it is imperative that progressive law enforcement agencies incorporate the collection, preservation, and analysis of digital evidence into their routine investigative efforts.

Recognizing this need and considering budget constraints, in September 2005, the U.S. Department of Agriculture, Office of Inspector General (USDA OIG) entered into a Memorandum of Understanding

Everything from white collar crimes to murders has been **successfully prosecuted** using digital forensics.

(MOU) with the Federal Bureau of Investigation (FBI), to become a participating agency in the Heart of America Regional Computer Forensic Laboratory (HARCFL). In partnering with HARCFL, the agency has gained access to a nationwide network of state-of-the-art digital evidence laboratories and training centers.

Participation in the HARCFL has been beneficial in obtaining training, sample policies and procedures, and, as needed, FBI assistance in our forensic examinations. As part of the MOU, USDA OIG's National Computer

Forensic Division (NCFD) details Forensic Examiners to the HARCFL. In doing so, we have direct access to a Regional Computer Forensics Laboratory's (RCFL) policies, procedures, and training. This ensures that our NCFD Laboratory's guidelines parallel those of a RCFL – moving us one step closer to our goal of becoming an accredited laboratory and ensuring that our digital forensics work is readily accepted in court.

As an additional benefit, all NCFD Forensic Examiners have access to the RCFL's multimillion dollar examination hardware and software, allowing us to maximize our equipment budget.

Because of the sizable investment in both equipment and training needed to support a digital forensics unit, collaborating with the RCFL Program is an economical solution to

help law enforcement meet its digital forensics needs. By partnering with one of the RCFLs, agencies obtain the use of secure, full-service digital evidence laboratories and training centers that provide expert assistance to law enforcement agencies within their designated service area. These services are provided to partnering agencies at no cost.

This article focuses on the benefits that USDA OIG has realized as a participating agency with the HARCFL.

## HISTORY OF USDA OIG'S NATIONAL COMPUTER FORENSIC DIVISION

"It is the mission of the NCFD to provide computer forensic services, courtroom testimony and clear and understandable results of computer forensic examinations aid in the preservation, seizure and collection of computer evidence to the USDA OIG and any agency affiliated with the United States Department of Agriculture."

The USDA OIG computer forensic unit was created in 1987 with one forensic examiner who was supervised by a fieldspecial agent-in-charge.

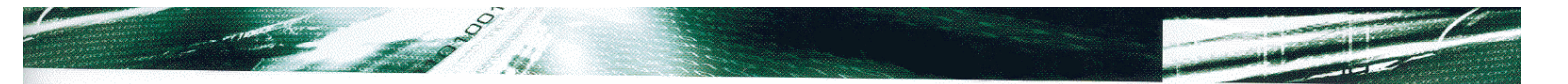
Since then the unit has evolved into a national program that reports directly to the Deputy Assistant Inspector General for Investigations.

The staff currently includes a director and four Forensic Examiners who are located in Kansas City, MO. The NCFD provides service to six USDA OIG regions across the United States.

These services include pre-search guidance, on-site assistance, complete forensic examinations, and related testimony in support of criminal prosecutions.

USDA OIG's use of the NCFD has increased steadily over the last few years. NCFD has already performed work on more OIG criminal cases in the first eight months of Fiscal Year 2007 (36 cases involving 9,058 gigabytes (GB) of data) than it performed in all of FY 2006 (33 cases involving 7,500 GB of data).





SomerecentexamplesofNCFD’swork include developing forensics evidence that was essential to negotiating a guilty plea from a USDA employee who had reproduced and sold 41 pirated copies of USDA-licensed software on two internet auction sites, and the recovery of computer evidence that was used to convince a subject to confess to the receipt and interstate transfer of stolen infant formula.

The NCFD is also being called upon by USDA agencies to provide technical support for their employee misconduct investigations.

Since most USDA agencies do not have the ability to analyze electronic evidence obtained during personnel investigations, they request assistance from NCFD.

In the first 8 months of Fiscal Year 2007, NCFD provided forensic analysis for 17 non-criminal cases referred from other USDA agencies. This compares to 13 cases in FY 2006. NCFD’s work on such cases has had the added benefit of fostering stronger relations between USDA OIG and other USDA agencies.

NCFD responsibilities have recently been expanded to include investigating intrusions into the Department’s computer systems as well as investigating allegations of compromised personal identifying information (PII).

Requests for technical support have recently come from USDA’s Office of the Chief Information Officer, Cyber Security Division for forensic analysis of USDA network intrusions.

Network intrusions are considered a homeland security issue that must be reported to the Department of Homeland Security.

As part of this expanded role, NCFD recently determined that two USDA computer servers had been compromised multiple times by hackers but that the database containing PII for 26,000 USDA employees had not been compromised or transferred from USDA computers.

The work that NCFD performed was critical in reassuring the Secretary of Agriculture that the sensitive and private information contained on these servers had not fallen into the hands of the identify theft industry.

## HISTORY OF THE REGIONAL COMPUTER FORENSICS LABORATORY PROGRAM

The RCFL Program is a nationwide FBI-funded network of state-of-the-art digital forensic laboratories and training centers devoted entirely to the examination of digital evidence in support of investigations such as:

- TERRORISM
- CRIMES OF VIOLENCE
- CHILD PORNOGRAPHY
- INTERNET CRIMES
- FINANCIAL CRIMES
- FRAUD
- THEFT OR DESTRUCTION OF INTELLECTUAL PROPERTY

From its beginning as a pilot project in 1999, the RCFL Program has grown to a network of 14 laboratories and training centers across the United States as illustrated in the map below.

Collectively, the RCFL Program is available to 4,321 law enforcement agencies in 17 states. In 2002, the RCFL National Program Office (NPO) was established to oversee the operations of all the RCFLs and to facilitate the creation of new facilities.

As part of a cooperative partnership, talented and experienced personnel are detailed from Federal, State, and local law enforcement agencies to the RCFLs. The details are performed on a full time basis and last approximately two years.

Individuals detailed to the RCFLs provide digital forensic examinations that benefit the entire law enforcement community. In return, the examiners are provided access to state-of-the-art forensic equipment and training at no cost to the participating agency. Typically, an RCFL consists of 15 people – 12 Examiners and 3 support personnel.

## HOW DO RCFLS OPERATE?

The RCFLs operate under detailed MOUs with each participating law enforcement agency. Funding for the RCFLs is provided by the FBI’s RCFL NPO.

Local Executive Boards, comprised of the heads of the participating Federal, State, and local law enforcement agencies, provide operational guidance





By requiring CART certification for each RCFL Forensic Examiner, we are ensured of the highest level of competence and proficiency for digital evidence examinations.

## WHAT IS THE HEART OF AMERICA REGIONAL COMPUTER FORENSIC LAB?

Part of the nationwide network of RCFLs, HARCFL provides complete digital and electronic forensic analysis to all law enforcement agencies in Kansas and the western two-thirds of Missouri at no cost.

To this end, its examiners are available to provide pre-search guidance, on-site assistance, complete forensic examinations, and related testimony in support of criminal prosecutions.

## BENEFITS OF THE USDA OIG PARTNERSHIP WITH THE HARCFL

The nearly 3-year-old partnership between USDA OIG and HARCFL has resulted in numerous benefits for USDA OIG including technical training; access to policies and procedures; research and development; exposure to the most technologically advanced computer equipment available; access to digital forensics examination and advisory services; broad experience in a variety of digital forensics cases; and a stake in the management of the RCFL.

## TECHNICAL TRAINING

The HARCFL serves as a training laboratory for its participating members. By detailing USDA OIG Forensic Examiners to the laboratory, we have received the following key training benefits:

- Two of the NCFD examiners have received at least seven weeks of training to become certified forensic examiners under the FBI's CART program. This training cost approximately \$15,000 and was paid for by the RCFL NPO. No USDA OIG funds were expended for this training.

- Following CART certification, the examiners were equipped with approximately \$60,000 in forensic tools and materials and received advanced forensic training to remain a certified examiner. The examiners were also provided the opportunity to achieve specialization in various related sub-disciplines, such as MAC, Linux, PDAs, cell phones, etc. Again, no USDA OIG funds were expended for the equipment or training.

- Our entire agency has gained access to the laboratory's state-of-the-art training room, allowing all NCFD employees and USDA OIG agents the ability to participate in a variety of digital forensics courses and workshops offered by the laboratory.

## ASSOCIATE EXAMINER CERTIFICATION


USDA OIG has been rotating NCFD staff through the HARCFL to take advantage of the training, thus allowing each member to receive

and oversight of their respective RCFL. The local boards oversee the activities of their RCFL, and in that capacity, may review any policy, procedure, practice, and/or rule affecting the day-to-day operations of the RCFL.

Currently, the USDA OIG NCFD Director is serving as the co-chair on the board of directors for the HARCFL. This provides NCFD with an opportunity for input into the operational guidance and oversight of the HARCFL. It also affords the NCFD the chance to establish relationships with the other partnering agencies.

As a benefit of the partnership between the RCFL and the participating agencies, the RCFL provides extensive training – free of charge – to the assigned Forensic Examiners and ensures that they become FBI Computer Analysis Response Team (CART) certified Forensic Examiners. All RCFL Examiners must be CART certified to conduct examinations.





and maintain their FBI CART certification through the Associate Examiner Program.

USDA OIG recently became the first participating agency in the RCFL program to have an examiner attain Associate Examiner Certification through the newly created formalized program.

Following certification under the Associate Examiner Program, the RCFL NPO continues to provide and/or pay for all training expenses that may be required for a Forensic Examiner to maintain his or her FBI CART certification.

In fact, the examiner is not only afforded the ability to maintain the certification in his or her primary discipline of digital forensics but may also maintain certification in various sub-disciplines. Completion of this training will normally require participation in two 40-hour courses and the successful completion of competency and proficiency tests, with final training requirements determined by the RCFL NPO.

In exchange, the Associate Forensic Examiner is required to conduct and complete five forensic examinations per year, involving digital evidence as assigned by the HARCFL. The required examinations may include USDA OIG cases.

## POLICIES AND PROCEDURES

In 2005, the USDA OIG NCFD was a rapidly growing forensic unit. As the NCFD continued to evolve into a routine part of USDA

OIG investigative efforts, we saw participation with the HARCFL as a means of ensuring that NCFD laboratory policies and procedures would parallel those of a state-of-the-art forensic laboratory.

Currently, the HARCFL is applying to become an American Society of Crime Laboratory Directors (ASCLD) accredited laboratory. In order to obtain certification a laboratory must demonstrate that its management, personnel, operational and technical procedures, equipment, and physical facilities meet ASCLD established standards.

While not currently required, accreditation may become necessary for all digital forensic labs desiring to present digital evidence in federal court. Keeping this expectation in mind, the President's Council on Integrity and Efficiency (PCIE) formed a working group to develop standards for digital forensics performed within the OIG community.

Members of the NCFD are currently participating in this working group. The first phase of this project resulted in the working group developing a series of questions to be included in the PCIE Investigations Peer Review Guide. During the second phase of the project, NCFD will play a significant role in developing a best practices guide on digital forensics for the PCIE IT Roundtable.

Through our work with HARCFL and the PCIE IT Roundtable, we have been able to develop internal policies and procedures that ultimately can be shared with the PCIE community and we expect to be well positioned when we seek laboratory accreditation. We

expect to realize both cost and time savings when seeking our accreditation by learning from the experience of the HARCFL in obtaining their accreditation and from the PCIE IT Roundtable's work on establishing best practices for computer forensic units.

## RESEARCH AND DEVELOPMENT

The RCFL Program continuously tests current forensic hardware and software. Our affiliation with HARCFL allows our Forensic Examiners access to these forensic tools as well. The ability to "test before you buy" provides the NCFD with valuable information that helps formulate our yearly budget request for the procurement of forensic hardware and software. Due to budget constraints, when procuring technology and training for our lab and its Forensic Examiners, we, like any other agency, must be sure that our return on investment is very high.

Participation in the HARCFL has enabled us to make extremely sound training and procurement decisions for the NCFD with little or no capital outlay or personnel commitment, based on the testing and research and development effort provided by the HARCFL, the RCFL NPO, and CART.

## OTHER BENEFITS

The RCFL NPO provides each Forensic Examiner with a baseline set of equipment valued at approximately \$26,000.



For Forensic Examiners certified in specific digital forensics examinations of such devices as cellular telephones, personal data assistants, video equipment, or specialized operating systems (e.g., Linux, Macintosh, etc.), the RCFL NPO provides additional advanced equipment and software.



Because forensic technology must be updated approximately every 18 to 24 months, joining the HARCFL represents a significant cost savings to our agency.

In addition, our examiner participates in a collegial and collaborative work environment where knowledge obtained by the laboratory is shared among all examiners and problems and issues are addressed collectively.

Furthermore, the expertise and knowledge gained by our examiners remains in and enhances our agency, with the individuals assigned to the HARCFL sharing their new found techniques with their colleagues at NCFD.

## USDA & HARCFL JOINT EFFORTS

The partnership between the USDA and the HARCFL has already proven to be valuable on multiple occasions.

For example, a USDA OIG investigation requiring the examination of 750,000 emails from 3 different email formats (Notes, Outlook, and GroupWise) was made possible through the utilization of state-of-the-art HARCFL software and hardware. The investigation, involving a health and safety issue with national and international ramifications, required the NCFD to provide the Inspector General with timely and accurate results from the analysis.

This could not have been accomplished had we not been provided access to the HARCFL equipment, software, and support staff. Through the use of HARCFL's Storage Area Network, NCFD was able to store and analyze the large volume of data in a timely fashion.

Access to this type of technology also provided NCFD management invaluable insight into the type of hardware and software that the NCFD would need to purchase to handle these types of large cases in the future.

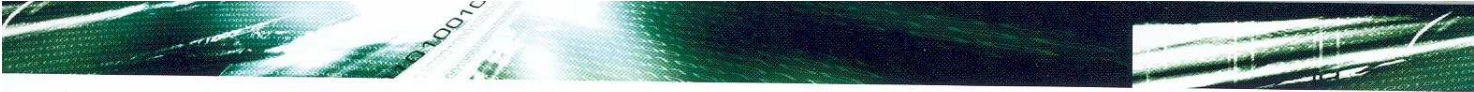
Similarly, prior to the execution of a USDA search warrant in Houston, the NCFD was informed that there were a minimum of 15 computers located within the search warrant site and that all computers would need to be imaged on-site.

Through our participation in the RCFL program, we were able to contact the Director of the Greater Houston RCFL and coordinate its participation in the warrant with just one phone call. The Greater Houston RCFL not only furnished five highly skilled examiners, but also provided the equipment necessary to image what ended up being a total of 18 workstations and 3 file servers. Having the Greater Houston RCFL on-site allowed USDA OIG to save resources and travel expenses by only sending one examiner to Houston. Additionally, because of our close working relationship with the RCFLs, we had confidence in knowing that the RCFL members providing on-site assistance were highly skilled and well-trained forensic examiners.

USDA OIG's partnership with HARCFL was vital when we received a request for forensic analysis of a video surveillance system seized during a USDA OIG search warrant. As part of the investigation, the case agent requested an analysis of the seized video equipment. This request had an unusually short time frame as the evidence was needed in court for the arraignment of a suspect. This proved to be problematic since NCFD did not have the capability to analyze video systems in-house.

Specialized equipment to perform forensic analysis of video systems is extremely cost prohibitive for the NCFD. Because of our affiliation with the HARCFL, we were able to call upon them for the analysis. Within two days of submitting our request to HARCFL, their analysis of the video surveillance equipment was complete. This video analysis proved critical to the advancement of the case





and could not have been performed in such a timely manner if the NCFD had not been a participating agency at the HARCFL.

## CONCLUSION

Since we began our partnership with the RCFL program, the benefits realized by the USDA OIG have far exceeded any expectations.

While the potential monetary savings to the USDA OIG were obvious, we did not anticipate the value of the indirect benefits such as direct access to the hardware, software, and personnel detailed to some of the most advanced computer forensic laboratories across the nation at a moment's notice.

Recent publications and expert opinion suggest that in the future, federal courts may require all digital evidence that is to be presented to have been analyzed by an accredited lab.

By continuing to align our policies and procedures with those of the RCFL, we will be in the best position possible to achieve the certification in a timely and cost effective manner.

Our gratitude to Kevin Steck, Director, HARCFL, who contributed to this article. ⚙️

THE OFFICE OF INSPECTOR GENERAL WAS LEGISLATIVELY ESTABLISHED IN 1978 WITH THE ENACTMENT OF THE INSPECTOR GENERAL ACT (PUBLIC LAW 95-452). THE ACT REQUIRES THE INSPECTOR GENERAL TO INDEPENDENTLY AND OBJECTIVELY:

- Perform audits and investigations of the Department's programs and operations;
- Work with the Department's management team in activities that promote economy, efficiency, and effectiveness or that prevent and detect fraud and abuse in programs and operations, both within USDA and in non-Federal entities that receive USDA assistance;
- Report OIG activities to the Secretary and the U.S. Congress semiannually as of March 31 and September 30 each year;

## WE ACCOMPLISH THIS MISSION BY:

- Investigating allegations of fraud and abuse;
- Using preventive audit approaches, such as reviews of systems under development;
- Conducting audits of the adequacy and vulnerability of management and program control systems; and
- Auditing the adequacy of large USDA payments, such as insurance and deficiency payments, major loans, and retailer food stamp redemptions.

## MISSION

OIG exists as a statutorily created independent and objective unit within USDA, the purpose of which is to conduct audits and investigations; provide leadership and coordination to promote economy, efficiency, and effectiveness and prevent fraud in USDA's programs and operations; and keep the Secretary and the Congress informed as to deficiencies in such programs and operations. USDA's mission is to provide leadership on food, agriculture, natural resources, and related issues based on sound public policy, the best available science, and efficient management. OIG, though independent, must work toward USDA's effectiveness to serve its statutory purpose.



## Craig M. Goscha, U.S. Department of Agriculture OIG



### DIRECTOR, NATIONAL COMPUTER FORENSIC LABORATORY

Craig Goscha is the Director, National Computer Forensic Laboratory (NCFD), Office of Inspector General, U.S. Department of Agriculture (USDA OIG). Prior to joining USDA OIG, Craig spent the previous eight years as a Senior Network Engineer and a Network Security Specialist for the Kansas Department of Transportation and Zurich North America in Kansas City, Missouri.

Craig joined USDA OIG in April 2001 as a Computer Specialist in the National Computer Forensic Unit. In March of 2003, Craig was promoted to Supervisory IT Specialist in the National Computer Forensic Unit. The NCFU was elevated to the National Computer Forensic Division in August 2006 at which time Craig was promoted to Director of the Division. Craig has spent the last six years developing the NCFD's presence within USDA as well as within the IG community. He has participated in the PCIE IT Roundtable group, the Computer Crimes and Intellectual Property Section group at the Department of Justice, multiple Curriculum Review Conferences for the Federal Law Enforcement Training Center, and as co-chair of the Local Executive Board of the FBI's Heart of America Regional Computer Forensic Lab in Kansas City.

## Eileen M. Sanchez Rehrig, U.S. Department of Agriculture OIG



### MANAGEMENT ANALYST OFFICE OF INSPECTIONS AND RESEARCH

Eileen Sanchez Rehrig is a Management Analyst in the Office of Inspections and Research at the Office of the Inspector General, U. S. Department of Agriculture (USDA OIG).

Ms. Rehrig began her federal career in 1991 with the U. S. Department of Justice as a Paralegal Specialist. She then transferred to USDA OIG in 1992.

While at USDA OIG, Ms. Rehrig has held a number of positions including Management Analyst, EEO Specialist, and Planning Specialist. Ms. Rehrig is a graduate of the Pennsylvania State University and holds a Bachelor of Arts in Foreign Service and International Politics. She holds a certificate in Project Management from the George Mason University.