Office of the Inspector General
U.S. Department of Justice

Audit of the Federal Bureau of Investigation's New Jersey Regional Computer Forensic Laboratory Hamilton, New Jersey

Audit Division 16-11 March 2016

AUDIT OF THE FEDERAL BUREAU OF INVESTIGATION'S NEW JERSEY REGIONAL COMPUTER FORENSIC LABORATORY HAMILTON, NEW JERSEY

EXECUTIVE SUMMARY

The Federal Bureau of Investigation (FBI) Regional Computer Forensic Laboratory (RCFL) Program is a partnership between the FBI and other federal, state, and local law enforcement agencies operating within a geographic area. In 2001, Congress directed the Attorney General to establish new RCFLs, and provide support for existing RCFLs, to ensure that they have the capability to perform forensic examinations of computer evidence related to criminal activity and cyberterrorism, as well as to train and educate federal, state, and local law enforcement personnel and prosecutors about computer crime. The USA Patriot Act of 2001 authorized $50 million in annual appropriations to develop this capacity.[1] In 2002, the FBI established the RCFL National Program Office (NPO) to oversee the establishment and operations of the RCFLs.

This audit report focuses on the operations of the New Jersey RCFL (NJRCFL), located in Hamilton, New Jersey. The objectives of the audit were to assess the: (1) efficiency and effectiveness of the NJRCFL's performance, (2) effectiveness of the NJRCFL's outreach and partnership with the law enforcement community, and (3) NJRCFL's case management system and its efforts to address any service request backlog. To accomplish these objectives, we interviewed officials from the NJRCFL and reviewed documents related to the NJRCFL's structure, its accomplishments, and operational standards. We also interviewed the eight agencies that participate with the NJRCFL.

We found that the NJRCFL experienced mixed results in achieving its various performance goals in fiscal years 2011 through 2014. We found that although the FBI revised the definition of a backlog case, that reduced the number of backlog cases at the NJRCFL, a material backlog still existed as of June 2015. We found the backlog was attributable to a number of factors, but chief among them was the need for both more examiners and additional advanced training for those already conducting exams. However, we also found that participating agencies were generally satisfied with the work performed by the NJRCFL.

In addition, similar to what we found in a previous audit at the Philadelphia RCFL, we identified material weaknesses in Cell Phone Investigative Kiosk (Kiosk) usage that, if not addressed, could leave the Kiosk vulnerable to abuse.[2] A Kiosk allows users to quickly and easily view data stored on a cell phone, extract the data to use as evidence, put the data into a report, and copy the report to an electronic

[1] Pub. L. No 107-56 (2001).

[2] U.S. Department of Justice Office of the Inspector General, *Audit of the Federal Bureau of Investigation's Philadelphia Regional Computer Forensic Laboratory Radnor, Pennsylvania*, Audit Report 15-14 (April 2015), 2-9.

storage device. Although FBI policy requires Kiosk users to confirm they possess the proper legal authority for the search of data on cell phones or loose media, we found that the *Technical Assistance Form* used by the NJRCFL did not require users to confirm the legal authority for the search conducted using the Kiosk. However, after our audit fieldwork was complete, the RCFL National Program Office introduced a mandatory electronic form to be used on Kiosks. Law Enforcement Officers logging onto a Kiosk are required to complete the mandatory electronic form and indicate the type of legal authority and the number of devices processed. The NJRCFL has implemented the new mandatory form, which mitigates the Kiosk weaknesses we previously identified. We also found that 26 percent of Kiosk users that examined a cell phone did not certify that they had completed self-paced or hands-on training as required by FBI policy.

We also found that the current process used to capture data for the number of law enforcement personnel that the NJRCFL trained, did not include adequate supporting documentation. For example, training participants registered for courses online using a system managed by the RCFL National Program Office. The NJRCFL used that registration information to identify the number of individuals that participated in training; however, we found that not everyone who registered for a class actually attended the class, and that the registration data was never updated to reflect actual attendance information. As a result, the FBI was unable to accurately determine the degree to which the RCFL program accomplished one of its core missions.

Our report contains three recommendations to help minimize potential abuse or mishandling of the Kiosk program, maintain adequate supporting documentation to support training, and manage the current backlog.

AUDIT OF THE FEDERAL BUREAU OF INVESTIGATION'S NEW JERSEY REGIONAL COMPUTER FORENSIC LABORATORY HAMILTON, NEW JERSEY

TABLE OF CONTENTS

AUDIT OF THE FEDERAL BUREAU OF INVESTIGATION'S NEW JERSEY REGIONAL COMPUTER FORENSIC LABORATORY HAMILTON, NEW JERSEY

INTRODUCTION

According to the Federal Bureau of Investigation (FBI), the Regional Computer Forensic Laboratory (RCFL) Program was created in response to law enforcement's urgent demand for expert digital forensics services and training. It is a partnership between the FBI and other federal, state, and local law enforcement agencies operating within a geographic area. In 1999, the FBI piloted the first RCFL in San Diego, California, as a full service forensics laboratory and training center devoted to examining digital evidence in support of criminal investigations and the detection and prevention of terrorist acts.

In 2001, Congress directed the Attorney General to establish more RCFLs and provide support for existing RCFLs to ensure that each had the capability to: (1) perform forensic examinations of intercepted computer evidence related to criminal activity and cyberterrorism; (2) train and educate federal, state, and local law enforcement personnel, and prosecutors in computer crime; (3) assist federal, state, and local law enforcement in enforcing federal, state, and local laws related to computer-related crime; (4) facilitate and promote the sharing of federal law enforcement expertise and information about the investigation, analysis, and prosecution of computer-related crime, including the use of multijurisdictional task forces; and (5) to carry out such other activities as the Attorney General considers appropriate. The USA Patriot Act of 2001 authorized $50 million in annual appropriations to develop these capabilities.[3] In 2002, the FBI established the RCFL National Program Office (NPO) to oversee the establishment and operations of the RCFLs. In June 2015, the FBI's RCFL Program consisted of 16 RCFLs.

FBI Regional Computer Forensics Laboratories

RCFLs were established to strengthen law enforcement computer forensic capabilities throughout the United States and have provided forensic expertise and training to thousands of law enforcement personnel. The primary forensic responsibilities of an RCFL are to:

1. Conduct a comprehensive examination of digital evidence;

2. Provide a complete and timely report to the contributor;

3. Provide testimony as needed; and

[3] The USA Patriot Act is an antiterrorism law enacted by Congress in October 2011 in response to the terrorist attacks of September 11, 2001. Title VIII of the USA Patriot Act directs the Attorney General to create RCFLs to strengthen the fight against terrorism.

4. Act as a regional focal point for digital evidence issues.

According to the FBI, the key goals of the RCFL Program are to:

1. Provide timely, professional, and technically advanced digital forensic services to law enforcement agencies in an RCFL's service area;

2. Fully utilize applied science and engineering capabilities to support digital forensic examinations;

3. Increase the confidence of investigators, prosecutors, and judges in the digital forensics examination discipline through standardized training and forensic protocols;

4. Provide responsive and flexible services in support of diverse investigative programs; and

5. Meet legal and administrative requirements of diverse judicial systems.

General information on the governance of RCFLs, RCFL personnel and Program Membership, RCFL accreditation, and a summary of backlog service requests at RCFLs for fiscal years (FY) 2011 through 2013 can be found in our previous audit report on the Philadelphia RCFL.[4]

New Jersey Regional Forensic Laboratory

The New Jersey Regional Forensic Laboratory (NJRCFL), located in Hamilton, New Jersey, was established in 2004 and obtained its American Society of Crime Laboratory Directors (ASCLD)/ Laboratory Accreditation Board (LAB) Legacy Accreditation in 2006, and its ASCLD/LAB International Accreditation in 2012.[5] From FYs 2011 through 2014, the NJRCFL had a combined budget of $452,470 that was used for rent, equipment, supplies, administrative services, and other items such as travel and training.[6]

The NJRCFL's mission is to provide its customers with high quality digital forensics services and training. In FY 2014, the NJRCFL had 29 staff members from

[4] U.S. Department of Justice Office of the Inspector General, *Audit of the Federal Bureau of Investigation's Philadelphia Regional Computer Forensic Laboratory Radnor, Pennsylvania*, Audit Report 15-14 (April 2015), 13-15.

[5] The American Society of Crime Laboratory Directors (ASCLD) is a nonprofit professional society of crime laboratory directors and forensic science managers dedicated to providing excellence in forensic science. The ASCLD/LAB Accreditation Program, currently known as the ASCLD Legacy Accreditation Program, was the first accreditation program in the world for crime laboratories. The Legacy Accreditation Program has been replaced by the International Accreditation.

[6] The NJRCFL is located within a New Jersey Department of Law and Public Safety (NJ L&PS) facility. There is a current Memorandum of Agreement in place which states, "FBI will not reimburse L&PS for… apportionment for space rent, building utilities, building security, custodial services…."

8 participating agencies, including: 8 FBI Special Agents, 6 FBI support staff, 10 sworn task force officers and 4 non-sworn task force officers, and 1 FBI contractor (a system administrator).[7] The NJRCFL provides law enforcement agencies in New Jersey with pre-seizure consultation, on-site seizure and collection, duplication and storage of electronic equipment and other digital evidence, examination of digitally stored media, and courtroom testimony. Organizationally, the NJRCFL is a laboratory facility operated out of the FBI's Operational Technology Division (OTD) under the RCFL NPO and the third largest RCFL by staff size. Within the NJRCFL, the Lab Director position is funded by the OTD as a temporary position and not a permanent position within the Newark Field Office. All other FBI positions assigned to the NJRCFL report to the Newark Field Office.

Office of the Inspector General Audit Approach

The objectives of our audit were to assess the: (1) efficiency and effectiveness of the NJRCFL's performance, (2) effectiveness of the NJRCFL's outreach and partnership with the law enforcement community, and (3) NJRCFL's case management system and its efforts to address any service request backlog.

To accomplish these objectives, we interviewed officials from the NJRCFL and reviewed documents related to the NJRCFL's organizational structure, accomplishments, and operational standards. We also interviewed representatives from the 8 NJRCFL participating agencies and 1 non-participating agency to obtain their opinions on the effectiveness of the NJRCFL operations. To assess the NJRCFL's efforts to address its service request backlog, we examined the FBI's Computer Analysis Response Team's (CART) database information to determine if a backlog existed. After determining that the NJRCFL had a backlog, we reviewed the NJRCFL requests for examination for unassigned cases and aging reports for open cases to determine the cause of the backlog.

The results of our review are detailed in the Findings and Recommendations section of this report.

[7] The eight participating agencies at the NJRCFL are the New Jersey State Police, the Essex County Prosecutor's Office, the Mercer County Prosecutor's Office, the Middlesex County Prosecutor's Office, the Monmouth County Prosecutor's Office, the New Jersey Division of Criminal Justice, the FBI Newark Field Office, and the New Jersey Attorney General's Office. The Somerset County Prosecutor's Office was a participating agency through FY 2013; however, in FY 2014 it was no longer able to participate because its lone assignee became a part-time employee and the NJRCFL rules require participating agencies to provide at least one full-time employee.

FINDINGS AND RECOMMENDATIONS

NEW JERSEY RCFL PERFORMANCE, PARTNERSHIPS, AND CASE BACKLOG

RCFLs are responsible for providing timely and high quality digital forensics services and training to the FBI and their RCFL partners. The NJRCFL had mixed success in meeting its various performance goals in FYs 2011 through 2014. We identified weaknesses in the Cell Phone Investigative Kiosk (Kiosk) program that, if not addressed, could increase the risk of abuse and mishandling in the NJRCFL's Kiosk. Further, we also identified weaknesses in the training program that could result in the misreporting of the number of personnel trained, one of the key goals of the RCFL program. Finally, we found that NJRCFL had a backlog as of June 2015. Despite the backlog, participating agencies were still satisfied with the work completed at the NJRCFL.

Performance

Performance for RCFLs is measured across a wide range of services – including laboratory performance, partnerships, and casework. We focused our audit testing on the capabilities that the USA Patriot Act of 2001 cited as the basis for the creation of the RCFLs.

Forensic Examinations, Assisting Law Enforcement, Sharing Expertise

The FBI's Operational Technology Division maintains the CART Database, which tracks forensic examination work from inception to completion. In our audit of the Philadelphia RCFL, we assessed the reliability of the information in the CART Database and found it to be reliable for the purpose of evaluating performance achievements during the period covered by our audit. Additionally, the OTD recently identified the need for a more robust digital evidence tracking system. OTD has engineered and is in the process of fielding its new Digital Evidence Management System (DEMS) to better capture digital forensic matrices and replace the CART Database. The NJRCFL is in the process of transitioning from the CART Database to DEMS.

The NJRCFL is the third largest RCFL by staff size and number of cases. The performance of an RCFL can be measured by different sets of data, including the number of service requests received, examinations completed, and terabytes of data processed. Table 1 provides a summary of these metrics included in our period of review for this audit.

Table 1

CART Database Performance Data
For the NJRCFL in FYs 2011 through 2014

Performance Area	FY 2011	FY 2012	FY 2013	FY 2014	Average
Service Requests Received	535	494	422	470	**480**
Exams Completed	476	423	352	423	**419**
Terabytes Processed	302	346	458	227	**333**

Source: OIG Analysis of CART Database Data

Cell Phone Kiosk Program

The Cell Phone Investigative Kiosk (Kiosk) allows users to quickly and easily view data stored on a cell phone, extract the data to use as evidence, put the data into a report, and copy the report to an electronic storage device such as a compact disk.[8] In addition to the Kiosk, there is also a Loose Media Kiosk, which processes digital evidence stored on loose media, such as a DVD or memory card. Kiosks may be located at an FBI field office, FBI resident agency, or at an RCFL.[9] The NJRCFL Kiosk, which was first available for use in December 2008, is located in the reception area of the NJRCFL, which is outside of the FBI laboratory. To use the Kiosk, law enforcement personnel are required to schedule an appointment. However, the NJRCFL does not require Kiosk users to sign its Visitors Log since users do not go beyond the reception area or enter the NJRCFL's laboratory space. While the Kiosk is housed in the reception area, the cables necessary to connect the Kiosk to a cell phone are not stored with the Kiosk. Instead, the NJRCFL examiner responsible for supervising the Kiosk provides the cables to a visiting user. Without the cables, cell phones cannot be connected to the Kiosk, ensuring that the examiner on duty would have to know that a person was attempting to use the Kiosk because the examiner would have to supply the appropriate cable. This procedure provides the appropriate level of assurance that a person cannot use the Kiosk without the knowledge of the examiner on duty.

To make an appointment to use the Kiosk, generally, users email the NJRCFL Management and Program Analyst or the Operational Support Specialist to schedule their visit. According to the Director, sometimes one investigator will schedule a Kiosk appointment and another investigator will show up in his or her place, or

[8] Unlike a full exam by a Certified Forensic Examiner, the report generated by a law enforcement officer using the Kiosk might not be acceptable as evidence at trial. However, its value in providing police and agents with quick access to the information on a cell phone without having to wait for a full exam to be conducted, which could be delayed for weeks or months, is often critical in helping law enforcement obtain investigative leads, gather evidence for additional arrest or search warrants or to convince a defendant who doesn't contest the charges to plead guilty.

[9] According to the FBI, non-FBI law enforcement personnel are allowed to use the Kiosks located in FBI field offices and resident agencies, but FBI personnel must escort them at all times.

more than one investigator may accompany the scheduled investigator to use the Kiosk. According to the Director, NJRCFL personnel assume that all of the personnel who arrive for a scheduled appointment are part of the same case. However, he said that the NJRCFL does not verify that everyone arriving for a scheduled appointment is working on the same investigative matter.

As a result of the procedures and practices described above, we found that the NJRCFL did not have adequate controls over the access to and use of its Kiosk. FBI policy requires Kiosk users to confirm they possess the proper legal authority for the search of data on cell phones or loose media. During our fieldwork, neither the FBI nor the NJRCFL provided any confirmation to show that NJRCFL Kiosk users possessed the proper legal authority to search for evidence on the devices examined. In addition, the FBI did not provide us with any information regarding controls in place at the NJRCFL to ensure that users do not use the Kiosk for non-law enforcement matters, an inherent risk of Kiosks without adequate controls.

We reviewed two versions of NJRCFL's *Technical Assistance Form*, which Kiosk users are required to complete and return to the NJRCFL for their records. The first version of the form, used from January to June 2011, included the user's name, agency, type of case, case number, and the type of technical assistance requested and/or provided. It also included a signature line. In June 2011, the form was revised to add the following four statements and corresponding signature lines:

- I certify that the legal authority indicated above is valid and authorizes a preview/examination of the items described above and this preview/examination does not exceed the scope of such authorization.

- I certify that I have taken the Kiosk training (when applicable).

- I understand that I must conduct all processing with the Kiosk and am responsible for testifying to any results generated. I also understand that laboratory personnel will not conduct any processing, prepare reports as to processing, or testify regarding results.

- I certify that I have AUSA [Assistant United States Attorney] concurrence to conduct this preview (FBI/LMK only).

While the first of the four statements asks each user to certify that he or she has valid legal authority to examine the device in question, the form does not request that the person completing the form list the specific legal authority for the examination, nor does it even offer a list of possible legal authorities for conducting such a search. When we brought this concern to the attention of the NJRCFL Director, he said he was not aware of this omission. Because the *Technical Assistance Form* used by the NJRCFL did not require users to cite the legal authority for their search each time they used the Kiosk, we were unable to determine if the Kiosk users had the appropriate legal authority to use the Kiosk.

As discussed in our previous report on the Philadelphia RCFL, we believe that although the Kiosk is an efficient tool for Law Enforcement Officers to use to examine digital evidence that may not require the extensive examination of a Certified Forensic Examiner, they are potentially vulnerable to serious abuse.[10] In its July 2015 response to our audit, the FBI stated that the RCFL NPO introduced a mandatory electronic form on the front end of all Kiosks requiring that any Law Enforcement Officer logging on to the Kiosk provide the type of legal authority and the number of devices processed. This new mandatory electronic form was not being used at the NJRCFL Kiosk at the time of our initial visit.

We reviewed all 330 *Technical Assistance Forms* that were made available to us during our fieldwork to verify that each form had the required content and signatures. We found that more than a quarter of the forms did not have a signature attesting that the user had completed the required Kiosk training. According to the FBI's Digital Evidence Corporate Policy Directive and Policy Implementation Guide (Implementation Guide), prior to Kiosk use, self-paced or hands on training is required.[11] Training is required to familiarize the user with the Kiosk equipment to prevent improper usage. In addition, as shown in Table 2, we also found that five percent of the forms were missing a signature for the statement concerning the user's responsibility for testifying about the results generated by the Kiosk and two percent were missing all of the signatures.

Table 2

OIG Review of NJRCFL Technical Assistance Forms

	Frequency	Total Universe	Percent
Missing All Signatures	5	330	**2%**
Missing Kiosk Training Signature	77	301	**26%**
Missing "Testifying to any Results" Signature	18	330	**5%**

Source: OIG Analysis of NJRCFL Technical Assistance Forms

We believe that without completing the required training, Kiosk users could mishandle or improperly use the Kiosk or the results generated by it. However, after our audit fieldwork was complete, the NJRCFL implemented the new mandatory electronic form requiring Law Enforcement Officers to cite the legal authority allowing the officer to search the device and the number of devices processed.

[10] U.S. Department of Justice Office of the Inspector General, *Audit of the Federal Bureau of Investigation's Philadelphia Regional Computer Forensic Laboratory Radnor, Pennsylvania*, Audit Report 15-14 (April 15), 13-15.

[11] FBI Operational Technology Division, *Digital Evidence Corporate Policy Directive and Policy Implementation Guide,* January 03, 2014.

Training

The RCFL program's mission includes training law enforcement personnel around the nation on topics related to seizing and handling digital evidence, using FBI-developed preview tools, and understanding digital forensic examination results. The NJRCFL included expanding the number of tools on which laboratory examiners are trained as one of its annual goals for FYs 2013 and 2014. Additionally, during that period, the NJRCFL offered training to law enforcement personnel that included the proper techniques for seizing, handling, and examining digital evidence.

According to information provided by the FBI, the NJRCFL trained 422 personnel in FY 2011, 493 in FY 2012, 303 in FY 2013, and 301 in FY2014. However, as described below, we were unable to verify the accuracy of these reported accomplishments because the NJRCFL did not maintain adequate documentation for training. As shown in Table 3, the FBI accomplishment data did not match the training records made available to us by the NJRCFL.

Table 3

NJRCFL Number of Persons Trained

Fiscal Year	FBI Accomplishment Data	Training Records	Percent Difference
2011	422	394	7%
2012	493	388	21%
2013	303	309	-2%
2014	301	277	8%

Source: OIG Analysis of NJRCFL Training Records and FBI Data

As a result of not having adequate documentation, the accomplishment data reported by the FBI on the number of personnel trained was not reliable. Until spring 2014, personnel attending training offered by the NJRCFL registered using the RCFL NPO's Training Registration System (TRS). All training data, including the attendance roster, was maintained on the registration website. However, according to a NJRCFL staff member, the instructors at the NJRCFL never retrieved an updated attendance sheet from TRS and therefore could not remove those registered participants who did not actually attend.

According to the FBI, in spring 2014, the TRS was compromised after an intruder gained unauthorized access, and it was taken out of service until a more secure website could be deployed. During our audit, we compared the number of participants listed on the NJRCFL's training records to the information reported in the accomplishment data the FBI provided to the Office of the Inspector General (OIG). As the comparison in the Table 3 above shows, the training records did not support the information reported to the OIG. The percent difference between the FBI accomplishment data and the NJRCFL training records ranged from 2 to 21 percent. According to a NJRCFL staff member, since TRS was taken offline, the

NJRCFL has been responsible for printing the class roster, creating and maintaining a sign-in sheet, and subsequently reporting training data to the RCFL NPO.

In addition to the training conducted at the NJRCFL, staff also conduct seminars and speak outside of the NJRCFL. For this outside training, NJRCFL personnel did not require participants to sign-in. Instead, attendance at these events was estimated. These estimates were reported to the RCFL NPO and included in the Annual Report. Because no supporting documentation was available for training conducted outside the NJRCFL, we could not reconcile the numbers provided by the FBI or those subsequently included in the Annual Reports.

Because the RCFL NPO maintains the TRS, the challenges encountered by the NJRCFL are not unique to the NJRCFL. In our previous report on the Philadelphia RCFL, we recommended that the FBI create a secure automated system to register users for training held at local RCFLs, record user attendance at RCFL training, and report training data to the NPO. Following this audit, the FBI stated that while the RCFL NPO had sought to develop a technical solution to track all training, the cost and current budget do not permit such a training registration system at this time. Despite this, we recommend that the FBI develop interim procedures to accurately capture all training registrations and attendance for training conducted at the NJRCFL and at off-site locations.

Law Enforcement Agency Participation

According to the FBI, partnering is a central part of the RCFL Program and the key to its success. As of May 2015, there were 8 participating agencies at the NJRCFL. To become a participating agency, a law enforcement agency must sign a Memorandum of Understanding (MOU) and detail personnel certified as forensic examiners to the local RCFL. According to officials from participating agencies, performance reviews of law enforcement personnel assigned to the NJRCFL are performed by their parent agency. Therefore, each agency is responsible for the conduct of its own NJRCFL assignee.

Since partnering with other agencies is critical to the RCFL Program's success, through 2014, the NJRCFL has made it a goal to expand the number of participating agencies. However, NJRCFL did not successfully meet this goal in 2011 and 2012, but had success in adding three new agencies in 2013 and 2014. According to the NJRCFL Director, efforts to recruit additional agencies have not always been successful because: (1) travel time to the NJRCFL has been problematic for some agencies, and (2) at least one agency utilized the same forensic services that are available at the NJRCFL from another source at no cost and without a commitment for personnel to be detailed to the agency.

We interviewed all eight participating agencies and one non-participating agency to obtain their opinions on the effectiveness of the NJRCFL operations. Overall, the participating agencies were satisfied with the services provided by the NJRCFL. However, when it came to the timeliness of examinations, the

participating agencies agreed that the timeliness of examinations was an issue, but it did not present a problem for their daily operations.

Case Backlog

Beginning in January 2014, the FBI defined a 'backlog' request as a service request that had not been assigned to an examiner within 30 days of the request. Prior to January 2014, a 'backlog' request was any request not closed within 60 days of receipt from the requesting agency. According to the FBI, the change was necessary because the original definition did not take into account the complexity of each case. According to the January 2014 Implementation Guide, to ensure an effective and efficient workflow, supervisors should assign service requests as examiners become available. At no time should a service request be assigned to avoid being identified as a backlog.

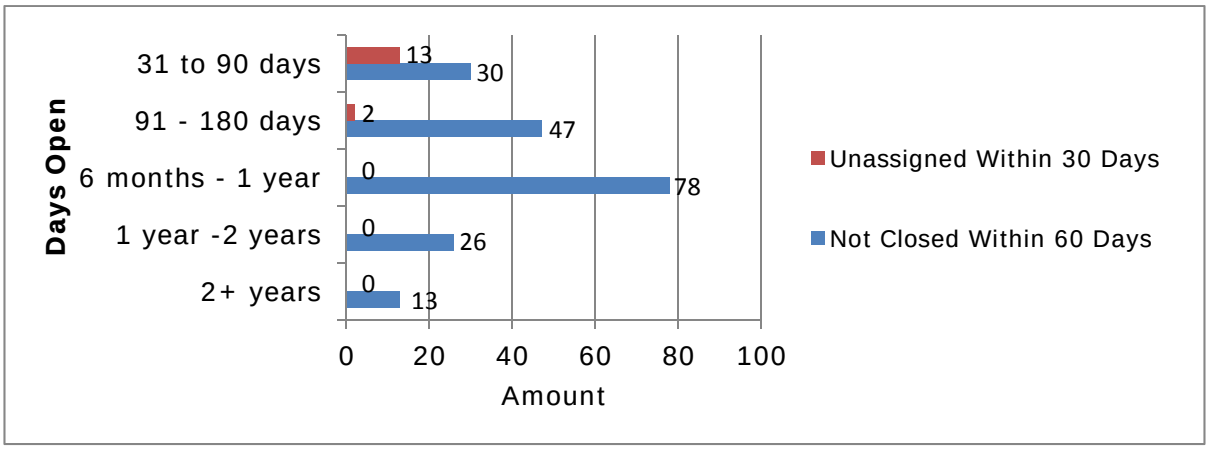
According to the FBI, the goal of the new definition is to more accurately track any backlog by identifying requests that an RCFL does not have the resources to address. To help keep an accurate accounting of backlogged requests, FBI policy now limits service requests to no more than 10 unique items.[12] The case agent or requesting agency should list the items in the service request and rank them in order of priority to the investigation.

Using these criteria, we reviewed the case backlog and aging reports from the CART Database and interviewed the NJRCFL Director. Based on our review, the NJRCFL carries a backlog of requests, both assigned and unassigned. As shown in the figure below, using the new backlog definition, the NJRCFL carried 15 backlog service requests at the time of our review. However, when using the previous backlog definition, the NJRCFL had 194 service requests that were not closed within 60 days, including 39 that were more than a year old.

[12] A unique item is considered a laptop, cell phone, desktop, tablet, etc. An exception is made for numerous items of the same type of disposable media (e.g., CDs, DVDs, flash drives and SD cards less than 1 GB), which can be counted as one item in a service request.

Table 4

Backlog Service Requests by Days Open



Source: OIG Analysis of FBI Data

The NJRCFL Director requires that each examiner close at least 2 cases each month. However, according to NJRCFL's Director, Deputy Director, and the Chief Forensic Examiner, this goal has become increasingly difficult to achieve as the storage capacity of the items to be reviewed has dramatically increased over the past three years.

In December 2014, all RCFLs were informed by FBI's Operational Technology Division that service requests that remain open for more than a year are seen as a high risk and could potentially impact the FBI's operational cycle and ability to conduct effective and timely investigations. Therefore, a new measurement for CART service requests open for 1 year or more has been added to the Director's Scorecard.[13] The FY 2015 target is to have less than 20 percent of total service requests open for longer than 1 year. According to the FBI, less than 20 percent is a target that all CART programs are requested to work towards; it is not a mandate. As shown in the table below, even when using a different definition of what constitutes a backlog, the NJRCFL is still trying to reduce its backlog.

[13] The Director receives a Scorecard monthly that provides the same information as the service request but at the program level and encompasses the entire CART/RCFL Programs.

Table 5

Status of Open Service Requests

Month (2015)	Percentage of Total Service Requests Open for a Year or More
January	17%
February	17%
March	17%
April	19%
May	21%
June	22%

Source: FBI Data

Efforts to Address Service Request Backlog

Based on our interviews, the NJRCFL has made several efforts to manage their case backlog, including bringing on more examiners, implementing policies specific to reducing the backlog that have been approved by the NJRCFL Local Executive Board (LEB), streamlining the examination process, and providing additional advanced training to staff.[14] However, these efforts have not effectively reduced the case backlog.

According to the Director, the clearest solution to the backlog is bringing on additional examiners. However, the NJRCFL wants to balance the need for more examiners that come with more participating agencies against the need to complete the additional examination work. The Director estimated that it takes approximately 14-24 months to get a new RCFL employee through the training program to become a Certified Forensic Examiner. According to the Implementation Guide, Forensic Examiners in Training (FET) are only authorized to perform forensic tasks under the supervision of a Certified Forensic Examiner, which therefore limits the amount of exams they can complete. Accordingly, the NJRCFL Director cited their high percentage of FETs as a cause for the backlog.

Table 6

NJRCFL Certified Forensic Examiner and Forensic Examiners in Training Staffing Levels by Fiscal Year

Fiscal Year	Forensic Examiner	Forensic Examiner in Training	TOTAL
2011	16	4	20
2012	12	5	17
2013	13	4	17
2014	13	7	20

Source: FBI Data

[14] The Local Executive Board (LEB) sets policies for the NJRCFL. The LEB is comprised of the head of each of the participating agencies, or a chosen representative.

NJRCFL's LEB implemented new policies to help manage the case backlog. In FY 2011, the LEB adopted a policy to only process non-participating cases that involved crimes that were at least 2nd degree offenses, except for crimes against children. In FY 2012, the LEB established that all case-related cellular devices must be processed on the Kiosk prior to laboratory submission. This policy was fine-tuned in FY 2013 requiring all agencies to provide a "Page 2" in conjunction with any cellular device or loose media service request. Page 2 is the supplemental form for cellular phones that accompanies all service requests that include a cellular telephone as a submission. As mentioned earlier, all cellular devices must be analyzed utilizing the Kiosk before being submitted for a forensic examination. If the Kiosk is unable to recover the necessary information, the cellular telephone will be assigned to a forensic examiner for further analysis. No cellular telephone will be accepted for examination without this supplemental form.

The NJRCFL sought to streamline the examination process through the Digital Crime Analysis Position (DCAP), the Virtual Machine Forensics Platform, and Centralized Imaging. DCAP was designed to enable state and local cases to have their review process performed remotely by the persons most familiar with the case, the investigator. DCAP is similar to FBI's Case Agent Investigative Review in that it helps to free up the specialized examiner time for case processing and not image and review analysis. At the time of our audit, there were six stations with DCAP access available for state and local use at the NJRCFL. Additionally, three participating agencies obtained DCAP access outside of the NJRCFL; however, none of the three agencies were able to establish the remote connection at the time of our audit – which may be a result of certain firewall issues.

According to the NJRCFL Director, participating agencies have been encouraged to use DCAP; however, he acknowledged that while this was supposed to alleviate some of the backlog issues, it may have actually caused some additional delays. He said that while it is a great idea to have the investigator most closely related to a particular case reviewing the data; it may take additional time because of the investigator's competing priorities, which may result in un-reviewed data on the network. Additionally, many of the participating agencies we interviewed stated that DCAP is cumbersome to navigate and too time consuming to use.

The Virtual Machine Forensics Platform enables NJRCFL examiners to work numerous cases on a single workstation. Additionally, Centralized Imaging is a tool that can image numerous computers in a large case simultaneously, reducing the wait time for pending cases to begin examination. According to the NJRCFL Director, Centralized Imaging has worked for the NJRCFL, especially with exigent, large cases; however, it also has not helped reduce the backlog as much as he thought it would. According to the NJRCFL Director, RCFL examiners have found that the Virtual Machine Forensic Platform was more troublesome than helpful in streamlining the examination process.

According to the NJRCFL Director, in recent years, there had been very few advanced examiner training classes offered by the FBI and none were offered during sequestration. According to the FBI, the training budget has been

significantly reduced every year for the past 5 years. The Digital Forensic Analysis Section, Digital Sciences Development and Staffing Unit has encouraged examiners to find local sources of training and has made funds available to allow examiners to attend advanced training. When a class was advertised, before an examiner could sign up for it, it would be either cancelled or quickly filled by other RCFL examiners. The more advanced training an examiner receives, the greater the examiner's skill sets. A well-rounded examiner with multiple skill sets can complete most, if not all, of the different service requests received (e.g., Linux, Mac, cell phone, etc.). However, examiners cannot examine particular evidence if they have not received certification in that specific area. For example, if an iPhone arrives at the NJRCFL, the examiner must be cell phone certified as well as Mac certified. The Director explained that at least part of the backlog could be attributed to the lack of advanced training. Some of his examiners are unable to get certification in specialized areas because the training is unavailable. Therefore, NJRCFL has examiners that cannot complete certain exam requests and must wait until the certified examiners are available to complete the task.

One of the primary responsibilities of an RCFL is to provide a complete and timely report to the requestor. Because the NJRCFL maintains a backlog, the timeliness with which the requestor receives the report can be problematic and may hinder an investigation where digital evidence plays a significant role. As a result, we recommend that the FBI ensure that the NJRCFL continue to examine its backlog to determine the causes and to develop and implement new measures to address the causes. In its July 2015 response to our Philadelphia RCFL report, the FBI stated that the Forensic Operations Unit has been in contact with the RCFLs experiencing a backlog to determine the reason for the backlogs and to assist with addressing them on a weekly basis. Furthermore, the FBI stated that the RCFL NPO will temporarily transfer personnel to RCFLs that are unable to address the backlog on their own, or identify other RCFLs, Field Divisions, or Headquarters' laboratories that are able to accept additional workload to help reduce the backlog.

Conclusion

In FYs 2011 through 2014, the NJRCFL experienced mixed results in achieving its various performance goals. We found that while a material backlog existed at the NJRCFL, participating agencies were still satisfied with the work performed there. We also found that the current process for training law enforcement personnel was inadequate. As a result, the FBI was unable to accurately determine the degree to which the RCFL program is accomplishing one of its core missions. Therefore, we make the following recommendations.

Recommendations

We recommend that the FBI:

1. Ensure compliance with the FBI's Implementation Guide policy that requires Kiosk users to have taken proper training prior to Kiosk usage.

2. Continue to examine NJRCFL's backlog to determine the causes and to develop and implement new measures to address them.

3. Develop interim procedures to accurately capture all training registrations and attendance for training conducted at the NJRCFL and at off-site locations.

STATEMENT ON INTERNAL CONTROLS

As required by the *Government Auditing Standards*, we tested, as appropriate, internal controls significant within the context of our audit objectives. A deficiency in an internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to timely prevent or detect: (1) impairments to the effectiveness and efficiency of operations, (2) misstatements in performance information, or (3) violations of laws and regulations. Our evaluation of the Federal Bureau of Investigation's internal controls was *not* made for the purpose of providing assurance on its internal control structure as a whole. FBI management is responsible for the establishment and maintenance of internal controls.

Through our audit testing, we did not identify any deficiencies in the FBI's internal controls that are significant within the context of the audit objectives and based upon the audit work performed that we believe would affect the FBI's ability to effectively and efficiently operate, to correctly state performance information, and to ensure compliance with laws and regulations.

Because we are not expressing an opinion on the FBI's internal control structure as a whole, this statement is intended solely for the information and use of the FBI. This restriction is not intended to limit the distribution of this report, which is a matter of public record.

STATEMENT ON COMPLIANCE WITH LAWS AND REGULATIONS

As required by the *Government Auditing Standards* we tested, as appropriate given our audit scope and objectives, selected transactions, records, procedures, and practices, to obtain reasonable assurance that FBI management complied with federal laws and regulations, for which noncompliance, in our judgment, could have a material effect on the results of our audit. FBI's management is responsible for ensuring compliance with applicable federal laws and regulations. In planning our audit, we identified the following law that concerned the operations of the auditee and that was significant within the context of the audit objectives:

- Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA Patriot Act of 2001).

Our audit included examining, on a test basis, the FBI's compliance with the aforementioned law that could have a material effect on the FBI's operations, through interviewing FBI personnel, surveying NJRCFL participants, and reviewing program performance documentation. Nothing came to our attention that caused us to believe that the FBI was not in compliance with the aforementioned law.

APPENDIX 1

OBJECTIVES, SCOPE, AND METHODOLOGY

Objectives

The objectives were to review performance in the following areas: (1) assess the efficiency and effectiveness of the NJRCFL's laboratory performance; (2) assess the effectiveness of the NJRCFL's outreach and partnership with the law enforcement community; and (3) assess the NJRCFL's case management system and its efforts to address its service request backlog.

Scope and Methodology

We conducted the audit in accordance with generally accepted government auditing standards. These standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We conducted work at the NJRCFL in Hamilton, New Jersey.

In conducting our audit, we interviewed officials from the NJRCFL and from the eight participating agencies. We also reviewed documents related to the NJRCFL organizational structure, RCFL accomplishments, and operational standards.

To assess the efficiency and effectiveness of the NJRCFL's laboratory performance, we examined the NJRCFL's progress towards achieving its annual goals. We reviewed and compared the annual goals to the statistics maintained in the CART Database. We compared the number of participants listed on the training roster to the information reported in the accomplishment data the FBI provided to the OIG. In addition, we compared the number of law enforcement and non-law enforcement persons trained at the NJRCFL.

To assess the effectiveness of the NJRCFL's outreach and partnership with the law enforcement community, we interviewed representatives from NJRCFL participating agencies to determine the effectiveness of the work conducted at the NJRCFL. In addition, we assessed the practices regarding the NJRCFL Kiosk usage and training.

To assess the controls surrounding the NJRCFL Kiosk usage, we reviewed the NJRCFL Technical Assistance Form for required items, selected a judgmental sample of NJRCFL Technical Assistance Forms and compared the names on the forms to those for whom an appointment was made. In addition we reviewed the forms to determine whether they contained the required signatures.

To assess NJRCFL training practices, we compared the number that attended NJRCFL training as reported by the FBI in its Accomplishment Data to the number of sign-ins for those training classes. Additionally, we tabulated the number of Law Enforcement Officers and non-law enforcement persons trained.

To assess the NJRCFL's efforts to address its service request backlog, we examined CART Database information to determine if a backlog existed. Based on the information obtained, the NJRCFL had a backlog. We also reviewed the NJRCFL requests for examination for unassigned cases and aging reports for open cases.

APPENDIX 2

FEDERAL BUREAU OF INVESTIGATION RESPONSE TO THE DRAFT AUDIT REPORT

U.S. Department of Justice

Federal Bureau of Investigation

Washington, D. C. 20535-0001

March 14, 2016

The Honorable Michael E. Horowitz
Inspector General
Office of the Inspector General
U.S. Department of Justice
950 Pennsylvania Avenue, N.W.
Washington, DC 20530

Dear Mr. Horowitz:

The Federal Bureau of Investigation (FBI) appreciates the opportunity to review and respond to your office's report entitled, *Audit of the Federal Bureau of Investigation's New Jersey Regional Computer Forensics Laboratory Hamilton, New Jersey.*

We are pleased that you found, "…the participating agencies were satisfied with the services provided by the NJRCFL."

We agree that it is important to minimize potential abuse of the Kiosk program, maintain adequate supporting documentation to support training, and manage backlogs appropriately. In that regard, we concur with your three recommendations for the FBI.

Should you have any questions, feel free to contact me. We greatly appreciate the professionalism of your audit staff throughout this matter.

Sincerely,

Cindy L. Hall
Acting Section Chief
External Audit and Compliance Section
Inspection Division

Enclosure

The Federal Bureau of Investigation's (FBI) Response to the Office of the Inspector General's Audit of the FBI's New Jersey Regional Computer Forensics Laboratory, Hamilton, New Jersey

Recommendation #1: Ensure compliance with the FBI's Implementation Guide policy that requires Kiosk users to have taken proper training prior to Kiosk usage.

FBI Response to Recommendation #1: Concur. The Digital Forensics and Analysis Section (DFAS) will issue a new version of the Cell Phone Investigative Kiosk (CPIK) statistic report program which will require the Kiosk user to indicate, via a checkbox prompt at sign on, whether or not they have received the self paced training associated with the Kiosk. If user indicates they have not yet received training, a training document will open allowing the user to take a self paced course with step by step instructions on how operate the Kiosk. Once the user passes the course, they will be able to access the functionality of the Kiosk. DFAS will implement this update for all Regional Computer Forensic Laboratories (RCFLs) by the end of June 2016.

Recommendation #2: Continue to examine NJRCFL's backlog to determine the causes and to develop and implement new measures to address them.

FBI Response to Recommendation #2: Concur. Digital Evidence Field Operations (DEFO) personnel will continue to contact the RCFLs to assess the material backlog. Thus far, the material backlog is trending down for all RCFLs. Prior to the OIG Audit, the Field Operations Unit was contacting the RCFLs experiencing a backlog to determine reasons for the backlogs and to assist with addressing the backlog. Currently, DEFO personnel are contacting the RCFLs quarterly to assess the material backlog. DEFO will canvas and provide travel for Temporary Duty (TDY) assignments to RCFLs that are unable to address the backlog on their own. NJRCFL currently has no backlog.

Recommendation #3: Develop interim procedures to accurately capture all training registrations and attendance for training conducted at the NJRCFL and at off-site locations.

FBI Response to Recommendation #3: Concur. DEFO is currently working with the developers of RCFL.GOV to include a link on the web page allowing for the recording of trainees registered for training held at RCFLs and their personnel attendance, which will be reported back to the DEFO Unit. In discussions with the web developers, it was determined that security restrictions will not allow the RCFL.GOV website to function as a training portal at this time. Training is currently tracked manually and reported to the RCFL National Program Office by each RCFL. DEFO Unit continues to work to get this functionality added to the RCFL.GOV website or find another viable method of tracking.

APPENDIX 3

OFFICE OF THE INSPECTOR GENERAL ANALYSIS AND SUMMARY OF ACTIONS NECESSARY TO CLOSE THE REPORT

The Office of the Inspector General (OIG) provided a draft of this audit report to the Federal Bureau of Investigation (FBI). The FBI's response is incorporated in Appendix 2 of this final report. The following provides the OIG analysis of the response and summary of actions necessary to close the report.

Recommendation:

1. Ensure compliance with the FBI's Implementation Guide policy that requires Kiosk users to have taken proper training prior to Kiosk usage.

Resolved. The FBI concurred with our recommendation. In its response, the FBI stated that its Digital Forensics and Analysis Section will issue a new version of the Kiosk statistic report program which will require the Kiosk users to indicate, via a checkbox prompt at sign on, whether or not they have received the self-paced training associated with the Kiosk. If users indicate they have not yet received training, a training document will open allowing the user to take a self-paced course with step by step instructions on how to operate the Kiosk. Once the user passes the course, he or she will be able to access the functionality of the Kiosk. The FBI stated that it will implement this update for all Regional Computer Forensics Laboratories (RCFL) by the end of June 2016.

This recommendation can be closed when we receive evidence that the Digital Forensics and Analysis Section has implemented a new version of the Kiosk statistic report program for all RCFLs that requires Kiosk users to indicate that they have taken the proper training or prompts the user to take the proper training prior to using the Kiosk.

2. Continue to examine New Jersey RCFL's (NJRCFL) backlog to determine the causes and to develop and implement new measures to address them.

Resolved. The FBI concurred with our recommendation. In its response, the FBI stated that Digital Evidence Field Operations (DEFO) personnel will continue to contact the RCFLs to assess the material backlog. Further, the FBI stated that DEFO personnel are currently contacting the RCFLs quarterly to assess the material backlog. DEFO will canvas and provide travel for Temporary Duty assignments to RCFLs that are unable to address the backlog on their own. The FBI's response also stated that the NJRCFL

currently has no backlog, however, no documentation demonstrating that the backlog no longer exists was provided.

This recommendation can be closed when we receive evidence that DEFO personnel have assessed the RCFLs material backlog, the underlying causes and measures to address them and, when necessary, have provided additional resources to RCFLs unable to address their backlog on their own. We also ask that the FBI provide evidence to demonstrate that the NJRCL has no backlog currently, or as of the response to our audit report.

3. Develop interim procedures to accurately capture all training registrations and attendance for training conducted at the NJRCFL and at off-site locations.

Resolved. The FBI concurred with our recommendation. In its response, the FBI stated DEFO is currently working with the developers of RCFL.GOV to include a link on the web page allowing for the recording of trainees registered for training held at RCFLs and their personnel attendance, which will be reported back to the DEFO. In discussions with the web developers, it was determined that security restrictions will not allow the RCFL.GOV website to function as a training portal at this time. The FBI further stated that training is currently tracked manually and reported to the RCFL National Program Office by each RCFL. In addition, the DEFO continues to work to get this functionality added to the RCFL.GOV website or find another viable method of tracking.

This recommendation can be closed when we receive evidence that the FBI has developed a viable method of tracking who registered for and attended training held at the RCFLs and off-site locations.

The Department of Justice Office of the Inspector General (DOJ OIG) is a statutorily created independent entity whose mission is to detect and deter waste, fraud, abuse, and misconduct in the Department of Justice, and to promote economy and efficiency in the Department's operations. Information may be reported to the DOJ OIG's hotline at www.justice.gov/oig/hotline or (800) 869-4499.

Office of the Inspector General
U.S. Department of Justice
www.justice.gov/oig