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

OVERSIGHT ★ INTEGRITY ★ GUIDANCE

Audit of the Federal Bureau of Investigation's Intermountain West Regional Computer Forensics Laboratory – Salt Lake City, Utah

Audit Division 20-040

March 2020

Executive Summary

Audit of the Federal Bureau of Investigation's Intermountain West Regional Computer Forensics Laboratory – Salt Lake City, Utah

Objective

The objectives of the audit were to assess: (1) the efficiency and effectiveness of the Federal Bureau of Investigation's (FBI) Intermountain West Regional Computer Forensics Laboratory's (IWRCFL) performance; (2) the effectiveness of the IWRCFL's outreach and partnership with the law enforcement community; and (3) the IWRCFL's case management system and its efforts to address its service request backlog.

Results in Brief

We found that the IWRCFL performance was generally efficient and effective, and partnering agencies were satisfied with the service received. According to IWRCFL officials, it met all of its performance goals for fiscal year (FY) 2016, and all but one performance goal for FYs 2017, 2018, and 2019. The performance goals not met were goals to increase staffing, upgrade a phone system, and in FY 2019, maintain minimal backlog and aging requests.

We also determined that the Cell Phone Investigative Kiosks (CPIK) and Loose Media Kiosk (LMK) at the IWRCFL did not include a training certification question asserting that users met training requirements, and in further assessing this issue we determined that the FBI could not confirm all RCFL CPIKs included a training certification question, and CPIK software updates were not being tracked.

Finally, we noted that as of June 30, 2019, the IWRCFL had 26 backlogged cases. According to the partnering agencies, the backlog has not affected the IWRCFL's ability to be responsive and successful.

Recommendations

Our report contains six recommendations to the FBI to improve the IWRCFL's operations.

Audit Results

IWRCFL Performance – The current and former partnering agencies we spoke with were satisfied with the services received by the IWRCFL, reporting to us that the IWRCFL has been responsive, timely, and reliable. The IWRCFL conducted 44 presentations and 6 training courses from FY 2016 through 2019. However, IWRCFL officials were unable to locate attendance sheets for two of the six training courses. As a result, we were unable to verify attendance for the two training courses. In addition, according to IWRCFL officials, it met all performance goals for 2016, while meeting all but one performance goal for each year from 2017 through 2019. In FY 2017 due to resource constraints, the IWRCFL did not increase staffing. In FY 2018, it did not complete an upgrade of the phone system, which was approved and initiated in FY 2018, but not completed until FY 2019. In FY 2019, the IWRCFL was able to achieve a minimal backlog through March. However, since then the backlog has grown due to the loss of senior staff and more case submissions for advanced cell phone extractions.

IWRCFL Outreach – In an effort to form partnerships and fill open Task Force Officer positions, we found the IWRCFL reached out to larger Law Enforcement Agencies with greater resources. The IWRCFL Director also conducted presentations on the IWRCFL capabilities and services offered.

Kiosk Services - The FBI Digital Evidence Policy Guide requires self-paced or hands-on training prior to use of a CPIK. The CPIK statistics form usually contains a checkbox for users to certify that they have completed training on how to use the CPIK. However, prior to August 2019, none of the IWRCFL's CPIK statistics forms included the training certification question. In August 2019, after the CPIK software crashed, the Montana satellite office thought it was re-installing the CPIK software. Instead, it installed a newer version of the software, which included the training certification question in the statistics form. However, the CPIK user data log was no longer capturing usage, meaning that IWRCFL had no record of who had used the CPIK. A record of who has used the CPIKs is important for statistical reporting, as well as to monitor who has used

the CPIK. As of October 2019, both issues were resolved at all three IWRCFL locations. However, the FBI was not aware if this problem is occurring at other RCFLs, and it was not tracking if and when the CPIK software updates are being completed. Tracking the deployment and implementation of CPIK software updates would be a best practice to ensure the updates are being done, and to aid in trouble shooting any issues that might occur as a result of an update.

Finally, the LMKs at the IWRCFL were also not compliant with the FBI Digital Evidence Policy Guide, as they did not include a prompt requiring users to certify they had taken self-paced training, or had received hands-on training prior to use of the LMK.

Service Request Backlog - As of June 30, 2019, the IWRCFL had 26 backlogged cases. According the IWRCFL officials, the cause of the recent backlog is the loss of a senior examiner and an increase in cases being submitted for advanced cell phone extractions. To address the backlog, the IWRCFL plans to add staff, and two forensic examiners are currently in training to become certified examiners. According to the partnering agencies we spoke with, the backlog has not affected the IWRCFL's ability to be responsive and successful.

AUDIT OF THE FEDERAL BUREAU OF INVESTIGATION'S INTERMOUNTAIN WEST REGIONAL COMPUTER FORENSICS LABORATORY – SALT LAKE CITY, UTAH

TABLE OF CONTENTS

AUDIT OF THE FEDERAL BUREAU OF INVESTIGATION'S INTERMOUNTAIN WEST REGIONAL COMPUTER FORENSICS LABORATORY – SALT LAKE CITY, UTAH

INTRODUCTION

In 1999, a coalition of law enforcement agencies pooled their personnel and funding resources to open the first Federal Bureau of Investigation (FBI) sponsored computer forensics laboratory in San Diego, California. This became the starting point for what has now become a national, FBI sponsored computer forensics laboratory program. While Regional Computer Forensics Laboratories (RCFL) were operating in San Diego and North Texas prior to September 11, 2001, Congress officially authorized the program with the 2001 USA Patriot Act.[1]

The 2001 USA Patriot Act directed the Attorney General to establish RCFLs with the capability to (1) provide forensic examinations with respect to seized or intercepted computer evidence relating to criminal activity; (2) provide training and education to federal, state, and local law enforcement personnel and prosecutors regarding investigations, forensic analyses, and prosecutions of computer-related crime; (3) assist federal, state and local law enforcement in enforcing Federal, State, and Local criminal laws relating 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 with state and local law enforcement personnel and prosecutors, including the use of multijurisdictional task forces; and (5) carry out such other activities as the Attorney General considers appropriate. As of 2019, there were 17 operational RCFLs.

[1] The USA Patriot Act is an antiterrorism law enacted by Congress in October 2001 in response to the terrorist attacks on September 11, 2001.

Figure 1

RCFL Locations

Source: The FBI Digital Evidence Field Operations Unit Chief

FBI Regional Computer Forensics Laboratories

The RCFL program is a national network of FBI sponsored, full-service digital forensics laboratories and training centers. The FBI provides start-up and operational funding, training, and equipment, while state, local, and other federal law enforcement agencies assign personnel to staff the laboratory. RCFLs serve law enforcement agencies in their designated service areas and are devoted entirely to the examination of digital evidence in support of investigations involving criminal and terrorist activities.

The key goals of the RCFL Program are to: (1) provide timely, professional and technically advanced digital forensic services to the law enforcement agencies in the 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.

The RCFL National Program Office (NPO) was established in 2002 within the FBI's Operational Technology Division. The NPO manages and oversees the RCFL National Program. The NPO administers program funding, provides equipment, and supports communications, training, facilities, and information technology needs at the RCFLs. The NPO provides administrative support to ensure consistent operations among the RCFLs. In addition, the NPO publishes an annual report on the RCFL program. This report includes the program's accomplishments, as well as statistical information on each RCFLs performance for the year.[2]

As was stated in the 2015 Annual Report, during 2015 the NPO was strengthened with additional capabilities, and renamed, Digital Evidence Field Operations. The new structure allows the RCFL Program to be even more effective in working with other FBI technical personnel as well as directly with digital evidence programs at FBI headquarters. Each RCFL also has a local executive board (LEB) that includes one representative from each participating agency. These boards oversee the operations of the individual RCFL with which they are affiliated, including the establishment of policies and procedures. The LEBs meet on a biannual basis.

Intermountain West Regional Computer Forensics Laboratory

The Intermountain West Regional Computer Forensics Laboratory (IWRCFL) was established in 2005 and is located in Salt Lake City, Utah. The IWRCFL was the eighth laboratory to open under the RCFL program, and its mission is to provide the highest quality digital forensics services and assistance to law enforcement agencies with jurisdictions in Utah, Idaho, and Montana. In 2006, the IWRCFL launched the program's first Satellite Network to better reach its customers in remote areas of its vast 314,000 square mile service area. The satellite locations are in Billings, Montana and Boise, Idaho.[3] The satellite locations have the same capabilities and service offerings, but on a smaller scale, and they follow the same rules, standards, and methodologies established by the NPO. The IWRCFL was first accredited in 2008. The ANSI-

[2] The FY 2018 annual report had not yet been issued at the time of our audit. The FY 2019 annual report process will not start until January of 2020.

[3] Throughout the report, when we use the acronym IWRCFL we are referring to the Utah location and the two satellite offices in Montana and Idaho.

ASQ National Accreditation Board (ANAB), most recently accredited the IWRCFL in August 2018 for a period of 4 years.

As of October 2019, the IWRCFL has a total of 17 staff members, 12 in Utah, 3 in Idaho and 2 in Montana. Seven of the staff members are FBI employees, one is a federal contractor, eight are full time Task Force Officer's (TFO's) and one is a part time TFO Digital Evidence Laboratory Technician. The nine TFO's are detailed to the RCFL by eight partnering agencies. These staff members provide several different forensic services, including pre-seizure consultation, on-site seizure and collection, duplication, storage, and preservation of digital devices and files. They also conduct forensic examinations of digitally stored media and provide courtroom testimony. The IWRCFL has five Cell Phone Investigative Kiosks (CPIK), two at both the Salt Lake City and Boise locations and one at the Billings location; and three Loose Media Kiosks (LMK), one at each of the three locations. The IWRCFL supply budget for FY 2016 through 2019 is listed in table 1.[4]

Table 1

IWRCFL Supply Budget FY 2016 - 2019[5]

Fiscal Year	Funding Level
2016	$87,000
2017	$60,000
2018	$67,800
2019	$51,000

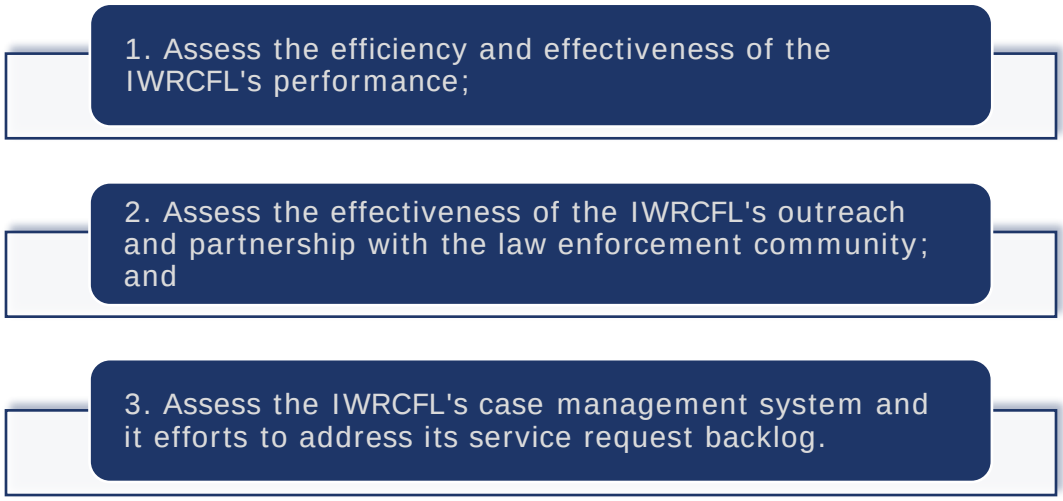
Source: The Digital Evidence Field Operations Unit of the FBI

[4] The purchase of equipment, including software and software licenses is not part of a RCFL's supply budget, it is part of the FBI's Digital Evidence Field Operations Unit's budget.

[5] In FY 2016 a supplement was provided to all RCFLs as additional funding became available. As a result, the IWRCFL FY 2016 funding level includes a $14,500 supplement. Additionally, there was a major delay in the processing of the requisition for accreditation fees when the payment requisition was submitted for processing in October 2017 then canceled in April of 2018 due to challenges encountered attempting to set up a multi-year contract. As a result, each RCFL individually paid the accreditation fees directly, and was sub-allocated the amount to cover its fees and the FY 2018 funding level includes $15,800 for accreditation fees.

Office of the Inspector General Audit Approach

The objectives of our audit were to:



To accomplish these objectives, we interviewed officials from the IWRCFL and reviewed documentation related to the IWRCFL organizational structure, accomplishments, and operational standards. We also interviewed personnel from IWRCFL participating agencies to obtain their opinions on the effectiveness of the IWRCFL operations.

To assess the IWRCFL's efforts to address any service backlog, we examined data from the IWRCFL Digital Evidence Management System (DEMS) to determine if a backlog existed. In addition, we analyzed the IWRCFL Aging report, generated from the FBI's Computer Analysis Response Team (CART) database and calculated the number of cases open by time period. We discuss our audit objectives, scope and methodology in greater detail in Appendix 1. The results of our review are detailed in the Audit Results section of this report.

AUDIT RESULTS

The Intermountain West Regional Computer Forensics Laboratory (IWRCFL) performance was generally efficient and effective, and partnering agencies were satisfied with the service received. The IWRCFL conducted 44 presentations and 6 training courses from fiscal year (FY) 2016 through June 2019, however, it was unable to provide attendance records for 2 of the 6 training courses. According to IWRCFL officials, it met all of its performance goals for FY 2016, and all but one performance goal in each of FYs 2017, 2018 and 2019. The performance goals not met were goals to increase staffing, upgrade a phone system, and, in FY 2019, maintain minimal backlogs and aging requests. We determined that as of June 30, 2019, the IWRCFL had 26 backlogged cases and, according to IWRCFL officials, the cause of the recent backlog is the loss of a senior examiner and an increase in cases being submitted for advanced cell phone extractions. To address the backlog, the IWRCFL plans to add staff, and two forensic examiners are currently in training to become certified examiners.

Prior to August of 2019, none of the IWRCFL's Cell Phone Investigative Kiosks (CPIK) included a training certification asserting that users met training standards. As of October 2019, this issue was resolved at all three IWRCFL locations. However, the FBI could not confirm this was the case for all the RCFLs, and it is not tracking if, and when, the CPIK software updates are being completed. Tracking the deployment and implementing of CPIK software updates would be a best practice to ensure the updates are being done, and to aid in trouble shooting any issues that might occur as a result of an update. Finally, the LMKs at the IWRCFL were not compliant with the FBI Digital Evidence Policy Guide because they did not include a prompt requiring users to certify they have taken self-paced training, or have received hands-on training prior to use of the LMK.

IWRCFL Performance

To assess the efficiency and effectiveness of the IWRCFL performance we talked with the partnering agencies, reviewed attendance records for the training provided by the IWRCFL, and assessed whether it met FY goals and objectives. Generally, we found the IWRCFL performance was efficient and effective. Specifically, we found the partnering agencies were satisfied with the service received by the IWRCFL, and according to the IWRCFL, it met all their goals for FY 2016 and achieved all but one goal for FY 2017, 2018 and 2019, respectively. The IWRCFL conducted 44 presentations and 6 training courses from FY 2016 through June 2019; however, it did not always maintain proper documentation to validate training course attendance.

Partnering Agencies

An RCFL is a partnership between the FBI and other law enforcement agencies operating within a geographic region. Organizations that enter into a Memorandum of Understanding with the FBI become participating agencies in the RCFL. In this capacity, they detail staff members to the laboratory, and in return, they and their personnel receive the following:

- Access to digital forensics examination and advisory services,
- The same sophisticated technical training that is provided to the FBI's certified computer forensic examiners,
- Exposure to the most technologically advanced computer equipment available,
- Broad experience in a variety of digital forensics cases, and
- A stake in the management of the RCFL.

RCFL detailees receive the same training and certification that is provided to the FBI's Computer Analysis Response Team (CART). Many RCFL Examiners cite the opportunity to obtain the CART certification, which they often described as "prestigious," and follow-on training as one of the greatest benefits of joining the program.

The IWRCFL has eight partnering agencies, including five in Utah, two in Idaho, and one in Montana. In order to gain an understanding of the IWRCFL's performance and its effectiveness, we interviewed all eight partnering agencies, and one former partnering agency. Everyone we interviewed expressed satisfaction with the services provided by the IWRCFL, telling us that the IWRCFL has been responsive, timely and reliable.

Training

Consistent with the USA Patriot Act, RCFLs have the capability to provide training and education to federal, state, and local law enforcement personnel and prosecutors regarding investigations, forensic analyses, and prosecutions of computer-related crime. The IWRCFL provided a list of the training items it offered from FY 2016 through June 2019, and the list included 44 presentations and 6 training courses. There is no formal guidance on how the RCFLs record training as each RCFL decides for itself how training records are kept. According to IWRCFL officials, training conducted outside the IWRCFL training center are considered presentations and no attendance or sign-in sheets are maintained. To verify the IWRCFL has been providing training, we requested course registration sheets for the courses taught at the IWRCFL from FY 2016 through June 2019 and were provided sign-in sheets as the IWRCFL does not have registration documents for the courses held. We were able to verify attendance for all but two of the training courses. IWRCFL officials could not locate attendance sheets for these two courses.

During the time of our audit, we learned that the Digital Evidence Field Operations (DEFO) Unit was working on an electronic method for training registration. We spoke with DEFO Unit officials on the status of the electronic method for training registration and were told that it is currently being tested by an RCFL, however any RCFL could choose to use it now. IWRCFL officials said they were aware of the capability and were looking into using it if it captures the information wanted and does not have any technical issues. To ensure the IWRCFL is able to validate the training records, it is important the IWRCFL maintain proper training documentation. As a result, until the implementation, and issuance of

formal guidance on the use of the electronic training registration system, we recommend the FBI ensure the IWRCFL maintains proper documentation to validate attendance at training courses.

Goals and Accomplishments

To assess the efficiency and effectiveness of the IWRCFL's performance we also looked at their goals for FY 2016 through FY 2019 and as can be seen in Table 2, all the FY 2016 goals were met and all but one goal for FY 2017, 2018 and 2019, respectively, were not met.

Table 2

IWRCFL Goals and Accomplishments
FYs 2016 through 2019

Goal	Results
Fiscal Year 2016	
1. Implement New Case Management System	Goal Met
2. Certify Forensic Examiners in Training (FETs)	Goal Met
3. Increase staffing	Goal Met
4. Increase advanced certifications	Goal Met
Fiscal Year 2017	
1. Upgrade Networks	Goal Met
2. Certify FET	Goal Met
3. Increase advance certifications	Goal Met
4. Maintain minimal backlog and aging requests	Goal Met
5. Increase Staffing	Goal Not Met
Fiscal Year 2018	
1. Upgrade / replace phone system	Goal not met
2. Enhance staffing, bring one new FET on board	Goal Met
3. Increase examiner advanced certifications for additional platforms	Goal Met
4. Maintain minimal backlog and aging requests	Goal Met
Fiscal Year 2019	
1. Replace telecommunications system	Goal Met
2. Enhance staffing – bring one new FET on board	Goal Met
3. Increase examiner advanced certifications for additional platforms	Goal Met
4. Maintain minimal backlog and aging requests	Goal not Met

Source: OIG review of IWRCFL provided documents

According to IWRCFL officials, the reasons they did not meet an individual goal in FY 2017, FY 2018, and FY 2019 were:

- One of the goals in FY 2017 was to increase staffing and according to IWRCFL Official's, while it worked with two agencies to fill vacancies, due to

budgetary and personnel constraints, a full commitment was not obtained from either agency by the end of FY 2017.

- One of the goals in FY 2018 was for the IWRCFL to upgrade/replace the telecommunications system. According to IWRCFL officials, the process of upgrading/replacing the telecommunications system was approved and started during FY 2018, however, it was not completed until FY 2019.
- One of the goals for FY 2019 was to maintain a minimal backlog and aging request. We found the IWRCFL maintained a minimal backlog through March 2019, however since then the IWRCFL has seen an increase in backlogged cases due to the departure of a senior FBI examiner, and because the IWRCFL has started doing advanced cell phone extractions, which take time and have led to more cases. IWRCFL officials told us that to help address the recent backlog they have two forensic examiners in training, to become a certified examiner, although according to these officials it takes a forensic examiner trainee about 1.5 years to complete the certification process.

While the IWRCFL did not meet one individual goal in FY 2017, FY 2018, and FY 2019, the missed goals for FY 2017 and FY 2018 were met in the next fiscal year. The missed FY 2019 goal of maintaining a minimal backlog and aging requests is addressed further in the Service Request Backlog section of this report.

IWRCFL Outreach

As described in the Performance section of the report, an RCFL is a partnership between the FBI and other law enforcement agencies operating within a geographic region. Organizations that enter into a Memorandum of Understanding with the FBI become participating agencies in the RCFL. The IWRCFL Director is responsible for coordinating outreach for partnering agencies, and in an effort to create awareness about the IWRCFL, the Director gives presentations on the IWRCFL capabilities and the services offered. Given the limited resources of smaller law enforcement agencies in this location, the IWRCFL looks to larger police departments as partnering agencies because it is more likely to be able to provide a Task Force Officer (TFO) to the IWRCFL. While there is no minimum number of partnering agencies the IWRCFL needs to maintain, the NPO implemented a cap of 10 TFO Full Time Equivalents (FTE) for the IWRCFL due to a lack of program funding that has impacted the FBI's ability to pay for advanced training. IWRCFL officials told us that the cap is intended to reduce the amount spent on introductory training for new TFOs, thereby preserving funds for advanced training.

At the time of our audit, the IWRCFL had eight full time TFO's, and one part-time Digital Evidence Laboratory Technician position. The part-time position does not count towards the 10 TFO FTE cap, so as a result the IWRCFL had two full time TFO positions open. According to IWRCFL officials, it is working to fill the open TFO positions, but described the process as time consuming.

Kiosk Services

RCFLs have two types of self-service kiosks that Law Enforcement Officers use to process digital evidence, Loose Media Kiosks (LMK) and Cell Phone Investigative Kiosks (CPIK). LMKs are used to process digital evidence stored on loose media, such as DVDs or memory cards. According to IWRCFL officials, the LMKs are not often used. CPIKs enable users to copy data from a cell phone, to a computer hard drive. The data is put into a report format, which can be examined on the computer screen and copied onto a portable device, such as a CD or DVD. The FBI's Digital Evidence Policy Guide states that prior to use, both LMK and CPIK users must confirm that they possess the proper legal authority for the search of data on a mobile phone or on loose media. In addition, the Digital Evidence Policy Guide requires self-paced or hands-on training prior to use of an LMK or CPIK.

Loose Media Kiosk

The IWRCFL has five CPIKs, two at both the Salt Lake City and Boise locations and one at the Billings location; and three LMKs, one at each of the three locations. When visiting each of the IWRCFL locations, we observed that all the kiosks were located in secure IWRCFL space. We also verified the LMKs had a prompt asking the user to confirm they have the proper legal authority to search the loose media prior to using the kiosk. However, the LMKs did not include the prompt requiring users to certify they have taken required training prior to using the LMK. IWRCFL officials confirmed the LMKs did not include the training certification question, but said the LMK user guide is in a binder next to the LMK for users to reference. To ensure the IWRCFL is compliant with the FBI's Digital Evidence Policy Guide, we recommend the FBI ensures the LMK users have taken either self-paced training, or have received hands-on training prior to use of the LMK.

Figure 2

Loose Media Kiosk at the Salt Lake City, Utah, IWRCFL Location

Source: OIG picture of a LMK at the Salt Lake City, UT IWRCFL location

Cell Phone Investigative Kiosk

The CPIKs have an electronic statistic form that each user is required to fill out prior to use. The form includes the following fields: name, agency, legal authority, case date, case type, case number, exhibit number, device model, total number of devices, and other case information. This information is maintained in an electronic log and allows the IWRCFL to keep track of CPIK users. It is important to track use of the CPIK to report accurate statistics for the RCFL annual report. In addition, it is important for the Montana satellite office to be able to review the CPIK user data log because, while its CPIKs are located in secure FBI Resident Agency office space, they are separated from the RCFL office space, increasing the likelihood that individuals could use the CPIK without the awareness of the Montana IWRCFL staff.

In addition to the CPIK user providing the legal authority when filling out the electronic statistics form, users must also check a box certifying they have the appropriate legal authority to examine the evidence. If the user does not check the

box the CPIK statistic form will close and the user will be unable to continue. The CPIK statistic form also includes a question requiring users to certify they have completed training on how to use the CPIK. If the user checks no, the CPIK self-paced training manual will pop up for the user to review. However, we found that the training certification question was not included in the CPIK statistic form for the CPIKs in Utah and Idaho. According to IWRCFL officials, in August 2019, after the CPIK software crashed, the Montana satellite office thought it was re-installed the CPIK software. Instead it installed a newer version of the software, which included the training certification question in the statistics form. However, the CPIK user data log was no longer capturing usage, meaning the Montana satellite office had no record of who was using the CPIK.

We discussed the software update process with the FBI Program Manager responsible for the CPIK at all the RCFLs, and learned he did not know whether all RCFLs currently have the updated CPIK statistic form, which includes the required training certification question. There is no requirement for the RCFLs to report back when software updates have been installed. Additionally, according to the Program Manager, there is no automated way to know whether the updates have been installed at each RCFL CPIK; the only way to know would be to ask each RCFL. As of October 2019, both issues have been resolved at all three IWRCFL locations. However, the FBI does not know if this problem is occurring at other RCFLs.

Since the FBI does not track whether software updates have been completed we were unable to determine if this problem is universal or isolated to a certain RCFL location. In addition, the Program Manager responsible for the CPIK at all the RCFLs is not part of the Digital Evidence Field Operations (DEFO) Unit, which the RCFL falls under. Rather, the Program Manager is with the Electronic Device Analysis Unit and does not report to the DEFO Unit Chief. The DEFO Unit Chief was unaware of the CPIK issues when we spoke in late September 2019.

While the problems tracking software updates that we identified with the CPIKs have not hindered the IWRCFL from providing service, the FBI should track software updates to ensure all RCFLs are using the current software version. In our judgment, the FBI should ensure all RCFLs CPIK statistic forms include the required training question, and all RCFLs CPIK user data logs are capturing CPIK usage. A record of who has used the CPIKs is important for statistical reporting as well as to review who has used the CPIK. It would also be good practice for the FBI to track the deployment and implementation of CPIK software updates to ensure it is being done, and to aid in trouble shooting any issues that might occur. As a result, we recommend the FBI ensures: (1) all RCFLs CPIK user data logs are capturing CPIK usage, (2) all RCFLs CPIK user forms include the training certification question, (3) CPIK software updates are documented, including the reason for the update, when the software update was deployed, and when each RCFL has completed the update, and (4) the CPIK software updates and documentation of the updates, are communicated to the Digital Evidence Field Operations Unit.

Service Request Backlog

In October 2015, the IWRCFL was the first RCFL to convert to the Digital Evidence Management System (DEMS). While the RCFLs are not required to use DEMS, it is a laboratory information management system that includes both case management and evidence control functionality.

The CART database is used to track FBI forensic examination work from inception to completion. The data from the CART database is used to provide statistics and metrics to Congress, FBI management, and the public regarding the productivity of the FBI's digital forensic professionals. To assess the IWRCFL efforts to address its service request backlog, we analyzed its open service request report from DEMS and determined, as of June 30, 2019 the IWRCFL had a backlog of 26 cases. We also interviewed IWRCFL officials to determine why there was a backlog, and what the IWRCFL was doing to address it. Finally, we analyzed the aging report from the CART database to calculate the number of cases open by time period.

- The open service request report is from DEMS.
- The aging report is from the CART database.

CART Database vs. DEMS

As part of our assessment of computer-processed data, we analyzed the IWRCFL's CART aging report and its DEMS open service request report. Our analysis showed a difference of 35 cases. Thirty-two cases were included in the DEMS open service request report that were not in the CART aging report, and conversely there were three cases on the CART aging report, that were not correctly on the DEMS open service request report. Specific to the 32 cases in DEMS and not in the CART database, according to IWRCFL officials;

- Two of the 32 cases were not in the CART database due to an unknown export error.
- Sixteen of the 32 cases were marked as pending, not accepted in DEMS and as a result, not included on the aging report. The CART aging report does not include requests that are pending, and not accepted in DEMS. A request is pending, and not accepted if it has not yet been reviewed to determine if the IWRCFL can do the work, or the request is missing information, such as the legal authority.
- Fourteen of the 32 cases in DEMS, but not in the CART database, were the results of either a search, or technical, or administrative request.[6] The CART

[6] As defined within the CART database, a search request is when assistance is needed in the execution of a search warrant, consent to search, or under any other legal authority where digital evidence is present. A technical request is when assistance is needed to provide extraction, review, presentation, preservation, or destruction of data contained in digital media. An Administrative search is when assistance is needed to provide any number of administrative functions performed by CART examiners, i.e. training, briefings, and presentations.

aging report only includes requests that are designated as examinations in DEMS. It does not include search, technical, and administrative request when taking in DEMS data.

In regards to the three cases on the CART aging report that were not on the DEMS open service request report, according to IWRCFL officials, these were closed requests and should not have been on the CART aging report. Specifically, two of the three requests were closed well before the aging report was run and should not have been on the aging report. The third request was closed around the same time the report was run and it is possible the export from DEMS to the CART database had not yet been done.

The CART database is being phased out and will be replaced by the Digital Evidence Management System 2 (DEMS2). The FBI's Digital Forensic Support (DFS) Unit took over responsibility for DEMS in 2016 and is currently handling the creation and deployment of DEMS2. According to the DFS Unit officials, an initial testing phase release is planned for the end of 2019 and deployment of DEMS2 is scheduled for the spring of 2020. All RCFLs will be required to utilize DEMS2 and when DEMS2 is released, the CART database will stop being used for the management of digital evidence. As a result of these efforts, we determined that the DEMS and CART data was sufficiently reliable for the purposes of this report.

Backlog

The FBI Digital Evidence Policy Guide defines digital evidence backlog as any unassigned request that is over 30 days old. The policy also directs supervisors, to ensure an effective and efficient workflow, to assign service requests as examiners become available to actively address those requests. At no time should a service request be assigned to avoid being identified as backlog. Our analysis of the IWRCFL DEMS open service request report showed, as of June 30, 2019 the IWRCFL had 26 cases that met the backlog definition.

According to IWRCFL officials, there are more cases coming in then the IWRCFL can complete. In addition, the IWRCFL recently lost a senior FBI examiner and has started performing advanced cell phone extractions, which take time, and has led to more backlogged cases.[7] Specifically, IWRCFL officials said one non-partnering agency recently brought the IWRCFL 10-15 cell phones, at one time for advanced cell phone extraction. The DEMS open service request report showed 10 of the 26 backlogged cases were from this non-partnering agency.

IWRCFL officials also said they are taking steps to address the backlog, they are adding staff, and two forensic examiners in training are working to become certified examiners.[8] The IWRCFL officials said the backlog has not affected its ability to be responsive and successful, as they triage their cases well, and can work on multiple cases at one time. The officials told us that they are candid with

[7] Advanced cell phone extractions include In-System Programming ISP, and chip offs (soldering and digital microscope work).

[8] The FBI examiner position was filled at the IWRCFL on September 30, 2019.

the submitting agencies about their work load, and the IWRCFL has not received complaints from participating agencies related to a backlog. As stated previously, we interviewed members from partnering agencies and in all cases, members were satisfied with the services received by the IWRCFL. This indicates that the IWRCFL has been responsive, timely and reliable. As a result, we take no exception to the 26 case backlog the IWRCFL had as of June 30, 2019; rather, we note the recent increase in backlogged cases, as we believe this trend represents a risk to the IWRCFL's mission.

Aging Report

The aging report generated from the CART database denotes cases by the number of days from when they were submitted. Factoring in the differences from the DEMS open service request report, we totaled up the number of cases by the time period open, and out of the 179 cases that should have been included in the CART aging report, as of June 30, 2019, 74 percent of the IWRCFL cases were open for less than 6 months and 26 percent were open for 6 months or more.[9] According to IWRCFL officials, they review the aging report every month and follow up on the status of aged cases. There are several reasons why a case would be open for an extended period of time, including:

- The IWRCFL needs the case agent's assistance on the case;
- A case has been opened, worked, closed, than re-opened for trial or prosecution. In the CART database the case goes back to the original date it was received;
- Different legal jurisdictions mean different rules in processing and prosecuting cases;
- Espionage cases take a long time; and
- A defense attorney claims there is privileged attorney client communication on a seized computer, and the RCFL has to work with the attorney to identify what might be privileged and filter that data out from the data that is made available to the case agent for review.

The OIG acknowledges there are legitimate reasons why a case would be open for an extended period of time. Further, we are satisfied that IWRCFL officials are periodically monitoring the aging report; and the partnering agencies we interviewed indicated the IWRCFL has been responsive, timely, and reliable. As a result, we are not providing any recommendation on this issue.

[9] According to the FY 2016 and 2017 RCFL Annual Reports, the IWRCFL received 401 service requests in FY 2016 and 389 in FY 2017. As stated previously, the FY 2018 RCFL Annual Report has not been issued.

CONCLUSION AND RECOMMENDATIONS

The Intermountain West Regional Computer Forensics Laboratory (IWRCFL) performed sufficient outreach to law enforcement communities in an effort to form partnerships, and partnering agencies were satisfied with the services received. While the IWRCFL conducted 44 presentations and 6 training courses from FY 2016 through 2019, it did not always maintain proper documentation to validate training course attendance for two training courses.

According to IWRCFL officials, it met all of its performance goals for fiscal years (FY) 2016, and all but one performance goal for each of FY 2017, 2018, and 2019. The performance goals not met were goals to increase staffing, upgrade a phone system, and in FY 2019, maintain minimal backlog and aging requests. As of June 30, 2019 the IWRCFL had 26 backlogged cases. To address the backlog, the IWRCFL plans to add staff, and two forensic examiners are currently in training to become certified examiners, however, according to the partnering agencies we spoke with, the backlog has not affected its ability to be responsive and successful.

The Cell Phone Investigative Kiosks (CPIK) at the IWRCFL did not include the training certification at the initiation of our audit and this has since been corrected. However, the FBI could not confirm all RCFLs CPIKs included the required training certification question. In addition, CPIK software updates are not being tracked. Tracking the deployment and implementing of CPIK software updates would be a best practice to ensure the updates are being done, and to aid in trouble shooting any issues that might occur as a result of an update. Finally, the LMKs at the IWRCFL were not compliant with the FBI Digital Evidence Policy Guide, since they did not include a prompt requiring users to certify they had taken self-paced training, or had received hands-on training prior to use of the LMK. Based on these findings, we make six recommendations to the FBI to improve program operations.

We recommend that the FBI:

1. Ensure that the IWRCFL maintains proper documentation to validate attendance at training courses.

2. Ensure that the LMK users have taken either self-paced training, or have received hands-on training prior to use of the LMK.

3. Ensure that all RCFLs CPIK user data logs are capturing CPIK usage.

4. Ensure that all RCFLs CPIK user forms include the training certification question.

5. Ensure that CPIK software updates are documented, including the reason for the update, when the software update was deployed, and when each RCFL has completed the update.

6. Ensure that the CPIK software updates and documentation of the updates, are communicated to the Digital Evidence Field Operations Unit.

APPENDIX 1

OBJECTIVES, SCOPE, AND METHODOLOGY

Objectives

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

Scope and Methodology

We conducted this performance audit in accordance with generally accepted government auditing standards (GAGAS). Those 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 believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

We defined the scope of our audit to be all examinations requested and completed within the fiscal years of 2016 through June 2019. In conducting our audit, we interviewed officials from the IWRCFL and from participating agencies. We also reviewed documents related to the IWRCFL organizational structure, accomplishments, and operational standards.

To assess the efficiency and effectiveness of the IWRCFL's laboratory performance, we examined the IWRCFL's progress towards achieving its annual goals. We also compared the number of participants listed on training rosters to the data the IWRCFL provided to the OIG.

To assess the effectiveness of the IWRCFL's outreach and partnerships with the law enforcement community, we interviewed representatives from the IWRCFL participating agencies to determine the effectiveness of the work conducted at the IWRCFL. To assess the controls surrounding the IWRCFL kiosk usage, we completed a walk-thru of the kiosk workstations and a demonstration of the kiosk.

To assess the IWRCFL's efforts to address any service backlog, we examined data from the IWRCFL Digital Evidence Management System (DEMS) to determine if a backlog existed. After determining the IWRCFL had a backlog of 26 cases, as of June 30, 2019, we interviewed IWRCFL staff to understand why there was a backlog, and identify the IWRCFL efforts to address it. In addition, we analyzed the IWRCFL aging report, generated from the FBI's Computer Analysis Response Team (CART) database and calculated the number of cases open by time period. We also discussed the reasons why some cases were open for long periods of time with IWRCFL officials.

Internal Controls

In this audit we performed testing, as appropriate, of internal controls significant within the context of our audit objectives. A deficiency in internal control design exists when a necessary control is missing or is not properly designed so that even if the control operates as designed, the control objective would not be met. A deficiency in implementation exists when a control is properly designed but not implemented correctly in the internal control system. A deficiency in operating effectiveness exists when a properly designed control does not operate as designed or the person performing the control does not have the necessary competence or authority to perform the control effectively.[10]

Through this 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 financial and performance information, and to ensure compliance with laws and regulations.

Computer-Processed Data

During our audit, we obtained and analyzed data from the IWRCFL's DEMS, as well as the CART database. DEMS is a laboratory information management system that includes both case management and evidence control functionality, and the CART database is used to track FBI forensic examination work from inception to completion. We reviewed this data for obvious inconsistency errors and completeness and found discrepancies. When we found discrepancies, we brought them to the attention of the IWRCFL officials and worked with them to correct the discrepancies before conducting our analyses. As a result of these efforts, we determined that the DEMS and CART data was sufficiently reliable for the purposes of this report.

[10] Our evaluation of the FBI's internal controls was not made for the purpose of providing assurance on its internal control structure as a whole. FBI's management is responsible for the establishment and maintenance of internal controls. 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.

APPENDIX 2

FEDERAL BUREAU OF INVESTIGATION RESPONSE TO THE DRAFT REPORT

U.S. Department of Justice

Federal Bureau of Investigation

Washington, D. C. 20535-0001

March 5, 2020

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 Intermountain West Regional Computer Forensics Laboratory – Salt Lake City, Utah.*

We are pleased you "found that the IWRCFL performance was generally efficient and effective" and that current and former partnering agencies you spoke to "were satisfied with the services received by the IWRCFL".

We agree that it is important to strengthen procedures for documenting training as well updating software for the Cell Phone Investigative Kiosks. In that regard, we concur with your 6 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,

Steven Pandelides
Acting Assistant Director
Operational Technology Division

Enclosure

AUDIT OF THE FEDERAL BUREAU OF INVESTIGATION'S INTERMOUNTAIN WEST REGIONAL COMPUTER FORENSICS LABORATORY – SALT LAKE CITY, UTAH 19-31

1) **Recommend that FBI Management:** Ensure that the IWRCFL maintains proper documentation to validate attendance at training courses

   FBI Response: The IWRCFL agrees with this recommendation. The IWRCFL will use Form TAR-525 (Training Attendance Roster) to document attendees at IWRCFL led/sponsored training classes held at the IWRCFL. The completed forms will be stored in a training folder in the Lab Director's office. Additionally, the completed forms will be scanned and saved on the IWRCFL's shared drive on its Admin server to ensure that the records are available for review.

2) **Recommend that FBI Management:** Ensure that the LMK users have taken either self-paced training, or have received hands -on training prior to use of the LMK.

   FBI Response: The IWRCFL agrees with this recommendation. For each LMK, the IWRCFL will use Form LTC-113 (LMK Training Certification) to maintain a log of LMK users and whether they received training when using the LMK. The logs will be used until FBIHQ-OTD finds a solution to include an electronic questionnaire which captures the training certification question and captures that data in a log.

3) **Recommend that FBI Management:** Ensure that all RCFLs CPIK user data logs are capturing CPIK usage.

   FBI Response: The IWRCFL agrees with this recommendation however, this matter is something which FBIHQ-OTD needs to consider as it addresses all RCFLs. The IWRCFL checks that CPIK user data logs are capturing CPIK usage each time it updates its CPIK machines with the newest approved Cellebrite software and/or new versions of the CPIK statistics form.

4) **Recommend that FBI Management:** Ensure that all RCFLs CPIK user forms include the training certification question.

   FBI Response: The IWRCFL agrees with this recommendation, however this matter needs to be addressed by FBIHQ-OTD as it includes all RCFLs. The IWRCFL's current CPIK statistic form on all IWRCFL CPIKs includes the training certification question.

5) **Recommend that FBI Management:** Ensure that CPIK software updates are documented, including the reason for the update, when the software update was deployed, and when each RCFL has completed the update.

FBI Response: The IWRCFL agrees with this recommendation. The IWRCFL is capturing this information for each IWRCFL CPIK on an Excel spreadsheet (CPIK Workstation Tracking) maintained on the IWRCFL admin server which is available to all IWRCFL facilities. FBIHQ-OTD would need to address the issue of whether all other RCFLs are capturing this data.

6) **Recommend that FBI Management:** Ensure that the CPIK software updates and documentation of the updates, are communicated to the Digital Evidence Field Operations Unit.

FBI Response: The IWRCFL agrees with this recommendation. The IWRCFL is documenting CPIK software updates in an Excel spreadsheet maintained on its admin server. This information can/will be provided to FBIHQ-OTD upon instructions from them as to the frequency and target for providing the information.

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. In response to our audit report, the FBI agreed with our recommendations and discussed the actions it will implement in response to our findings. As a result, the status of the report is resolved. The following provides the OIG analysis of the response and summary of actions necessary to close the report.

Recommendations for the FBI:

1. **Ensure that the IWRCFL maintains proper documentation to validate attendance at training courses.**

   Resolved. The FBI agreed with our recommendation. In its response, the FBI stated that the IWRCFL will use a Training Attendance Roster to document attendees at IWRCFL led or sponsored training classes held at the IWRCFL. The completed forms will be stored in the Laboratory Director's office. Additionally, the completed forms will be scanned and saved on the IWRCFL's server to ensure that the records are available for review.

   This recommendation can be closed when the FBI provides documentation supporting the use of the Training Attendance Roster and the Rosters being stored both in the Laboratory Director's office and on the server.

2. **Ensure that the LMK users have taken either self-paced training, or have received hands-on training prior to use of the LMK.**

   Resolved. The FBI agreed with our recommendation. In its response, the FBI stated for each LMK (Loose Media Kiosk), the IWRCFL will use the LMK Training Certification form to maintain a log of LMK users and whether they received training when using the LMK. The logs will be used until FBI's Operational Technology Division (FBIHQ-OTD) finds a solution to include an electronic questionnaire, which captures the training certification question and captures that data in a log.

   This recommendation can be closed when the FBI provides documentation supporting the IWRCFL's use of the LMK Training Certification form to maintain a log of LMK users, and whether the users received training when using the LMK. In addition, the FBI needs to provide documentation showing its efforts to find a solution to include an electronic questionnaire that captures the training certification question and the data in a log.

3. Ensure that all RCFLs CPIK user data logs are capturing CPIK usage.

Resolved. The FBI agreed with our recommendation. In its response, the FBI stated while it agrees with this recommendation, this matter is something that FBIHQ-OTD needs to consider as it addresses all RCFLs. The FBI also said the IWRCFL checks that CPIK (Cell Phone Investigative Kiosk) user data logs are capturing CPIK usage each time it updates its CPIK machines with the newest approved software and new versions of the CPIK statistics form.

This recommendation can be closed when FBIHQ-OTD provides documentation showing it has reached out to all RCFLs and verified their CPIK user data logs are, or are not, capturing CPIK usage. For RCFLs that have CPIKs that are not capturing CPIK usage, they should address the problem. In addition, the FBI needs to provide supporting documentation showing the IWRCFL is checking to ensure CPIK user logs are capturing CPIK usage each time it updates its CPIK machines with the newest approved software.

4. Ensure that all RCFLs CPIK user forms include the training certification question.

Resolved. The FBI agreed with our recommendation. In its response, the FBI stated that while it agrees with this recommendation, this matter is something that FBIHQ-OTD needs to consider as it addresses all RCFLs.

This recommendation can be closed when the FBI provides evidence it has reached out to all RCFLs to verify if their CPIK user forms include the training certification question, and, for those that do not, provide evidence the training certification question has been added.

5. Ensure that CPIK software updates are documented, including the reason for the update, when the software update was deployed, and when each RCFL has completed the update.

Resolved. The FBI agreed with our recommendation. In its response, the FBI stated the IWRCFL is capturing this information for each IWRCFL CPIK on an Excel Spreadsheet, which will be maintained on the IWRCFL sever. In its response, the FBI also said FBIHQ-OTD would need to address the issue of whether all other RCFLs are capturing this data.

This recommendation can be closed when the FBI provides evidence that it is documenting CPIK software updates, including the reason for the update, when the update was deployed, and when the update was completed at each RCFL.

6. Ensure that the CPIK software updates and documentation of the updates, are communicated to the Digital Evidence Field Operations Unit.

Resolved. The FBI agreed with our recommendation. In its response, the FBI said the IWRCFL is documenting CPIK software updates in an Excel spreadsheet maintained on its server. The FBI stated that this information will be provided to FBIHQ-OTD according to instructions on the frequency and target of providing the information.

This recommendation can be closed when the FBI provides evidence that all RCFLs are documenting software updates and communicating the completion of all software updates to the Digital Evidence Field Operations Unit.

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.

To report allegations of waste, fraud, abuse, or misconduct regarding DOJ programs, employees, contractors, grants, or contracts please visit or call the **DOJ OIG Hotline** at oig.justice.gov/hotline or (800) 869-4499.

U.S. DEPARTMENT OF JUSTICE OFFICE OF THE INSPECTOR GENERAL
950 Pennsylvania Avenue, NW
Washington, DC 20530 0001

Website	**Twitter**	**YouTube**
oig.justice.gov	@JusticeOIG	JusticeOIG

Also at Oversight.gov