A New Tactic in the Fight on Fraud; Federal auditors launch forensics teams

When most people think of forensics, they think of the TV show “CSI” where fibers can unravel a suspect’s alibi in 60 minutes flat, less commercials.

Now, federal auditors are starting to use forensic methods to root out fraud.

Inspector general criminal investigators have used forensics techniques for years to investigate fraud, embezzlement, cyber espionage and other crimes. But not IG auditors — until recently.

Forensic auditing combines advanced computer investigative work — such as data mining and analysis, combing the content of computer hard drives, and conducting in-depth Web searches — with traditional auditing and accounting techniques to investigate fraud.

The General Services Administration inspector general’s office last summer rolled out a five-person team devoted to using forensic auditing techniques to dig up evidence of fraud. Other agencies, such as Defense Department agencies, NASA and the Environmental Protection Agency, are doing the same. And still other agencies are considering starting new forensics auditing teams at the urging of the National Procurement Fraud Task Force, an interagency group that promotes the prevention, early detection and prosecution of fraud.

“Forensic auditing is the way of the future,” said Brian Miller, GSA’s inspector general and co-chair of the National Procurement Fraud Task Force.

Forensics auditing represents a new approach to auditing because it attempts to find — through forensic methods — improper activity.

Traditional audits don’t do that. They can uncover fraud, but they don’t seek it out. Instead, they look at records to check if prices charged on contracts were reasonable or if contractors have compliant accounting systems in place, said Conan Albrecht, a professor who teaches forensic auditing techniques at Brigham Young University in Provo, Utah.

As new computer-based data-mining techniques have evolved, new possibilities have emerged for auditors to be more proactive in looking for improper activity such as fraud. Now, auditors have tools that can allow them to more easily and regularly analyze and compare vast sets of data to reveal patterns of behavior that would evade traditional audit reviews.

“Forensic auditing is a new way of going about it that will find both anomalies and fraud,” Albrecht said. “It allows auditors to be more proactive about their work, rather than reactive and waiting for someone to give us a tip.”

Forensic auditors try to match symptoms of fraud and they think about how perpetrators might defraud the system and then run tests to see if the symptoms of that kind of fraud show up.

Most fraud investigation cases start with a tip called in on a hot line, said Ted Stehney, who directs the forensic auditing team at the GSA IG’s office. By being more proactive —through regular forensic audits — auditors can help keep some fraud from ballooning into multimillion-dollar cases, he said.

A New Tactic in the Fight on Fraud; Federal auditors launch forensics teams

A New Tactic in the Fight on Fraud; Federal auditors launch forensics teams - GSA Office of Inspector General

Connecting the dots

Forensic techniques allow auditors to compare various sets of data more easily and to connect the dots that point to a possible crime more easily, Stehney said.

For example, an auditor applying traditional auditing methods might examine a database of vendor payments and not find much. An auditor using forensic techniques, however, could view that database alongside other databases and spot anomalies of interest. For instance, examining a database of vendor payments alongside a database of employee bank accounts where paychecks are deposited might find that a vendor payment was directed to an employee's personal account. By regularly examining and comparing various databases like that, auditors can find red flags that could indicate fraud — and not have to wait for tips to be called into a hot line, he said.

Stehney admits that drilling for fraud is a bit like drilling for oil: Auditors are likely to come up with a lot of dry wells.

"I think we'll have the opportunity to find more fraud, but I also think one of the byproducts of it is a lot of waste will surface in the dry holes we drill," Stehney said.

One challenge auditors face is that government databases don't often mesh for easy data mining, said Tom Caulfield, assistant IG for investigations at the National Reconnaissance Office. In addition, privacy regulations prevent some databases from being linked for this kind of a search, said Caulfield, who lectures on using forensic techniques for the National Procurement Fraud Task Force.

Some successes

The GSA IG's forensics auditing team has one success already: a case of employee embezzlement involving a phony company used to mask 13 illicit transfers of government funds. The GSA employee, a supervisory accountant named Michael Harrington, was indicted in October on charges he stole nearly $600,000 while working at GSA's office in Kansas City, Mo.

Stehney declined to give details on how forensic auditing was used because the case is ongoing and it would reveal methodologies that could help criminals avoid detection.

The emergence of forensics auditing likely will impact the way auditors are trained in the future, Stehney said.

Traditional auditors are not expected to proactively seek out fraud. Instead, they try to ensure the government gets a good price, that government accounts are accurate, that internal controls are in place to ensure verifiable and accurate financial transactions and records, and that contractors' financial systems comply with government standards.

Forensic auditors, on the other hand, are seeking out fraud. So they need training on a different set of skills and techniques: data mining, technology skills, statistics and investigation skills, Albrecht said. They also must ask different types of questions said Steve Linick, deputy chief of the Justice Department's fraud division and director of the National Procurement Fraud Task Force.

By ELISE CASTELLI, Federal Times

A New Tactic in the Fight on Fraud; Federal auditors launch forensics teams - GSA Office of Inspector General

A new tactic in the fight on fraud

Federal auditors launch forensics teams

By ELISE CASTELLI
ecastelli@federaltimes.com

When most people think of forensics, they think of the TV show "CSI" where fibers can unravel a suspect's alibi in 60 minutes flat, less commercials.

Now, federal auditors are starting to use forensic methods to root out fraud.

Inspector general criminal investigators have used forensics techniques for years to investigate fraud, embezzlement, cyber espionage and other crimes. But not IG auditors — until recently.

Forensic auditing combines advanced computer investigative work — such as data mining and analysis, combing the content of computer hard drives, and conducting in-depth Web searches — with traditional auditing and accounting techniques to investigate fraud.

The General Services Administration inspector general's office last summer rolled out a five-person team devoted to using forensic auditing techniques to dig up evi-

See FORENSICS, Page 19

Forensics

From Page 1

dence of fraud. Other agencies, such as Defense Department agencies, NASA and the Environmental Protection Agency, are doing the same. And still other agencies are considering starting new forensics auditing teams at the urging of the National Procurement Fraud Task Force, an interagency group that promotes the prevention, early detection and prosecution of fraud.

"Forensic auditing is the way of the future," said Brian Miller, GSA's inspector general and co-chair of the National Procurement Fraud Task Force.

Forensics auditing represents a new approach to auditing because it attempts to find — through forensic methods — improper activity.

Traditional audits don't do that. They can uncover fraud, but they don't seek it out. Instead, they look at records to check if prices charged on contracts were reasonable or if contractors have compliant accounting systems in place, said Conan Albrecht, a professor who teaches forensic auditing techniques at Brigham Young University in Provo, Utah.

As new computer-based data-mining techniques have evolved, new possibilities have emerged for auditors to be more proactive in looking for improper activity such as fraud. Now, auditors have tools that can allow them to more easily and regularly analyze and compare vast sets of data to reveal patterns of behavior that would evade traditional audit reviews.

Ted Stebney, left, director of the forensic auditing team at the office of the General Services Administration inspector general, discusses a case with statistician Sarah Breen, center, and audit manager Patricia Sheehan.

"Forensic auditing is a new way of going about it that will find both anomalies and fraud," Albrecht said. "It allows auditors to be more proactive about their work, rather than reactive and waiting for someone to give us a tip."

Forensic auditors try to match symptoms of fraud and they think about how perpetrators might defraud the system and then run tests to see if the symptoms of that kind of fraud show up.

Most fraud investigation cases start with a tip called in on a hot line, said Ted Stebney, who directs the forensic auditing team at the GSA IG's office. By being more proactive — through regular forensic audits — auditors can help keep some fraud from ballooning into multimillion-dollar cases, he said.

Connecting the dots

Forensic techniques allow auditors to compare various sets of data more easily and to connect the dots that point to a possible crime more easily, Stebney said.

For example, an auditor applying traditional auditing methods might examine a database of vendor payments and not find much. An auditor using forensic techniques, how-

A New Tactic in the Fight on Fraud; Federal auditors launch forensics teams - GSA Office of Inspector General

ever, could view that database alongside other databases and spot anomalies of interest. For instance, examining a database of vendor payments alongside a database of employee bank accounts where paychecks are deposited might find that a vendor payment was directed to an employee's personal account. By regularly examining and comparing various databases like that, auditors can find red flags that could indicate fraud — and not have to wait for tips to be called into a hot line, he said.

Stehney admits that drilling for fraud is a bit like drilling for oil: Auditors are likely to come up with a lot of dry wells.

"I think we'll have the opportunity to find more fraud, but I also think one of the byproducts of it is a lot of waste will surface in the dry holes we drill," Stehney said.

One challenge auditors face is that government databases don't often mesh for easy data mining, said Tom Caulfield, assistant IG for investigations at the National Reconnaissance Office. In addition, privacy regulations prevent some databases from being linked for this kind of a search, said Caulfield, who lectures on using forensic techniques for the National Procurement Fraud Task Force.

Some successes

The GSA IG's forensics auditing team has one success already: a case of employee embezzlement involving a phony company used to mask 13 illicit transfers of government funds. The GSA employee, a supervisory accountant named Michael Harrington, was indicted in October on charges he stole nearly $600,000 while working at GSA's office in Kansas City, Mo.

Stehney declined to give details on how forensic auditing was used because the case is ongoing and it would reveal methodologies that could help criminals avoid detection.

The emergence of forensics auditing likely will impact the way auditors are trained in the future, Stehney said.

Traditional auditors are not expected to proactively seek out fraud. Instead, they try to ensure the government gets a good price, that government accounts are accurate, that internal controls are in place to ensure verifiable and accurate financial transactions and records, and that contractors' financial systems comply with government standards.

Forensic auditors, on the other hand, are seeking out fraud. So they need training on a different set of skills and techniques: data mining, technology skills, statistics and investigation skills, Albrecht said. They also must ask different types of questions said Steve Linick, deputy chief of the Justice Department's fraud division and director of the National Procurement Fraud Task Force. ■