March 2011

COMBATING CHILD PORNOGRAPHY

Steps Are Needed to Ensure That Tips to Law Enforcement Are Useful and Forensic Examinations Are Cost Effective

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-11-334, a report to congressional committees

Why GAO Did This Study

The Department of Justice (DOJ) reports that online child pornography crime has increased. DOJ funds the National Center for Missing and Exploited Children (NCMEC), which maintains the CyberTipline to receive child pornography tips. The Providing Resources, Officers, and Technology To Eradicate Cyber Threats to Our Children Act of 2008 (the Act) contains provisions to facilitate these investigations and create a national strategy to prevent, among other things, child pornography. The Act directed GAO to report on actions to minimize duplication and enhance federal expenditures to address this crime. This report examines (1) the extent to which NCMEC determines the usefulness of tips; (2) mechanisms to help law enforcement coordination (i.e., deconfliction); and (3) the extent to which agencies are addressing factors that federal law enforcement reports may inhibit investigations. GAO analyzed the Act and spoke to law enforcement officials who investigate these crimes, selected to reflect geographic range, among other things. Although these interviews cannot be generalized, they provided insight into investigations.

What GAO Recommends

GAO recommends that NCMEC enhance its processes to collect feedback to improve tips and that DOJ assess the costs and benefits of steps agencies take to ensure the integrity of forensic analysis. NCMEC and DOJ generally concurred with our recommendations and discussed actions to address them.

View GAO-11-334 or key components.
For more information, contact Eileen Larence at (202) 512-8777 or larencee@gao.gov.

What GAO Found

NCMEC takes steps to obtain feedback from law enforcement on the usefulness of CyberTipline reports; however, it does not systematically collect information on how useful individual reports are for initiating and advancing investigations or about information gaps that limit reports' usefulness. For instance, NCMEC solicits feedback via e-mail or in person quarterly from federal law enforcement liaisons at NCMEC about the overall usefulness of CyberTipline reports. However, according to many law enforcement officials GAO contacted, information in a CyberTipline report may not contain an image of apparent child pornography or may contain old data. NCMEC officials said that they are interested in obtaining additional feedback to enhance the usefulness of its reports and could explore additional methods to gather such information, such as creating a systematic process for obtaining feedback from federal law enforcement. Enhancing its processes for collecting feedback on the usefulness of CyberTipline reports could help NCMEC ensure that reports are as useful as possible to law enforcement.

Existing deconfliction mechanisms generally prevent pursuit of the same suspects but are fragmented; DOJ is in the early stages of developing a system to address this fragmentation. Many law enforcement officials GAO contacted reported using various nonautomated (e.g., task forces) and automated (e.g., investigative systems) mechanisms to avoid duplication of effort in investigations. But these officials reported that there is not a single automated system that provides comprehensive case information and deconfliction, which can contribute to difficulties coordinating investigations. As mandated in the Act, DOJ is developing a national system to, among other things, provide law enforcement with a single deconfliction tool. Specifically, DOJ is conducting a needs assessment—which it plans to complete in 12 to 24 months—to use as a basis for system development. However, because DOJ is waiting on the results of the needs assessment to begin system development, it may be several years before the system is operational.

Backlogs in the forensic analysis of digital evidence can delay or hinder online child pornography investigations; assessing the costs and benefits of taking extra steps to ensure the integrity of forensic analysis could help determine if there are efficiencies that could reduce backlogs. Forensic analysis of digital evidence consists of the review of information from digital media, such as hard drives, and can prove online child pornography crime. Several factors may contribute to backlogs in forensic analysis, including the steps federal law enforcement agencies believe enhance the integrity of analysis, such as making exact copies of digital evidence to discourage tampering. The FBI takes additional steps it believes enhance integrity, such as separating the forensic examination from the investigation. However, some federal officials and prosecutors GAO spoke with differed on the need for such steps. According to DOJ, the national strategy's working group is in a good position to address backlog issues and having this group assess the costs and benefits of steps taken to ensure the integrity of forensic analysis could help it determine potential efficiencies that could reduce backlogs.