United States General Accounting Office

GAO

Report to the Chairman, Committee on Government Reform, House of Representatives

June 2003

VIDEO SURVEILLANCE

Information on Law Enforcement's Use of Closed-Circuit Television to Monitor Selected Federal Property in Washington, D.C.

GAO-03-748

June 2003

VIDEO SURVEILLANCE

Information on Law Enforcement's Use of Closed-Circuit Television to Monitor Selected Federal Property in Washington, D.C.

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-03-748, a report to the Chairman, Committee on Government Reform, House of Representatives

Why GAO Did This Study

Law enforcement use of closed-circuit television (CCTV) as a tool to fight crime and terrorism has become more prevalent over time. Civil liberties advocates have raised privacy concerns about its use.

This report describes (1) the Metropolitan Police Department's and the United States Park Police's implementation of CCTV to monitor public spaces in the Washington, D.C., metropolitan area such as the National Mall and (2) the management controls they established to address privacy concerns. GAO also identified experiences of selected CCTV users that provide insights to help ensure the proper CCTV use.

www.gao.gov/cgi-bin/getrpt?GAO-03-748.

To view the full report, including the scope and methodology, click on the link above. For more information, contact Rich Stana at (202) 512-8777 or stanar@gao.gov.

What GAO Found

The Metropolitan Police Department of the District of Columbia's CCTV system was implemented, among other things, to facilitate crowd management during large demonstrations; however, officials indicated that the system could also be used to help combat terrorism. The system is used on an as-needed basis for such things as crowd control and when the national terrorism threat level is set to high alert (code orange). The Metropolitan Police Department obtained public comments on its implementation of CCTV. In contrast, the United States Park Police uses CCTV, among other purposes, primarily to combat terrorism and operates its CCTV system on a continuous basis. The United States Park Police has not obtained public input on its implementation of CCTV, but it is considering providing the public an opportunity to provide input.

The Metropolitan Police developed regulations and the United States Park Police developed draft policies for operating their CCTV systems. Both include management controls that address the protection of privacy and the proper use of CCTV such as the need for supervision to protect against improper use and the establishment of procedures to control access to CCTV images.

The experiences of CCTV users in the United Kingdom (UK) and selected U.S. cities revealed best practices for the implementation and use of CCTV. For example, UK and U.S. officials considered providing training and audits helpful to ensuring proper use of CCTV. Officials in the UK and others shared their best practices that include (1) operating CCTV systems in an open environment helps to alleviate privacy concerns; (2) having uniform standards helps to reassure the public that safeguards are in place when utilizing CCTV and provides CCTV operators guidance for proper use; and (3) establishing realistic, clear, and measurable goals helps make CCTV systems more effective and can also reassure the public about its use.

A CCTV Control Room

Source: Metropolitan Police Department of Washington, D.C.

Contents

Figures

Abbreviations

ABA	American Bar Association
ACLU	American Civil Liberties Union
CCTV	closed-circuit television
EPIC	Electronic Privacy Information Center
IACP	International Association of Chiefs of Police
MPDC	Metropolitan Police Department of the District of Columbia
SIA	Security Industry Association
UK	United Kingdom

GAO
Accountability * Integrity * Reliability

United States General Accounting Office
Washington, DC 20548

June 27, 2003

The Honorable Thomas Davis
Chairman
Committee on Government Reform
House of Representatives

Dear Mr. Chairman:

Surveillance video cameras have become a growing presence in the public arena over the past several decades in stores, civic buildings, and even on public streets. As part of this trend, law enforcement has increasingly used closed-circuit television (CCTV)—which involves a linked system of cameras able to be viewed and operated from a control room—as a tool for fighting crime. Police departments in the United States commonly use CCTV to, among other things, deter, detect, and investigate crime and control crowds. Since September 11, 2001, law enforcement has also begun to use CCTV to combat terrorism. In particular, both the Metropolitan Police Department of the District of Columbia (MPDC) and the National Park Service's United States Park Police within the Department of the Interior have used CCTV systems to monitor certain public spaces[1] under their jurisdictions in Washington, D.C. For example, the United States Park Police has responsibility for policing the area around the White House, the Franklin Delano Roosevelt Memorial, the Washington Monument, the Lincoln Memorial, the Jefferson Memorial, and the Vietnam Veterans War Memorial.

CCTV use in public spaces and varying methods of implementation have raised concerns among critics of CCTV use. Specifically, civil liberties advocates have raised issues concerning CCTV's potential impact on individual privacy as well as the potential for inappropriate use of CCTV systems and the mishandling of CCTV images. In addition, these advocates expressed concern about using the technology when its effectiveness for law enforcement use has not been proven. Civil liberties advocates propose that controls are needed to help ensure the protection of individual privacy and the proper use of CCTV systems. The American Bar

[1]For this report, public spaces are defined as public parks, public streets, and commercial/business districts.

Association[2] (ABA) and other organizations have developed guidelines for CCTV users that address some of the issues raised by civil liberties advocates through the use of management controls. These include developing written operating protocols, establishing supervision and training requirements, providing for public notification, and requiring periodic audits.

This report responds to a request from former Representative Constance A. Morella in her capacity as Chair of the House Government Reform Subcommittee on the District of Columbia, asking us to examine several issues surrounding the use of CCTV to monitor public spaces. As discussed with your office, we are sending you this report because of your oversight responsibility for the District of Columbia. This report discusses:

- How MPDC and the United States Park Police have implemented their CCTV systems.
- How MPDC's and the United States Park Police's management controls respond to issues raised regarding individual privacy and the use of CCTV.
- Whether the experiences of other CCTV users in the United States and the United Kingdom (UK) offer useful insights for MPDC and the United States Park Police regarding the issues that have been raised.

To determine how MPDC and the United States Park Police have implemented their CCTV systems, we interviewed MPDC and United States Park Police officials and reviewed relevant laws, regulations, policies, and other documents. To determine how MPDC's and the United States Park Police's management controls responded to issues raised regarding the use of CCTV, we interviewed MPDC and United States Park Police officials. We did not evaluate or test compliance with MPDC's or the United States Park Police's management controls. We also interviewed representatives from the ABA, the American Civil Liberties Union[3] (ACLU), the Electronic Privacy Information Center[4] (EPIC), the

[2]ABA is a nationwide organization that, among other things, provides law school accreditation, programs to assist lawyers and judges in their work, and initiatives to improve the legal system for the public. ABA published guidance for law enforcement's use of CCTV and other technologies in its "Standards for Criminal Justice: Electronic Surveillance, Part B: Technologically-Assisted Physical Surveillance."

[3]ACLU is a nationwide, nonpartisan organization whose stated mission is to defend the principles of liberty and equality embodied in the Bill of Rights.

[4]EPIC is a public interest research center located in Washington, D.C. It was established in 1994 to, among other things, focus public attention on emerging civil liberties issues.

International Association of Chiefs of Police[5] (IACP), and the Security Industry Association[6] (SIA) to obtain their views on the use of CCTV.

To learn about the experiences of CCTV users in other U.S. cities, we obtained documentation and interviewed officials and representatives in four U.S. locations—Baltimore, Maryland; Tampa, Florida; Columbia, South Carolina; and Virginia Beach, Virginia. These locations were selected for one or more of the following reasons: they had used CCTV for some time, had recently initiated the use of CCTV, were located close to D.C., or were using other technology in conjunction with CCTV. In addition, we visited the UK—a country that has used CCTV extensively to address crime and terrorism. We toured the control rooms and observed the operations of CCTV systems in some U.S. cities and in all of the UK locations visited. See appendix I for a more detailed discussion of our scope and methodology.

We performed our audit work from August 2002 to May 2003 in Washington, D.C., and the selected locations mentioned earlier, in accordance with generally accepted government auditing standards. We requested comments on a draft of this report from MPDC and the Department of the Interior, and their comments have been incorporated as appropriate.

Results in Brief

MPDC and the United States Park Police have their own CCTV systems implemented independently of each other. The purpose of MPDC's CCTV system is to facilitate crowd management and allocate police resources during major public events and demonstrations with the intended purpose of deterring crime such as destruction of property. The system is also used to coordinate traffic control on an as-needed basis. Finally, the system is used during exigent circumstances. In this regard, a senior MPDC official said that CCTV has the dual purpose of helping to combat terrorism. The D.C. City Council is considering whether CCTV might be used to fight crime in neighborhoods. According to its regulations, MPDC's system is to

[5]IACP is a nonprofit membership organization of police executives whose leadership consists of the operating chief executives of international, federal, state, and local agencies of all sizes.

[6]SIA is an international trade association whose mission is to, among other things, effectively and responsibly promote the use of electronic security equipment in commercial, institutional, commercial, governmental, and residential markets.

be operated on a limited basis during certain events such as major demonstrations or exigent circumstances such as when the Department of Homeland Security's national threat level is increased to high alert (code orange). MPDC obtained public comments on its implementation of CCTV. In contrast, the United States Park Police states that CCTV is to be used to counter terrorism but recognizes that it can be used to deter and detect crime as well. The United States Park Police is operating its system on a continuous basis. The United States Park Police has not obtained public input on the implementation of its CCTV system; however, it is considering doing so. MPDC has disclosed the locations of its cameras to the public, whereas the United States Park Police has chosen not to do so because of concerns about vandalism and concerns that individuals may attempt to defeat the system. For civil liberty advocates concerned about CCTV use, the unpredictability of how MPDC and the United States Park Police might use their CCTV systems, where it might be used, and when it might be used, contribute to their uneasiness about its use and a desire for controls on its use.

MPDC has adopted regulations, and the United States Park Police is in the process of developing a policy that includes management controls for operating their CCTV systems. According to officials from both police forces, they incorporated suggestions from guidelines published by the ABA, IACP, or SIA when developing their regulations and policies. MPDC's regulations and the United States Park Police's proposed policy include management controls such as providing for training and periodic audits to address concerns raised about improper use of CCTV systems. In addition, MPDC has received feedback from the public on its regulations. The ABA reviewed the draft regulations and indicated that it complies with the ABA's standards. However, a nonprofit scholarship and advocacy organization called the Constitution Project also reviewed MPDC's regulations and concluded that the regulations lacked clarity and specificity in some areas, such as training of CCTV operators. The United States Park Police's policy is in draft form and has not been reviewed outside of the Department of the Interior.

The experiences of CCTV users in the UK and the selected U.S. cities revealed best practices regarding the implementation and use of CCTV. For example, UK and U.S. officials considered providing training and conducting audits helpful to ensuring proper use of CCTV. Because of their extensive use of CCTV, UK officials were able to provide more experiences from which to learn and could offer useful insights for CCTV use. Officials in the UK shared their views that (1) operating CCTV systems in an open environment helps to alleviate privacy concerns;

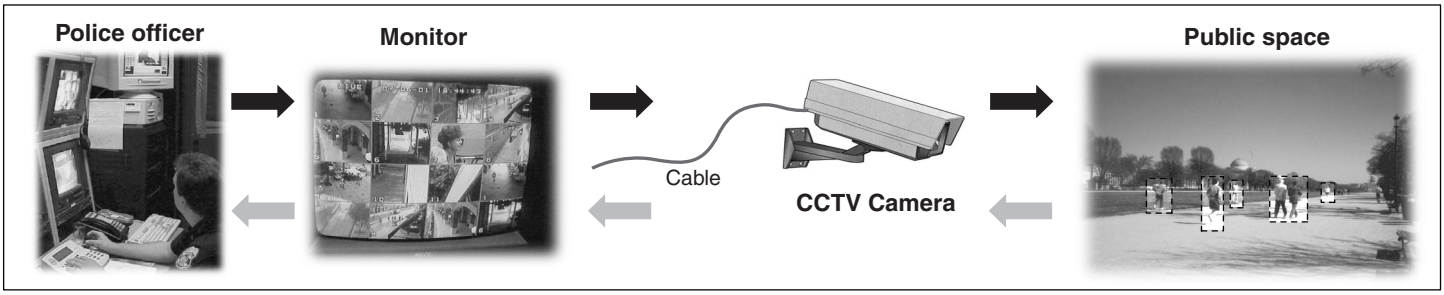
(2) having uniform standards helps to reassure the public that safeguards are in place when utilizing CCTV and provides CCTV operators guidance for proper use; and (3) establishing clear, realistic, and measurable goals helps make CCTV systems more effective and can also reassure the public about its use. Clear and measurable goals identify the problems to be addressed by CCTV and can include a range of measures to determine whether goals have been achieved, such as the change in crime levels or the change in public attitudes about crime. Researchers and others recognize the importance of measuring effectiveness to justify the potential impact on individuals' civil liberties and the costs associated with its use. At the same time, most CCTV users have not statistically measured the effectiveness of their CCTV systems and could only provide anecdotal evidence to demonstrate its effectiveness. CCTV users both in the UK and the selected U.S. cities told us that the effectiveness of CCTV is difficult to measure.

We provided a draft of this report to and received comments from officials representing MPDC and the Department of the Interior. Officials from both departments generally agreed with the report and our presentation of information regarding their CCTV use. The Department of the Interior provided technical comments, which were included as appropriate. MPDC had no technical corrections.

Background

CCTV is a visual surveillance technology designed for monitoring a variety of environments and activities. CCTV systems typically involve a dedicated communications link between cameras and monitors. Digital camera and storage technologies are rapidly replacing traditional analog systems. A CCTV system involves a linked system of cameras able to be viewed and operated from a control room.

Figure 1: Key Aspects of a CCTV System



Source: Tampa Police Department, Lachlan Cranswick, and GAO.

CCTV systems have evolved considerably over time and tend to fall into three different generations. The first generation consisted of wide-angle, fixed cameras (referred to as shoe boxes) that were targeted to crime hotspots. The second generation consisted of cameras that could be moved using a joystick in the control center focused on specific events or people, zooming in for closer scrutiny. The third generation uses both types of cameras with the additional capabilities to include software such as facial recognition or license plate recognition.[7] Relatively new features in CCTV technology that enhance its power and scope include night vision cameras, computer-assisted operations, and motion detectors. A camera that is integrated with a motion detection system would, for example, enable alerted law enforcement staff in a control room to remotely investigate potential security incidents such as a terrorist placing a package in an isolated location. Most CCTV systems are actively monitored by security or law enforcement personnel in a centralized setting, or they can be passively taped for future viewing if needed (such as in the event of a robbery).

The private sector began using CCTV in the early 1960s, first in banks, and later in commercial buildings. By the 1970s, CCTV was deployed in hospitals, all-night convenience stores, and many other commercial areas.

[7]Facial recognition technology identifies people by the sections of the face that are less susceptible to alteration-the upper outlines of the eye sockets, the areas around the cheek-bones, the sides of the mouth. Systems using this technology capture facial images from video cameras and generate templates for comparing a live facial scan to a stored template. License plate recognition software recognizes vehicle shape and 'looks' for a license plate. If the license plate number is located in a centralized database, the CCTV system triggers an alarm for appropriate personnel to take action. At the time of our review, MPDC and the United States Park Police did not use either of these technologies.

The private sector also began to use CCTV in retail stores to monitor for shoplifters and in hotels to help secure the safety of their guests. CCTV technology advanced during the 1980s with the introduction of video recorders, and even more in the 1990s with the introduction of digital technology. CCTV is also used in public safety-related applications across the United States, including traffic control, special events, public transportation, and public schools.

CCTV use by law enforcement to fight crime and terrorism is an evolving application of the technology. According to a number of reports, CCTV can benefit law enforcement in many ways. A survey of law enforcement agencies conducted by the IACP found that CCTV was useful in areas such as investigative assistance and evidence gathering. The survey identified other law enforcement benefits from CCTV use such as reducing time in court for officers, protecting police officers against claims of police misconduct, and using recorded images to train officers. A report by RAND[8] noted that proponents of video and similar types of surveillance claim that it prevents crime by deterrence, especially when overt surveillance activities remind potential criminals of police presence and observation. The same report also states that, if an area under surveillance becomes a crime scene, the surveillance can both alert police to the need for an operational response and/or provide evidence for subsequent criminal investigation and prosecution. A study commissioned by the SIA also stated that CCTV has the ability to enhance law enforcement capabilities by enabling officers to be deployed in areas that require more traditional police work (such as foot patrols where officers can interact with individuals), enabling the CCTV cameras to be used for general surveillance.

In the context of law enforcement surveillance activities, a common conception of privacy stems from criminal cases interpreting the Fourth Amendment of the Constitution. The Fourth Amendment protects people from unreasonable searches and seizures. According to the Supreme Court, if the person under surveillance has a reasonable expectation of privacy, the Fourth Amendment applies, and a warrant is generally required to conduct a lawful search. Conversely, if the person under surveillance does not have a reasonable expectation of privacy, the Fourth Amendment does not apply, and no warrant is required for police

[8]RAND is a nonprofit institution that helps improve policy and decision-making through research and analysis.

surveillance.[9] Applying these principles, the 10th Circuit Court of Appeals upheld the use of surveillance cameras placed on a public street without a warrant on grounds that "activity a person knowingly exposes to the public is not a subject of Fourth Amendment protection, and thus, is not constitutionally protected from observation."[10]

While there is generally no reasonable expectation of privacy under the Fourth Amendment for activities visible to the public, the ACLU and EPIC have argued that the use of surveillance systems to monitor public spaces may nevertheless infringe upon freedom of expression under the First Amendment. There does not appear to be any federal case law interpreting whether police use of video surveillance devices may infringe upon First Amendment rights. However, ACLU and EPIC believe that CCTV might "chill" protesters from demonstrating in public spaces such as on the National Mall and elsewhere in D.C. knowing that their images might be captured on police recordings.[11] There is also concern that CCTV cameras equipped with enhanced features, such as zoom capabilities, may give police the ability to read and record the print on political fliers being distributed in public places and to identify individuals engaged in political speech, which, in their view, undercuts the ability of citizens to engage in anonymous free speech.[12]

[9]*See Katz v. United States*, 389 U.S. 347, 360-61 (1967) (Harlan, J., concurring).

[10]*United States v. Jackson*, 213 F.3d 1269, 1281 (10th Cir. 2000), *remanded for further consideration of the sentence imposed*, 531 U.S. 1033 (2000). On remand, the 10th Circuit upheld the prior decision except with respect to the sentencing issue. *United States v. Jackson*, 240 F.3d 1245, 1247 n.2 (10th Cir. 2001).

[11]Although this case did not involve police use of video surveillance technology, the Supreme Court in *Laird v. Tatum*, 408 U.S. 1, 10 (1972) held that protesters' First Amendment rights could not be chilled by "the mere existence, without more, of a governmental investigative and data-gathering activity." The plaintiffs in *Laird* were political activists, who alleged that the Department of the Army's surveillance activities deterred them from exercising their First Amendment rights. The Supreme Court held that the plaintiffs lacked standing to sue because their alleged injury was too speculative, arising not from any specific action taken against them, but merely from their knowledge that the Army was engaged in surveillance activities.

[12]A ban on anonymous free speech was struck down in *McIntyre v. Ohio Elections Commission*, 514 U.S. 334 (1995). In that case, the Supreme Court declared unconstitutional an Ohio election law requiring the names and addresses of authors to be printed on political leaflets. Citing a longstanding tradition of anonymous free speech, the Court held that there was no overriding state interest to require the authors to identify themselves.

ACLU and EPIC officials said that they would like to see controls in place to help guard against improper use of CCTV systems and the mishandling of CCTV images. In addition, ACLU officials said that controls directing the use of CCTV should contain specific provisions for protecting CCTV images that include whether CCTV images are being recorded, under what conditions, and how long the recordings are retained, as well as criteria for access to CCTV images by the government or the public. An EPIC official also said that controls should address access, storage, and disclosure of records.

In the UK, CCTV and video surveillance have been used extensively. As of 2002, about 75 cities were using CCTV to monitor urban centers, and approximately 95 percent of all local governments were considering its use as a law enforcement tool. In 1990, according to the UK Home Office,[13] the UK had approximately three CCTV systems operated by local governments comprised of about 100 cameras. By the end of 2002, Home Office officials estimated that the UK had approximately 500 CCTV systems operated by local governments comprised of about 40,000 cameras. Nonlaw enforcement staff generally operate the CCTV systems in the locations we visited in the UK. In most cases, the systems were set up to address street-type crimes such as robbery, car theft, harassment, and public drunkenness. The UK CCTV systems that we observed had control rooms that were operational 24 hours per day, 7 days per week, and all maintained digitally recorded images. The UK Home Office provided funding for 684 CCTV systems as of October 2002, though not all were operational at the time. Home Office officials said that the level of funding per location has ranged from about $50,000 to $12 million to implement CCTV in town centers, parking garages, and residential areas.

During the 107th Congress, a Senate bill was introduced that would have established a commission to evaluate the use of investigative and surveillance technologies, including surveillance cameras, to meet law enforcement and national security needs in the manner that best preserves individual privacy.[14] Under the proposed legislation, the commission was to investigate and report on standards for using, selecting, and operating such technologies and to make recommendations for legislation or administrative actions, as appropriate. However, the bill was not enacted.

[13]The Home Office is the governmental department responsible for internal affairs in England and Wales.

[14]S. 2846, 107th Cong. (2002).

MPDC and United States Park Police Implementation of CCTV

MPDC and the United States Park Police have implemented their CCTV systems with varying purposes and guiding protocols. The purposes of MPDC's and the United States Park Police's CCTV systems differ; however, both entities have installed cameras in locations that are at high risk for terrorist attacks. When the Department of Homeland Security's national threat level was increased to high alert (code orange), MPDC and the United States Park Police utilized CCTV on a continuous basis. Both MPDC and the United States Park Police view their CCTV systems from secure control rooms, and each entity's CCTV cameras have enhanced features, such as zoom capabilities. MPDC, acting under D.C. law, has issued regulations pursuant to D.C. statute that provide operating protocols to govern its use of CCTV, whereas the United States Park Police's use of CCTV is not specifically governed by any federal law or regulation. However, the United States Park Police is in the process of developing a policy applicable to its use of CCTV.

Figure 2: CCTV Cameras Monitoring Public Spaces

Source: © 2002 Cédric Laurant, www.observingsurveillance.org.

Source: © 2002 Cédric Laurant, www.observingsurveillance.org.

Source: © 2002 Cédric Laurant, www.observingsurveillance.org.

MPDC Operates CCTV on a Limited Basis

MPDC's CCTV system is generally intended to help manage public resources (such as police officers) during major public events and demonstrations and to coordinate traffic control on an as-needed basis. In addition to these purposes, the system may be utilized during exigent circumstances (e.g., periods of heightened alert for terrorism) as designated by the police chief. While the purpose of MPDC's CCTV system is to manage public resources and to control traffic, it could be used for monitoring crime as well. For example, although CCTV can be used to deploy police resources in order to maintain crowd control, the implied reasoning for deploying officers to maintain control would be to deter or prevent criminal activity, such as looting and rioting.

MPDC has used CCTV cameras for events such as the Fourth of July celebration in 2002 and antiwar demonstrations in 2003. According to a senior MPDC official, the CCTV cameras are not operational on a 24-hour basis; they are activated only during certain events and are turned off when the event ends. For example, the Chief of Police said that political demonstrations resulted in MPDC activating and deactivating the cameras only to reactivate them again when the Department of Homeland Security increased the national threat level to high alert (code orange).

MPDC has increased its CCTV system operations over time and has the capability to expand its operations by accessing other CCTV systems. A senior MPDC official said that MPDC's CCTV system had been increased from two cameras in April 2000, to 14 cameras with pan, tilt, and zoom capabilities. The cameras are monitored from a control room called the Joint Operations Command Center[15] located within MPDC's headquarters. According to the MPDC Chief of Police, the locations of the cameras throughout D.C. were chosen because they were thought to be locations that were at the highest risk for terrorism. MPDC can obtain real-time video images from other D.C. agencies, including the District of Columbia Public Schools. These agencies must first give MPDC access to their camera images. In addition, MPDC can access real-time video images from certain private entities in the D.C. metropolitan area, although a D.C. official said that MPDC has not been doing so. MPDC's CCTV cameras were purchased and maintained with city funds.

[15]The Joint Operations Command Center is a secure facility operated by MPDC, but may include staff from other federal, regional, state, and local law enforcement agencies during joint operations. The Joint Operations Command Center is a part of MPDC's Synchronized Operations Command Complex.

Figure 3: A CCTV Control Room

Source: Metropolitan Police Department of Washington, D.C.

MPDC Has Regulations That Govern Its Use of CCTV

MPDC drafted regulations and an implementing general order on the use of CCTV in June 2002. These documents were made available to the ABA for approval on their contents to help ensure that they reflected ABA standards. MPDC incorporated ABA's comments when formulating proposed rules to govern the use of its CCTV system, and the Mayor presented the proposed rules to the D.C. City Council. At a hearing before the D.C. City Council, witnesses testified that the use of CCTV should be legislated by the D.C. Council before any further consideration of MPDC's proposed rules. The council subsequently enacted a D.C. statute,[16] which required MPDC to issue CCTV regulations subject to the approval of the D.C. City Council. MPDC's proposed regulations were subsequently published in the D.C. Register for public comment on September 6, 2002.[17]

[16]D.C. Code 5-133.19.

[17]49 D.C. Reg. 8465 (Sept. 6, 2002).

The D.C. Council passed a resolution approving the proposed regulations on November 7, 2002. The final regulations set out the above-mentioned purposes of D.C.'s CCTV system and provide operating protocols for its use.[18]

However, the D.C. City Council plans to consider CCTV legislation during the current council period that would, if enacted, impose additional requirements on the use of CCTV (such as a requirement to obtain a court order to use video surveillance technology with certain telescopic zoom capabilities) and would require MPDC and other D.C. government agencies to promulgate regulations consistent with the legislation.[19] In addition, the bill would authorize a pilot project for the purpose of evaluating the effectiveness of video surveillance as a crime prevention tool. In particular, the bill would allow the installation of video surveillance technology in two D.C. neighborhoods for a period not to exceed 1 year to assess whether it was an effective crime prevention tool. D.C. residents, neighborhood organizations, and advocacy groups provided testimony both for and against MPDC's use of CCTV during public hearings held in December 2002 on the proposed bill.

United States Park Police Operating CCTV on a Continuous Basis

The United States Park Police is installing CCTV cameras to combat terrorism and to further law enforcement and public safety objectives. According to the Chief of the United States Park Police, the United States Park Police's CCTV system is to operate cameras located along the Monumental Core. The United States Park Police used CCTV for a single day on July 4, 2002, during the celebrations on the National Mall, and then the system was turned off pending completion of system implementation and the development of a policy. The United States Park Police developed a one-page policy for its use of CCTV on this day, and this policy became inactive at the end of the day. According to the Chief, the United States Park Police initially planned to wait until its policy was complete to resume the operation of its CCTV system; however, they used the cameras during large-scale demonstrations on the National Mall and when the Department of Homeland Security increased the national threat level to high alert (code orange). Subsequently, officials said that the United States Park Police's CCTV system has been used continuously since March 2003,

[18]49 D.C. Reg. 11443 (Dec. 20, 2002) (to be codified at D.C. Mun. Regs. tit. 24, ch. 25).

[19]D.C. Bill 15-0033, "Limited Authorization of Video Surveillance and Privacy Protection Act of 2003."

following a security-related incident on the National Mall. The CCTV system was operated under a draft policy each time it was activated. The United States Park Police staff monitors the cameras from a secured, controlled access United States Park Police facility. According to the Chief, as of May 2003, the United States Park Police continues to add cameras to its system and is operating under the auspices of a draft policy. The United States Park Police does not plan to publicly disclose the exact locations or the number of cameras used in their system due to their concerns that individuals could use this information to defeat the system or vandalize the cameras. According to United States Park Police officials, the decision to post signs indicating that CCTV is in use is currently under evaluation, and a decision had not been made at the time of our review.

Some of the United States Park Police's cameras have pan, tilt, and zoom capabilities and others have motion detecting capabilities. The Chief of the United States Park Police said that their choice of CCTV equipment was based on what was determined to be the most appropriate technology at the time. According to the Chief, the United States Park Police does not have plans to network its cameras to other agencies such as MPDC, though the cameras are equipped to do so. The Chief said that, in addition to viewing its own CCTV monitors, the Park Police is authorized to view MPDC's monitors in MPDC's Joint Operations Command Center. The United States Park Police's CCTV system is being purchased with appropriated funds at a cost of approximately $2.037 million.

United States Park Police Is Developing a Policy to Guide Its Use of CCTV

The United States Park Police's use of CCTV is not specifically governed by any federal law or regulation. While there may be limitations protecting individuals against abuse of CCTV by federal law enforcement officers, such limitations do not arise from federal laws or regulations specifically addressing how federal law enforcement agencies are to use CCTV.[20] However, the United States Park Police is in the process of developing a CCTV policy. As of May 2003, the United States Park Police is in the process of finalizing a draft policy that is to guide the use of its CCTV system, and its policy has not been reviewed outside the Department of the Interior. According to an Interior official, the United States Park Police is not required to obtain public comment on its proposed CCTV policy;

[20]As an example, individuals may be able to sue federal law enforcement officers for conduct that violates a constitutional right, such as using CCTV without a warrant to peer into private residences. Such lawsuits are commonly called *Bivens* actions. *See Bivens v. Six Unknown Named Agents of Federal Bureau of Narcotics*, 403 U.S. 388 (1971).

however, it is considering providing the public an opportunity to comment.

MPDC and United States Park Police Officials Said that Regulations and a Draft Policy Address Concerns

MPDC officials said that they had adopted regulations, and United States Park Police officials said that they were drafting a policy to address issues raised by civil liberties advocates. Both the regulations and the draft policy have incorporated management controls to address issues regarding individual privacy and the proper use of CCTV. Regarding the issue of CCTV effectiveness, MPDC and the United States Park Police both maintained that CCTV is an effective law enforcement tool and that they plan to measure the effectiveness of their CCTV systems. However, both entities are of the opinion that measuring CCTV effectiveness may be difficult.

MPDC and United States Park Police CCTV Privacy Policies

MPDC's regulations and the United States Park Police's draft policy address the protection of individual privacy in the following ways: MPDC's regulations state that the CCTV cameras are to be used to observe locations that are in public view where there is no reasonable expectation of privacy. A senior MPDC official said that MPDC's CCTV cameras are equipped with software that blocks the viewing of private areas, such as apartment windows and residential backyards. According to the Chief of Police, the United States Park Police has taken a similar position. This official said that they would focus their cameras on public park areas and public activities where there is no constitutionally protected expectation of privacy.

Figure 4: Scope of a CCTV Camera Surveillance Area

Source: © 2002 Cédric Laurant, www.observingsurveillance.org and GAO.

MPDC and the United States Park Police both maintain that their CCTV systems are to be operated in public spaces without infringing on individuals' First Amendment rights. MPDC's regulations state that under no circumstances is the CCTV system to be used for the purpose of infringing on First Amendment rights. The regulations state that CCTV operators are not to focus on hand bills or fliers that are being distributed or carried pursuant to First Amendment rights. According to the Chief of the United States Park Police, the department is also committed to ensuring that individuals are able to freely exercise their First Amendment rights. The United States Park Police's draft policy states that CCTV operators are not to target or focus on the faces of individuals engaging in First Amendment protected activities unless there is an indication of a criminal activity or threat to public safety. In addition, according to the Chief, the United States Park Police's draft CCTV policy strikes a balance between providing safety for citizens and protecting the privacy of demonstrators at various rallies and protests on the National Mall.

MPDC and the United States Park Police CCTV Management Controls Address Proper Use of CCTV Systems

MPDC and United States Park Police officials have in place or are putting in place, respectively, management controls for operating their CCTV systems and handling CCTV images. Specifically, MPDC's regulations and the United States Park Police's draft policy address the need for appropriate supervision to protect against inappropriate use of their systems and establish procedures for appropriate access to and handling of CCTV images. According to MPDC's regulations, only the Chief of Police is to authorize use of the CCTV system. This authorization must be in writing except in situations involving exigent circumstances or demonstration purposes. In addition, an official in the rank of Lieutenant or above is to be present at all times during system activation and usage and is to supervise and monitor the CCTV activities. Only certified operators are to be allowed to operate the system. MPDC's regulations state that every system activation is to be documented and that the activation information is to include the disposition of any observed incidents, a copy of any written authorizations pertaining to each activation, the names of any individuals activating the system, and documentation of when activation began and ended. The United States Park Police's draft policy states that the supervisory official assigned to, or responsible for, the control room is to monitor the activities of assigned personnel to ensure full compliance with the policy statement. All CCTV system operators are to be trained and supervised while operating the system. To ensure compliance with its regulations, MPDC's regulations state that audits are to be conducted by its Office of Professional Responsibility on at least a quarterly basis. According to a senior MPDC official, a compliance audit had been completed recently and found that the system was in full compliance with MPDC's regulations. Similarly, the Chief of the United States Park Police said that random audits are to be performed to ensure that the CCTV system is used properly.

Furthermore, MPDC's regulations state that unauthorized use or misuse of the CCTV system by operators is subject to criminal prosecution and/or administrative sanctions, including termination. A policy drafted by the United States Park Police states that their CCTV cameras are to be operated and supervised by the United States Park Police in a professional manner and only to further legitimate law enforcement and public safety objectives. In addition, the United States Park Police draft policy states that no person is to be targeted or monitored merely because of race, religion, gender, or political affiliation. Further, the Chief of the United States Park Police said that the United States Park Police does not plan to make use of the zoom capability unless suspicious activity is detected.

MPDC and the United States Park Police have addressed data collection and management issues by restricting access to their CCTV systems and outlining the security procedures for maintaining recorded images. MPDC houses its CCTV system in a secure control room, which is protected against unauthorized access by the use of bar-coded identification cards and a palm-print recognition system. Only federal agencies with a valid interest in viewing the cameras, such as the Federal Bureau of Investigation and the United States Park Police, are to gain access to the CCTV control room. According to the Chief of Police, agencies that have access to the Joint Operations Command Center are required to sign a memorandum of understanding stating that they will comply with MPDC regulations. According to MPDC's regulations, the Chief of Police is to issue written authorization prior to recording any CCTV images, except in exigent circumstances or when recording is being done pursuant to a court order. The regulations also require that every recording is to be documented in the same manner as every system activation and that all recorded CCTV footage is to be secured. The regulations further state that recordings will be retained for 10 business days and then destroyed, unless they are to be retained as evidence in a criminal case, a civil suit against MPDC, or for training purposes, as authorized in writing by the Chief of Police. Recordings retained for criminal or civil proceedings must be secured as evidence; recordings retained for training purposes may only be retained for as long as they are actively used.

United States Park Police draft policy states that CCTV images are to be transmitted through secured channels, and monitoring of the CCTV cameras is to be done from a controlled facility. Access to the controlled facility, as well as access to live or recorded CCTV images is to be limited to authorized personnel, for law enforcement and public safety purposes, or for civil litigation and disciplinary purposes. In order for another law enforcement agency to gain access to the recorded CCTV images, the Chief of the United States Park Police opined that there would need to be a clear nexus with a crime. Additionally, according to the draft policy, recordings are to be retained for no more than 6 months and then destroyed unless needed as evidence for a documented criminal incident. The draft policy also states that in the event that a video recording needs to be retained for more than 6 months, the reason, length of time, and chain of custody is to be documented.

MPDC and the United States Park Police Perceive Measuring the Effectiveness of CCTV to be Difficult, but Plan to Develop Measures

A D.C. official said that the effectiveness of MPDC's CCTV system is difficult to measure because of its limited use of the cameras. Further, the Chief of Police said that crime statistics could not be used to evaluate the effectiveness of the cameras since MPDC currently does not use the cameras specifically to detect crime. The regulations state that the general purpose of the cameras is to help manage public resources during major public events and demonstrations and to coordinate traffic control. This purpose reflects a mission of deterring crime and minimizing traffic problems. Measuring deterrence can be difficult without a comparison between similar areas with and without CCTV. Measuring CCTV effectiveness may be further complicated by the use of other law enforcement interventions such as improved lighting and notices about CCTV. Thus, demonstrating a direct cause and effect relationship between decreased crime and CCTV may not be easy to do.

MPDC's CCTV regulations require MPDC to prepare an annual report that includes, among other things, an evaluation of whether the cameras have achieved their purposes as outlined in the regulations. According to a senior MPDC official, an annual report has not been prepared to date because the system has not been operational for one year. Although crime control is not the stated purpose of MPDC's CCTV system, an MPDC official said that MPDC's CCTV cameras have caught crimes. The official provided an anecdotal example of the system's effectiveness—the CCTV cameras were activated for a high-profile sporting event and subsequently caught some car thieves.

United States Park Police officials also said that it has been difficult to find measures of effectiveness for such things as crime prevention related to CCTV use. To measure effectiveness of their CCTV system, the Chief of the United States Park Police said that once their system is activated, they plan to track arrests made resulting from camera use.

Overall, both MPDC and the United States Park Police view CCTV as a valuable complement to their other policing efforts. MPDC and United States Park Police officials said that they have received positive feedback from the community, including, in some cases, requests for more CCTV cameras and in others, gratitude from residents for going the extra mile to make them feel safe.

Public Feedback on MPDC's Regulations

MPDC made its regulations available for public comment and held hearings regarding the operation of its CCTV system. At hearings, MPDC received positive and constructive feedback regarding its CCTV

regulations. MPDC also received positive feedback from the ABA regarding its regulations. ABA reviewed MPDC's draft regulations in comparison with its published standards and concluded that MPDC's regulations comply with ABA's standards on video surveillance.

Other feedback was less positive. The Constitution Project, a nonprofit scholarship and advocacy organization, provided draft comments on MPDC's regulations and noted several areas that lacked clarity and specificity. For example, the Constitution Project stated that comprehensive training and instruction for CCTV operators is essential to enable them to better navigate the line between appropriate investigation and infringement of civil liberties, noting that there are no provisions in MPDC's regulations that detail what credentials and training are required to obtain certification to operate the CCTV system.

The Constitution Project also commented, among other things, that posted signs indicating the presence of CCTV cameras should contain contact information of an independent entity that concerned residents can contact should they believe that the cameras' presence is invasive, unnecessary, or utilized improperly. Further, the Constitution Project stated that the audit provisions in MPDC's regulations raise the larger question of whether the entity conducting the audit is sufficiently independent to perform a credible audit function.

Experiences of Other CCTV Users in the United States and UK Reveal Best Practices for Other Interested Locations

Officials in the selected U.S. cities and in the UK shared with us practices that they considered beneficial to help ensure proper and effective use of CCTV systems. Because of their extensive use of CCTV to deter, detect, and investigate crime, the experiences from UK officials offered a greater number of best practices than the selected U.S. cities, though models from other countries are not always applicable to the United States. Like MPDC and the United States Park Police, the UK and the selected cities have grappled with how to measure the effectiveness of their CCTV systems.

Public Notice Helps to Address Privacy Concerns

UK officials said that gaining acceptance of their CCTV systems was based on having honest, open, and fair communication between the community and the authorities. CCTV users who managed the CCTV systems in the UK said that obtaining buy-in from stakeholders such as the public, in addition to operating the system in an open environment, was an important factor in mitigating concerns about the use of CCTV. For example, according to a UK official, one borough invited the public (and in

some instances, former and suspected criminals) to tour its control room to show them the reality of how the system is used to identify criminals.

Figure 5: Depiction of a CCTV Sign

Source: GAO.

Like MPDC and the United States Park Police, many of the selected U.S. cities encountered concerns and skepticism by the ACLU and others regarding their use of CCTV to monitor public spaces. In some cases, the public has also voiced concerns about how CCTV may be used and whether it might infringe upon their individual privacy. In response to the privacy concerns, CCTV users in the selected U.S. cities have generally provided citizens with notification of the intent to use CCTV and provided avenues for the public to comment and provide feedback. Each city posted signage that indicated that CCTV was in use. Also, CCTV users in some of the selected cities allowed the public to comment on aspects of the CCTV system through community meetings and public hearings. Officials in one city said that the public was also informed through a media campaign that detailed the specifics of the CCTV system. The Chief of Police in one city said that he had personally held conversations with residents to assure them that the CCTV cameras would not compromise their privacy.

Having Standards Helps to Alleviate Objections to the Use of CCTV

The UK government saw a need to establish controls over the use of CCTV systems in order to maintain public confidence. UK officials generally recognized the importance of having regulations in place to govern CCTV systems, stating that having standards makes citizens feel more comfortable and safe regarding how the system is being operated. CCTV

standards were established through the Data Protection Act of 1998.[21] Among other things, the standards addressed individual privacy issues in relation to CCTV use. According to a UK official, there was no statutory basis for systematic legal control of CCTV surveillance over public areas in the UK until March 2000, when the Data Protection Act of 1998 was implemented.

The Data Protection Act is the principal legislation that impacts the operation of public space CCTV systems in the UK. Under the Data Protection Act, the UK Information Commissioner[22] issued a CCTV Code of Practice to provide specific standards to CCTV operators on how to comply with the act's data handling principles. According to the UK Information Commissioner, the Code of Practice has the dual purpose of assisting CCTV operators to understand their legal obligations while also reassuring the public of the safeguards that should be in place when utilizing CCTV. The Code of Practice also indicates standards that are not strict legal requirements, but represent good practice. UK Home Office officials said that CCTV users follow the Code of Practice and comply with the Data Protection Act of 1998 because they recognize that the act and the code both help to alleviate objections to the use of CCTV.

For the selected U.S. cities, there were no state laws or regulations specifically governing how state or local law enforcement officers were to use CCTV systems to monitor public spaces. While there may be limitations on law enforcement's use of CCTV in these states, such limitations do not stem from comprehensive state CCTV laws or regulations.[23] However, police departments in these cities generally had

[21]The Data Protection Act 1998, ch. 29 (Eng.) is available at http://www.legislation.hmso.gov.uk/acts/acts1998/19980029.htm. The CCTV standards issued under the Data Protection Act, called the CCTV Code of Practice, can be accessed at http://www.dataprotection.gov.uk/dpr/dpdoc.nsf/0/db76232b37b5bb648025691900413c9d?OpenDocument

[22]The UK Information Commissioner is an independent supervisory authority reporting directly to the U.K. Parliament. The Commissioner enforces and oversees the Data Protection Act of 1998. The Commissioner has a range of duties including the promotion of good information handling and the encouragement of codes of practice for data controllers, that is, anyone who decides how and why personal data, (information about identifiable, living individuals) are processed.

[23]For example, state "Peeping Tom" statutes provide criminal sanctions for unauthorized spying or peeping into private places. These statutes might apply to CCTV surveillance that lacks a valid law enforcement purpose, is voyeuristic in nature, and occurs in a private place as defined by the statute. *See, e.g.*, Fla. Stat. 810.14; Md. Code Ann., Crim. Law 3-902(b)(c); S.C. Code Ann. 16-17-470; Va. Code Ann. 18.2-130.

policies, which varied in detail and in content, to govern the use of their CCTV systems. Organizations, including the ABA, IACP, and SIA, have developed standards and guidelines that address privacy issues and controls on CCTV use. ABA saw a need to develop standards in order to help ensure that law enforcement agencies are aware of all the relevant considerations with regard to CCTV use and to prompt these agencies to create their own internal guidelines for the use of CCTV technology. According to the IACP and SIA they collaborated to produce guidelines because, despite the prevalence of CCTV use on national and local levels, there were no consistent policies or procedures guiding the use of CCTV systems. The IACP and SIA recommend that law enforcement agencies and public safety officials adopt some or all of their guidelines to assist in their use of CCTV.

Figure 6: Police Officer Monitoring a CCTV System

Source: Tampa Police Department.

Clear Goals and Purpose Help Ensure Appropriate Use and Alleviate Concerns Raised

To help ensure that CCTV systems are used effectively, some CCTV users in the UK indicated that it is important to have a plan prior to the implementation of the CCTV system that should include clear, realistic, and measurable goals for the CCTV system, as well as how CCTV might address the goals. For example, clear goals would include, among other things, identifying the highest-priority problems to be addressed by the system, problem locations, and what is to be observed. UK officials also said that matching the CCTV technology to the purpose and goals of the system is a key factor in the effective use of CCTV. For example, if the purpose of the CCTV system is to deter crime, CCTV users may not need cameras that pan, tilt, and zoom. Rather, the CCTV users may determine that viewing and/or recording activity from fixed cameras used to observe broad areas is sufficient to meet their needs. However, if the purpose of the CCTV system is to detect crime and intervene, a CCTV user may consider continuously monitoring the CCTV cameras in order to be able to quickly respond to certain incidents. Clear and measurable goals identify the problems to be addressed by CCTV and can include a range of

measures to determine whether goals have been achieved, such as the change in crime levels or the change in public attitudes about crime.

CCTV users in the selected cities whose CCTV systems were fully operational have been able to make the systems more effective and respond to some privacy concerns by appropriately matching the technology being used with the intended purpose. In one instance, a representative said that the ACLU's concerns were mitigated because they installed cameras without enhanced features, such as zoom capabilities. They said that limited monitoring of the CCTV images, along with the fact that the cameras do not pan, tilt, or zoom limits the potential for the invasion of individual privacy. In contrast, CCTV users in selected cities that installed cameras that did pan, tilt, or zoom lessened their chances of abuse by reducing the time spent visually monitoring the cameras. For example, in two cities, CCTV users only monitored the cameras during designated times or at designated events, such as Sunday nights preceding Monday holidays in a busy entertainment district. Officials in one of the two cities said that the cameras were visually monitored everyday during the tourist season and only monitored on weekends during the off-season.

Training and Audits May Help to Ensure Proper Use of CCTV

UK officials said that they preferred a well-trained and professional staff to operate their CCTV system. According to one UK official, CCTV systems involve human interaction, requiring a manager and requiring training on how to use the system. The official also said that the most successful CCTV systems have good managers, good training, and sound procedures.

UK officials have identified performing audits of CCTV systems as a way to hold CCTV users accountable for their actions and deter misuse while operating CCTV systems. In one UK location, the activities of each CCTV operator can be traced and audited via computer. In addition, a CCTV user in the UK planned to employ the use of outside inspection teams to perform random audits. The inspection teams are to have full authority to observe how the CCTV system is being operated, although the CCTV system observed had not yet performed any audits at the time of our visit.

In the selected U.S. cities, CCTV operators were trained to use CCTV by the vendor providing the CCTV technology, or in some cases, by senior management. For example, one city official said that the city's CCTV vendor would provide a minimum of approximately 2 to 3 days of training on the use of the CCTV system in two parts: (1) command and control of the system and (2) retrieving CCTV images from the system.

CCTV users in selected U.S. cities also found audits to be helpful. To help ensure that CCTV systems are not misused, an official in one city said that the city formed a steering and audit committee comprised of citizens to ensure that CCTV operations were in compliance with written procedures in order to avoid misuse of the CCTV system. Another city official said that committee members were allowed to visit the CCTV control room whenever they wanted to review the recorded CCTV images. An official in another city said that, while not an audit per se, they would review tapes for inappropriate use of the cameras. For example, he said that review of the tapes would allow them to determine if the officers monitoring the cameras were focusing voyeuristically on women.

Figure 7: CCTV Monitor

Source: Tampa Police Department.

Procedures for Handling Data Helps to Ensure Data Are Used Appropriately

CCTV users in the United States and the UK have indicated that an important consideration in handling CCTV images is providing controls to guard against abuse or misuse that enable CCTV users to operate CCTV systems openly enough to gain public acceptability, but not so open as to

invade individual privacy by releasing personal information to unauthorized individuals. To address concerns related to the maintenance and storage of data and individual access to data, policies developed by the selected CCTV users covered various topics related to these issues. In all of the selected U.S. cities and in the UK, CCTV images were retained for a specific period of time, after which they were destroyed or reused, unless they were retained for a bonafide law enforcement investigation. A UK official said that citizens could obtain access to images of themselves; however, they have to supply the exact date, time, and location where they were recorded and the CCTV system blocks any other individuals in view.

In the UK, the Data Protection Act limits the way personal data are processed in order to protect the privacy of individuals. The act requires organizations that process personal data to comply with the eight statutory principles of good data handling. These principles provide that personal data must be: (1) fairly and lawfully processed in accordance with applicable statutory conditions; (2) obtained and processed only for specified, lawful purposes; (3) adequate, relevant, and not excessive in relation to the purpose for which they are processed; (4) accurate; (5) not kept longer than necessary; (6) processed in accordance with the data subject's rights; (7) secure; and (8) not transferred to countries outside the European Economic Area without adequate protection for personal data. The UK Information Commissioner, which is an independent supervisory authority, enforces and oversees the act's provisions.

Measuring Effectiveness of CCTV Perceived to be Difficult, but Desirable

Researchers and others stress the importance of measuring effectiveness of CCTV systems in order to justify costs and the potential impact on individuals' civil liberties. There is general consensus among CCTV users, privacy advocates, researchers, and CCTV industry groups that there are few evaluations of the effectiveness of CCTV in reducing crime, and few jurisdictions are keeping data to demonstrate that their CCTV systems are effective.

A study undertaken on behalf of the Home Office, found mixed results for the crime prevention effectiveness of CCTV. However, in October 2002, a Home Office official said that the Home Office had provided funding for an evaluation of effectiveness for 17 CCTV systems as part of a CCTV initiative begun in 1999 for the implementation of 684 local government-operated CCTV systems in the UK. The evaluations are to be completed in November 2004. Home Office officials cautioned that using crime statistics as a measure of effectiveness may not be a good measure. They said that arrest rates might increase because the CCTV cameras view more criminal

activity and police are reacting to more reports originating from CCTV control centers. They also said that increased crime rates are not necessarily bad because it may mean more crimes are being reported that had previously gone undetected. Furthermore, one CCTV user in the UK said that the effectiveness of various CCTV systems could vary due to differences in CCTV supervisory personnel, training, and procedures.

Officials in the UK provided anecdotal evidence of how CCTV cameras have been effective. For instance, officials in one UK location said that CCTV cameras have observed drug deals and fraudulent passports being passed. An official also gave an example of a little boy who was abducted from a shopping center. When the images on the CCTV tape were shown, officials could discern that the relative heights of the abductors indicated that two other children took the little boy. Another example involved bombings of several London pubs. Officials said that CCTV tapes were used to trace various pieces of evidence to identify the bomber. While the quality of the pub's CCTV cameras was not good, the police were still able to use the images to locate the perpetrator by reviewing CCTV footage from various entities thereby tracking him on various videotapes until they were able to identify him and trace his whereabouts. For example, police used a store's CCTV cameras to view the perpetrator buying equipment for the bombs. The official said that the police were convinced they would not have found the perpetrator without the CCTV cameras, since the bomber did not have a criminal record and there was no reason to suspect him.

Most CCTV users in the selected U.S. cities whose systems were fully operational at the time of our visit did not statistically measure the effectiveness of their CCTV systems. They perceived it to be difficult to measure, although officials in the selected cities said that CCTV had been very effective in, among other things, detecting and investigating crime, monitoring areas for public safety, and enhancing security. Officials provided anecdotes to demonstrate their system's effectiveness. For example, an official in one city said that the CCTV cameras filmed a drug transaction that resulted in an arrest.

Concluding Observations

MPDC and the United States Park Police have implemented CCTV systems as part of their overall strategies to address crime and terrorism. While specific uses and guiding protocols vary, both MPDC and the United States Park Police have installed cameras in areas that are high risk for terrorist attacks, view their systems from secure control rooms, and use cameras that have enhanced features, such as zoom capabilities. Measuring CCTV effectiveness is difficult because of the lack of comparisons of similar

areas with and without CCTV to show a direct cause and effect relationship, and because it is often used in tandem with other law enforcement tools. Nevertheless, both MPDC and the United States Park Police plan to identify performance measures and evaluate effectiveness.

Civil liberties advocates have raised concerns about the protection of privacy and the proper use of CCTV systems. MPDC has adopted regulations and the United States Park Police is drafting a policy aimed at incorporating management controls to address such issues. These include developing written operating protocols, establishing supervision and training requirements, providing for public notification, and requiring system audits. It is too early to fully assess the sufficiency and effectiveness of these controls.

The use of CCTV as a law enforcement tool is growing in the United States and abroad. The experiences of CCTV users in the United States and the UK can help guide other jurisdictions that are considering the use of this law enforcement tool with regard to openness and community involvement; uniform standards and management controls; and the establishment of realistic, clear, and measurable performance goals.

Agency Comments and Our Evaluation

In letters dated June 6, 2003, we requested comments on a draft of this report from MPDC and the Department of the Interior. Officials from both police departments generally agreed with the report and our presentation of information regarding their CCTV use.

On June 23, 2003, the Department of the Interior provided written technical comments, which were included as appropriate. In its comments, Department of the Interior officials indicated that the United States Park Police's draft CCTV policy is in the final stages of review and is expected to be finalized within 2 weeks of the date of its written comments. MPDC had no technical corrections.

We are providing copies of this report to the Chairman and Ranking Minority Members of the Senate Committee on Governmental Affairs, the Senate and House Committees on Appropriations, and the Senate and House Committees on the Judiciary. We are also providing copies of this report to the Deputy Mayor for Public Safety and Justice for Washington, D.C.; the Chief, Metropolitan Police Department of Washington, D.C.; Secretary of the Department of the Interior; the Director of the National Park Service; and the Chief, United States Park Police. Copies of this

report will be made available to other interested parties. This report will also be available on GAO's Web site at http:/www.gao.gov.

If you have any questions, please contact me at (202) 512-8777 or by e-mail at stanar@gao.gov or Linda Watson, Assistant Director, at (202) 512-8685 or by e-mail at watsonl@gao.gov. Key contributors to this report were Leo Barbour, Christine Davis, Glenn Dubin, Michele Fejfar, Jamila Jones, Nettie Richards, Amy Rosewarne, and Carrie Wilks.

Sincerely yours,

Richard M. Stana
Director, Homeland Security and Justice Issues

Appendix I: Scope and Methodology

To determine how the Metropolitan Police Department of the District of Columbia (MPDC) and the U.S. Department of the Interior's United States Park Police have implemented their closed-circuit television (CCTV) systems, we interviewed officials from both agencies. We obtained and reviewed congressional hearing records related to the use of CCTV in Washington, D.C. We attended a D.C. City Council public hearing and obtained testimonies of officials and civilians who addressed the city council. At the United States Park Police, we obtained documents related to the use of CCTV as well as congressional testimony regarding their use of CCTV. We interviewed representatives from the American Bar Association (ABA), the American Civil Liberties Union (ACLU), the Electronic Privacy Information Center (EPIC), the International Association of Chiefs of Police (IACP), and the Security Industry Association (SIA) to obtain their views on the use of CCTV and obtained documentation from them regarding issues of concern to their organizations. In addition, we toured MPDC's Joint Operations Command Center.

To determine how MPDC and the United States Park Police have implemented management controls to respond to the issues surrounding their use of CCTV, we interviewed MPDC and United States Park Police officials and obtained and reviewed relevant laws, regulations, policies, and other documents. We also obtained and reviewed testimonies of officials and civilians at D.C. City Council public hearings and reviewed draft comments by the Constitution Project that critiqued MPDC's regulations. We did not evaluate or test compliance with MPDC's or the United States Park Police's management controls.

To learn about the experiences of other CCTV users in the United States and the United Kingdom (UK) we reviewed various studies and reports on CCTV use by law enforcement. We reviewed studies and reports by or for SIA, the California Research Bureau, RAND, and the UK Home Office, among others. We judgmentally selected four U.S. cities to visit and obtained information on their use of CCTV. The four cities selected were: Baltimore, Maryland, because of its proximity to D.C.;[1] Columbia, South Carolina, because officials in this city were in the early stages of

[1]We interviewed officials regarding the CCTV system implemented by the Downtown Partnership of Baltimore, a nonprofit corporation founded to, among other things, shape public policy and implement programs to strengthen the economic vitality of downtown Baltimore. The Baltimore City Police Department is a member of the Downtown Partnership of Baltimore.

implementing their CCTV system; and Tampa, Florida, and Virginia Beach, Virginia, because their CCTV systems were equipped with facial recognition software, and we wanted to include locations that were using CCTV with advanced features. At each location, we interviewed officials regarding privacy concerns, if any, that had resulted from their use of CCTV, conducted research for any relevant state laws or regulations, obtained and reviewed policies and other documentation related to the operation of their systems, and inquired about whether they had measured the effectiveness of their CCTV systems. In two cities, we toured the control rooms from which the cameras were operated and monitored. We visited the UK to learn from its experiences with CCTV use in a law enforcement capacity. We met with UK Home Office officials and CCTV users in the UK to determine what their experiences have been and whether they measured the effectiveness of their systems. In the UK, we interviewed government officials in the Home Office and CCTV users in Newham and Westminster—boroughs of London—and the city of Sheffield. We also observed CCTV operations in these locations. In addition, we interviewed a representative of a private UK CCTV User Group that provides assistance to CCTV users. To obtain a broader perspective on privacy issues, we also interviewed a representative of Privacy International[2] in London.

We performed our audit work from July 2002 to May 2003 in Washington, D.C., and other cited locations in accordance with generally accepted government auditing standards.

[2]Privacy International is a human rights group that serves as a watchdog on surveillance by governments and corporations.

Appendix II: Implementation of CCTV Systems in Selected U.S. Cities

The following provides a summary of how each of the four cities we selected to visit has implemented their respective CCTV systems. The four cities were at different stages of development in implementing their systems and, generally were using CCTV to achieve different purposes.

Baltimore, Maryland

In Baltimore, a representative said that the city's CCTV system was implemented in 1994 to deter crime. This system consisted of 64 CCTV cameras installed in the downtown area. The CCTV system was implemented to address property crimes and the community's negative perception of safety. Both Baltimore City law enforcement personnel and staff from organizations and businesses that participate in the Downtown Partnership of Baltimore operate the system. The cameras did not have remote zoom capability and were generally not monitored. Recorded CCTV images are reviewed for investigative purposes if crimes occur.

Columbia, South Carolina

The Columbia Police Department implemented a pilot CCTV program in 2002 prior to implementing a final CCTV system. The city's final CCTV system was not fully implemented at the time of our review. The pilot CCTV system involved 3 fixed cameras located in residential areas and public parks. The Chief of Police in this city said that the city did not hold any formal hearings before the pilot CCTV system was implemented, although the use of CCTV was subject to a majority vote by the city council members. Although a city official said that the city purchased an additional 12 CCTV cameras for the final system, 3 pilot cameras were installed and operational at the time of our visit. Through the pilot program, a city official determined that in addition to monitoring the cameras from police headquarters, an added benefit would be to enable officers to monitor cameras from their police cars while on patrol. City officials decided to expand the CCTV viewing capability by linking the CCTV system to laptop computers which enabled officers to monitor CCTV images from their police squad cars.

Tampa, Florida

In Tampa, the police department first deployed CCTV in December 1997 in a busy entertainment district. An official said that the cameras were installed to address specific issues in the completion of the public safety mission, including management of large crowds and the adequate deployment of police personnel. The system was comprised of 36 CCTV

cameras, all with the ability to pan, tilt, and zoom. The system was also equipped with facial recognition software. The cameras were monitored during certain nights of the week and during special events by police personnel.

Virginia Beach, Virginia

Officials in Virginia Beach said that the police department began operating the cameras in 1993 after an incident at a local event provided the impetus. A city official said the CCTV cameras were used to deter, detect, and investigate crime; monitor and enhance the security of certain areas; and apprehend and prosecute suspected criminals and counter terrorism. The system records images 24 hours per day, 7 days per week and is monitored every day during the tourist season. During the nonvacation season, police officers only monitored the cameras on weekends. According to officials, the police department installed 10 CCTV cameras in a busy oceanfront/business district. Each CCTV camera had the ability to pan, tilt, and zoom. The system was also equipped with facial recognition software.

Appendix III: Implementation of CCTV Systems in the United Kingdom

The United Kingdom (UK) locations that we visited operated CCTV systems that were similar in purpose and application. There were subtle variations in the purposes of each system; however, all CCTV systems we observed were implemented to control some aspect of crime.

Newham, London

In Newham, use of CCTV resulted from a public call to do something about the increasing crime rate. An official said that since the late 1960s and early 1970s, the borough had experienced an increase in street-type crime, which stemmed from structural unemployment and the existence of a known but relatively small criminal element. Most crime involved robbery, car theft, harassment, public drunkenness, drug trafficking, and hooliganism. Officials said that the public felt unsafe doing everyday things like walking down certain streets or shopping in certain areas. Therefore, officials said that it was easy to sell CCTV to the borough council, because the borough had one of the highest burglary and auto theft rates in the UK, and the public perceived CCTV to be an effective response to the crime. In 1997, Newham began using CCTV to address these crime problems.

Officials said that about 10 uniformed civilians per shift operate the system, which has over 400 CCTV cameras. They explained that one operator could be responsible for viewing up to about 60 monitors, given that some of them have screens that can show several camera images simultaneously. The operators key in on certain areas known to be crime prone, but also scan other areas to detect potential crimes or crimes in progress. The operators' actions are monitored by cameras to help ensure compliance with rules governing CCTV use. Officials said that officers operate the system 24 hours a day, and the control center also has a tape library and facilities for police to review the tapes for evidence.

Westminster, London

In Westminster, the borough council and the police department—jointly with business and community trustees—manage its CCTV system, which became operational in July 2002. An official noted that the purpose of the system is to improve the management of public space to enhance public safety. For example, the officials said that in addition to controlling crime and disorder, they strive to keep the streets clean and ensure free flow of traffic. The officials also said their purposes differ between day and night in that daytime operations often focus more on the environment on the

street such as transportation issues, whereas at night they focus more on crime and disorder.

At the time of our visit, officials said that 17 cameras were in operation, but that they expected more. An employee of the borough council managed the center, and the system operators were civilians (contract staff). Officials noted that the center was a business area partnership and that the space they were using was provided rent free to the council for CCTV operations, adding that capital funding for the center came from the Home Office and local businesses helped to support the operations. The center had three operator control positions to monitor CCTV cameras and 18 monitors on the wall for viewing and from which operators could pull images down to their individual monitors to pan, tilt, and zoom to get a better view.

Officials noted that they perceive their CCTV system as being a "graded response system" whereby on the basis of what they observe, they can notify the relevant agency to take action. For example, if an assault is observed they notify the police, if trash is left on the street they notify the trash collectors, or if a car were behaving erratically they would call the traffic department. Officials told us that this type of approach is the success of CCTV because it helps to focus on what the problem is and what the solution is. They also said that usually it is not just CCTV that is the solution, but the intelligence from CCTV that can be used to solve the problem.

City of Sheffield

The city of Sheffield has been utilizing CCTV, operated by the city council, since about 1997. Officials said that the UK Home Office funded the capital costs with grants, while the city council funds system operations and maintenance. Although this city's CCTV system is similar in application to the others we visited, the distinction is that this city has a more "joined up" concept, whereby all area stakeholders that have CCTV systems (city, train, mall) can forward camera images to other stakeholders' systems to provide a more integrated view of the area. Officials explained that, if needed (bomb scare or terrorist act), the central control center can take control of any camera in the integrated system, or the command/control function can be shifted to one of the other two centers. The police can also be fed the images real-time from the central control center instead of viewing images later to assemble evidence. Operators can more easily follow criminals or criminal activity from one camera/system to the next. This is important, as these officials noted that the area has two of the UK's

top 20 terrorist targets (a six-lane bridge that is a vital economic link to the north, and one of the UK's largest shopping malls). If called on a crime, however, this city's cameras can be focused to those areas. At the time of our review, officials said that the actual linkage between the three control centers (city, train, mall) was to occur in the near future.

Officials in Sheffield consider the linkage to other CCTV control centers as essential to the future success of CCTV. For example, officials said that linking of CCTV could be used to determine how many police and ambulance units should be deployed or make command/control decisions after a terrorist attack, such as finding the best route for emergency response vehicles, and re-routing citizen evacuation traffic.

GAO's Mission

The General Accounting Office, the audit, evaluation and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through the Internet. GAO's Web site (www.gao.gov) contains abstracts and full-text files of current reports and testimony and an expanding archive of older products. The Web site features a search engine to help you locate documents using key words and phrases. You can print these documents in their entirety, including charts and other graphics.

Each day, GAO issues a list of newly released reports, testimony, and correspondence. GAO posts this list, known as "Today's Reports," on its Web site daily. The list contains links to the full-text document files. To have GAO e-mail this list to you every afternoon, go to www.gao.gov and select "Subscribe to daily E-mail alert for newly released products" under the GAO Reports heading.

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. General Accounting Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone:
Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Public Affairs

Jeff Nelligan, Managing Director, NelliganJ@gao.gov (202) 512-4800
U.S. General Accounting Office, 441 G Street NW, Room 7149
Washington, D.C. 20548