CCTV:
DEVELOPING PRIVACY BEST PRACTICES

Report on the DHS Privacy Office Public Workshop

December 17 and 18, 2007

TABLE OF CONTENTS

Executive Summary

In December of 2007, the Department of Homeland Security (DHS) Privacy Office convened a two-day public workshop to examine best practices for government use of camera technology, commonly referred to as closed circuit television (CCTV). Titled *CCTV: Developing Privacy Best Practices*, the Workshop examined how technology, local and international communities, law enforcement, government agencies, and privacy advocates are shaping the use of CCTV and what safeguards should be in place as the use of CCTV expands.

The Workshop served as a valuable resource to the Privacy Office in its joint effort with the DHS Office for Civil Rights and Civil Liberties to develop an informational guide to best practices for government use of CCTV. The best practices guide, along with sample templates for Privacy Impact Assessments (PIAs) customized for CCTV and the DHS template for Civil Liberties Impact Assessments, are included in the Appendix to this Workshop report. The DHS Privacy Office and Office for Civil Rights and Civil Liberties hope that government agencies will consider these resource materials in developing their CCTV programs and policies. These resources may be useful in helping government agencies build privacy and civil liberties protections into the design and implementation of a CCTV program. Failure to address privacy and civil liberties can undermine public support for the use of CCTV and erode confidence in government's ability to protect privacy and civil liberties while protecting the Homeland. Government agencies can avoid project delays and gather public support by ensuring that the appropriate safeguards and policies are in place before launching CCTV systems.

The Workshop brought together leading academics, international government officials, researchers, law enforcement representatives, technologists, community leaders, and policy experts. These panelists identified a range of challenges facing local governments, communities, and law enforcement regarding privacy and use of CCTV. The key topics discussed at the Workshop included:

- CCTV technology and its impact on privacy;
- International perspectives on the use of CCTV;
- Law enforcement use of CCTV;
- Community perspectives on use of CCTV;
- Legal and policy considerations regarding the use of CCTV; and
- Best practices for the implementation and use of CCTV.

The panel on Technology Perspectives opened the Workshop by providing a basic understanding of the current CCTV technologies in use. This discussion led into a more in-depth discussion on the capabilities of the technology and video analytics being used today. The panel then discussed computer vision technology (privacy protections and visual surveillance); equipment and architecture considerations (placement); and large system implementations and concluded with a discussion on large system information management.

The second panel addressed International Perspectives. Regulators and academics provided perspectives on lessons learned from abroad. The panel addressed implementing surveillance

programs while taking into consideration the Fair Information Practices Principles (FIPPs) as well as considering the general knowledge and understanding of the public. The academic panelists highlighted the changing notion of public versus private space and the impact technology has on these definitions.

The third panel focused on Law Enforcement Perspectives. This panel discussed the challenges community law enforcement organizations are experiencing as a result of the demand by communities for CCTV systems. The Law Enforcement representatives discussed such issues as the reasons to have a CCTV system, the staff required to monitor the video screens, the partnership between businesses and police departments, and the need to have in place policies and procedures governing the operation of the cameras.

The fourth panel, on Community Perspectives, profiled five U.S. cities in various stages of implementing CCTV systems. Representatives of Baltimore, Maryland; Chicago, Illinois; Hyattsville, Maryland; Stamford, Connecticut; and Norfolk, Virginia discussed how they were proceeding to implement CCTV programs in their communities. The panelist from Hyattsville highlighted its policy-first approach before installing any cameras, which included an independent assessment to review surveillance requirements for the city. The panelists discussed their challenges to date and their policies to address privacy and civil liberties concerns.

The fifth panel, Legal and Policy Perspectives, provided an overview of constitutional considerations and case law in the area of privacy, illegal searches, and the use of CCTV. In addition, the panelists discussed the lack of legal precedent regarding the use of CCTV and individual rights and indicated that many cities are installing CCTV systems without clear purpose or enforceable policies and procedures outlining protections for privacy, civil rights, and civil liberties. The panel gave suggestions for what a community or agency should consider when developing policies and procedures and establishing best practices. The panel further discussed the effects CCTV systems have on every day activity and how the public, although supportive of these systems, may alter everyday behaviors when they know they are being captured on cameras.

The sixth and final panel of the Workshop, Best Practices Perspectives, provided examples on community policies and best practices based on the FIPPs. In addition, the panel provided suggestions for how the DHS grant program could be enhanced to encourage CCTV applicants to take into consideration public comments and community involvement prior to awarding money for surveillance programs. Appendix B, *Best Practices for Government Use of CCTV*, builds upon the recommendations of this panel, as well as the panel discussions throughout the Workshop. The Workshop agenda and a full transcript of the Workshop are available on the DHS Privacy Office website at www.dhs.gov/privacy.

Following the summary of the highlights of the Workshop, the Appendices provide a series of resources to aid government agencies in drafting policies to protect privacy and civil liberties when implementing CCTV programs. Appendix A is the Workshop Agenda. Appendix B, *Best Practices for Government Use of CCTV*, provides a set of practices based upon the FIPPs that build privacy considerations into CCTV decision making. Appendix C, *Template for Privacy Impact Assessment for the Use of CCTV by DHS Programs*, is the PIA template the DHS Privacy

Office will use to analyze the privacy considerations associated with DHS activities involving CCTV. Appendix D, *Template for Privacy Impact Assessment for the Use of CCTV by State and Local Entities*, is intended as a sample PIA for non-Federal agencies seeking to identify and address the privacy concerns posed by a CCTV program. Finally, Appendix E, *Template for Civil Liberties Impact Assessments (CLIA)*, is the template the DHS Office for Civil Rights and Civil Liberties uses to evaluate DHS activities. Although the analysis in the CLIA focuses on Federal law, the civil liberties issues are consistent with those that a State and Local agency may need to address.

As government agencies increasingly turn to technologies such as CCTV as a tool for law enforcement and public safety, the need for policies to protect privacy and civil liberties grows stronger. The Workshop evidenced the need for such policies and revealed that many communities may not yet have them in place. The DHS Privacy Office and Office for Civil Rights and Civil Liberties, therefore, hope that this report will help government agencies craft these policies and demonstrate that privacy and civil liberties are valued and protected.

CCTV: Developing Privacy Best Practices
Report on the DHS Privacy Office Public Workshop

Panel on Technology Perspectives

The panel on Technology Perspectives (Technology panel) opened the Workshop with an overview of CCTV technologies, including how the technology works, what it does today and will do in the future. The panel also discussed the problems and issues end users experience with the rapid development of new technologies, not only in equipment but also storage and transmission of data.

In the development and design of any CCTV system, the Technology panel recommended getting the information technology (IT) team involved early to establish the partnership between physical security and the IT infrastructure. The panel further recommended thinking through the day-to-day support plan, as if designing any other critical application. A camera program requires more than just the initial purchase of the cameras; it requires long-term operational planning and support.

The greatest issue that the Technology panel identified with regard to implementing a CCTV program was the application of video analytics – tools for analyzing motion, people, vehicles, and places. The panel described the rush to get more cameras as people find more value in the technology, but purchasing the cameras is the easy part, while using technology in an effective manner is much more challenging. The more cameras that are operating, the more video screens that are needed, as well as more human monitors to view the screens. This then results in more data that has to be analyzed, transported, stored, protected, etc. The panel stressed that quickly implementing video analytics requires more resources and may require more planning and time to reach the intended goal. In some instances, programs may have to be pulled due to inadequate resources to handle the number of false positives/false negatives that may result. The key, as stated by the panel, is to make sure that the use of the video -- the value that is being attained -- is equal to or greater than the cost of deploying the solution.

In addition to discussing video analytics, panelists also discussed computer vision technology and current research on quickly analyzing footage from large-scale video surveillance systems in order to track suspicious people or view suspicious activities. Panelists discussed applying privacy protections (*e.g.*, blurring images, encrypting data) for those persons who are not being tracked or involved in a particular incident, and noted that technology exists to unmask or recover high-resolution accurate images of faces if necessary.

The panel further discussed key considerations when installing CCTV systems, including the type of equipment based on the area under surveillance, the architectural requirements for placing the cameras, and the infrastructure requirements, including existing and non-existing, lighting, power, and weather.

The panel concluded its discussion by reviewing the challenges faced in implementing complex, large-scale CCTV systems and managing the large amount of data a large-scale CCTV system generates. The panelists noted the need to consider such items as: building relationships with

those individuals or organizations that can influence the outcome of the project; managing community commissions (*e.g.*, planning); managing owners of critical national infrastructure; dealing with potential union issues; continuity of operations with surrounding municipalities; addressing underestimated cost-drivers; ensuring availability of proper power and back-up power, if the system goes down; making key decisions such as LAN versus standalone systems; implementing overt versus covert systems to deal with deterring crime versus capturing acts of terrorism; and finally, addressing engineering, configuration control, and life-cycle management. In managing the large amount of data a large-scale CCTV system generates, the technology panel stressed the need to address: the challenge of information overload; information management and retrieval; what is done with the information after it is collected; and the personnel and expertise needed to actually use the system effectively.

Panel on International Perspectives

During the International Perspectives panel, privacy regulators from Canada and the United Kingdom discussed how their countries took the FIPPs into consideration either before or after implementing CCTV programs in their countries. The international privacy regulators referenced their guidelines or codes of practice on surveillance, which specify:

- Purpose specification (*e.g.*, what is the surveillance scheme trying to do? Is CCTV the best alternative?);
- Accountability/oversight (*e.g.*, who is legally responsible for the CCTV system? Private sector? Local government?);
- Use limitation *(e.g.*, cameras not intruding on private space when monitoring a town center, appropriate use of stored images, blurring faces);
- Transparency (*e.g.*, providing notice and contact information to the general public);
- Data quality (*e.g.*, image quality, hardware maintenance, etc.);
- Use limitation/retention (*e.g.*, restricting access, specifying timeframe for retention and in what mode);
- Security (*e.g.*, clear and well-documented handling procedures, training, guidelines for onward transfers, audit procedures; building privacy and security safeguards into the programs from the outset); and
- Access/redress (*e.g.*, staff awareness of the rights of individuals to have access to their images, exceptions, and a redress procedure).

The regulators evaluated the general population (through privacy impact assessments and consultations) and found that where individuals understand the benefit of CCTV technology, they are more trusting in its use. When they gauged how citizens felt about surveillance (including CCTV), however, they found that it was critically important to invest time garnering the public's trust when deciding to utilize this technology. Having a "consultative, collaborative, cooperative approach" was particularly important when implementing video surveillance cameras, and encouraging the private sector and concerned individuals to consult with regulators helped the regulators implement video surveillance within the law while still meeting the government's surveillance needs. Government agencies often found that technical surveillance was not the best use of resources; rather, additional police forces, better lighting, and the like were more effective.

The academics on the International panel discussed the rapid change in what is considered a "public" versus "private" space. They also defined surveillance to include audio, visual, and olfactory capturing devices, as well as other more technical systems, such as radio frequency identification devices (RFID). They described surveillance as a "complex cluster of technologies that are morphing all the time into different kinds of relations" and as such, privacy policies need to fluidly adapt to such emerging technologies. Trying to pinpoint the reasons for using CCTV also posed a problem, as they reported that most evaluations of CCTV have returned very mixed messages regarding its use and usefulness. In fact, most research found that CCTV did not stop crime, but was useful for obtaining evidence after the fact. Yet, many jurisdictions abroad continue to spend large amounts of money procuring such technology.

One of the academic panelists emphasized two important points addressing the FIPPs of oversight and transparency. He called out the data protection authority's ability to ensure compliance with the written CCTV guidelines; although with the privacy regulators limited resources, such oversight is almost impossible given the number of systems. Additionally, despite the requirement under the guidelines to provide notice to individuals that CCTV is in place, the public does not have a meaningful opportunity to withhold consent to having an image captured, used, or stored.

After the Workshop, the United Kingdom's Information Commissioner's Office issued an updated "CCTV Code of Practice,"[1] which takes into account technology, advances in the use of CCTV, and the wider legal environment in which it operates. The Office of the Privacy Commissioner of Canada and the Ontario Information and Privacy Commissioner have also issued a number of publications dealing with video surveillance.[2]

Panel on Community Perspectives

Five communities took part in the Community Perspectives panel discussion. The cities included Stamford, Connecticut; Baltimore, Maryland; Norfolk, Virginia; Chicago, Illinois; and Hyattsville, Maryland. Each city representative discussed their community's approach to implementing CCTV technology. Two cities have very elaborate programs in place (Chicago and Baltimore), while others were in the process of designing their program (Stamford and Hyattsville). Each city discussed lessons learned and noted some of their successes and recommendations for other cities to consider when implementing CCTV programs.

The board representative from the city of Stamford, Connecticut began the Community panel by noting lessons learned from Stamford's CCTV implementation experience. First, he advised

---

[1] Information Commissioner's Office, *CCTV Code of Practice, revised addition,* (2008), a*vailable at* http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/ico_cctvfinal_2301.pdf

[2] Office of the Privacy Comm'r of Canada, *OPC Guidelines for the Use of Video Surveillance of Public Places by Police and Law Enforcement Authorities* (Mar. 2006), *available at* http://www.privcom.gc.ca/inforamtion/guide/vs_060301_e.asp. *See also* Info. & Privacy Comm'r of Ontario (Canada), *Guidelines for Using Video Surveillance Cameras in Public Places* (Sept. 2007), *available at* http://www.ipc.on.ca/images/Resources/video-e.pdf.

communities to have policies and procedures in place before launching a program. Second, he recommended having a collection of "horror stories" about CCTV abuses to share with council members in order to stress that abuses can and do occur and need to be accounted for in the CCTV policies. Finally, he recommended including specific language in local ordinances referencing what abuses can occur in the absence of clear policies and procedures, so where council members are unable to understand the specific technical language of the ordinance, they can still understand what abuses the ordinance is intending to prevent.

The council member from Norfolk, Virginia discussed Norfolk's approach to implementing CCTV technology by addressing key first steps such as having policies in place, conducting site visits to other cities, and obtaining public support. The council member noted the importance of integrated resources (*e.g.*, courts, transportation, and government entities) and the need to not oversell the abilities of the cameras. Further he stressed the importance of having protections in place to guard against abuses to the extent possible since abuses will happen. Finally, the council member provided insights into making Norfolk's CCTV program more effective by using cameras in conjunction with other safety measures, such as more lighting, better public access, and promoting community action.

Two representatives participated from the city of Baltimore, Maryland, one from the mayor's office and the other from the private-public partnership that funded the city's downtown camera program. The representatives discussed the implementation of the city's CCTV system and its effectiveness in deterring crime. Baltimore hired a law firm to help develop protocols that had even more privacy protections than what the law required. The Baltimore representatives also noted the transparency of Baltimore's program, including signs on every block notifying of the use of video surveillance and allowing the community to come in and view the monitoring sites. The Baltimore representatives further noted the checks and balances that are in place to deter abuse, including only using cameras that see what the naked eye can see, having two or more well-trained monitors on duty at all times, and having video feeds that can be viewed in numerous locations, so people can see what the monitors are looking at. The panelists noted that, after the first month, there was a 50 percent decrease in crime from the previous year, and that crime dropped in every area where cameras were placed. From 2000 to 2006, the crime in the downtown area declined 47.75 percent and is now considered the safest place in Baltimore.

Chicago is another city with a mature CCTV system. The Chicago panelist noted a number of items that make Chicago's system effective, including the use of multiple and legacy systems; the varied sources of funding for each system (*e.g.*, state, federal, city and forfeiture money); the policies and procedures the city has in place (including data retention schedules); and the city's adherence to a consent decree, which addresses issues like audits, training, and data storage, and ensures everyone understands the requirements for operation of a surveillance system. He noted a number of key challenges, including understanding the power of developing technologies and the integration of different technologies, such as gunshot detection technology with video, olfactory technology with video, and targeted video along with bomb detection technology. He also identified a number of other challenges: funding system maintenance; Freedom of Information Act (FOIA) requirements; concerns regarding requests for certain data and the potential for abuse (*e.g.*, people using data about others to violate privacy or to perpetrate

identity theft); and managing and preserving data so as to not violate evidentiary requirements or destroy exculpatory evidence.

Taking a different approach, the city of Hyattsville, Maryland contracted an IT consulting firm to help develop a roadmap for implementing its CCTV program, which would focus on commercial and development areas based on crime statistics. The panelist from Hyattsville highlighted its recently completed, independent assessment to review surveillance requirements for the city. The assessment included site surveys at locations of interest, deployment and operations recommendations, and an outline of steps to meet the city's surveillance goals. The city held public meetings to make sure the community had ample opportunity to weigh in on its program. Following the introduction of the program, a final report was made available to the community. The report addressed system design, technology, effect on the community, awareness, views from all the proposed camera locations, and feedback or concerns on camera views. The city partnered with local businesses and developers for funding assistance and infrastructure and has seen a great deal of success as a result of its planning.

A key part of the assessment was the recommendation that the system must allow for accountability of the data being captured and how it is handled. The assessment stated that the surveillance system must have the ability to demonstrate that the use of the system has been limited to its intended justice and public safety purposes. It provided that this could be accomplished by including accountability features that allow for the city to report on the usage of the system – access, data capture and retention policies. The assessment noted that such accountability is paramount in maintaining public confidence that the information being gathered is properly protected and utilized in a manner that demonstrates respect for individual rights and privacy.

Hyattsville has adopted a policy-first approach before installing any cameras. The city is using policy recommendations from the Urban Institute and is contacting other municipalities who have proceeded with CCTV implementation to obtain their policies for review. Community involvement and transparency considerations include a joint monitoring program and community access to observe what is being monitored, how it is being monitored, and how it works. The community is also involved in the development of training requirements and policies. Hyattsville's goal is to be a model city for the implementation of a CCTV system.

Panel on Law Enforcement Perspectives

The panel on Law Enforcement outlined three reasons to implement CCTV technology: deterrence; response; and investigation. The Law Enforcement panelists commented favorably on the use of CTTV for evidence after a crime has been committed and gave many examples of how it has served as a key tool in solving crime. All panelists agreed it is typically most beneficial for "after the fact" cases, where you can go back and search the video camera for clues. One law enforcement official stated that their camera system is "event driven," meaning no one actually watches the footage 24/7, but they use it when incidents arise and the cameras potentially hold information that may help to solve a crime.

Law Enforcement panelists further noted that CCTV can benefit the safety of officers responding to calls as well as spot crimes taking place. If the cameras are monitored while a crime is taking place, law enforcement would be able to dispatch an officer to the scene. In situations where officer safety is an issue, a dispatcher or monitor would be able to observe the scene even before an officer is sent.

CCTV can also assist with the allocation of key resources. For example, cameras can be set up in safer areas of a community allowing municipalities the opportunity to allocate additional police officers to more troubled areas of a city. In addition, cameras in high surveillance detection areas can be used to avoid unnecessary police investigations and responses (*e.g.*, determine that an activity is legal and no police response is necessary.)

Law Enforcement representatives stated that if given the option to choose between more police officers or CCTV, they would always choose the officers. Nevertheless, most communities are welcoming and inquiring about CCTV placement. All of the panelists agreed, however, that it is absolutely critical for communities to think carefully through their needs, understand what the cameras can and cannot do, have a thorough review and assessment, and then develop policies to address how the cameras will be used and privacy protected before rolling out a CCTV program.

Many businesses have requested that law enforcement install cameras in "business districts," often times offering to pay for the cost of the equipment. Private businesses have increased interest in CCTV for crime prevention and to assist in solving crimes after the fact. This brings up a number of challenges for local law enforcement. For example, will police monitor these privately-owned cameras? If so, who will pay for the police to do so? Will the police have real-time access to these cameras? Will poorer neighborhoods that do not have businesses to subsidize the cost of cameras in their area be neglected?

Law Enforcement panelists made the case for having relationships with local businesses to save on the cost of cameras and to cover more public space than with law enforcement controlled cameras (*e.g.*, parking lots and streets).

As the conclusion of the panel, researchers from the Urban Institute previewed their outline for a new two-year study into the effectiveness of CCTV in four selected communities. The study, funded by the Department of Justice, hopes to provide important findings to help guide policymakers' future decisions regarding CCTV deployment. The Institute study will examine how camera systems are implemented and used, as well as look at ways that cameras may have both positive and negative impacts, including exploring some of the unintended consequences of CCTV use. The research will look at community needs, camera types, implementation decisions such as camera location, and will also seek to evaluate the costs and benefits of these systems in these four communities.

Panel on Legal and Policy Perspectives

The panel on Legal and Policy Perspectives provided the context for the many issues and concerns raised by the previous four panels. The Legal and Policy panelists agreed that it would be difficult to argue against the use of CCTV on the basis of current case law, but the growing

pervasiveness of the technology could lead to more stringent requirements and a call for greater Fourth Amendment protections in the future. The challenge with developing laws and regulations for the use of CCTV is the traditional notion that there is a lower expectation of privacy in public places. Some Legal and Policy panelists suggested, however, that this notion should be revisited in light of the growing use of CCTV and its capabilities. Others also suggested using criminal procedure principles and limiting police discretion through judicial oversight, while providing transparency in the process.

Although the panelists agreed that CCTV technology may be a helpful tool for law enforcement, they expressed the need to protect individual privacy and civil rights and civil liberties when deploying this technology. Because cameras can capture everyday behavior, some people may cease to do certain activities or refrain from acting in certain ways if they know they are being watched. For example, CCTV could capture intimate behavior that individuals routinely do in public in a free society (*e.g.,* going to a doctor, an Alcoholics Anonymous meeting, an HIV-Aids or abortion clinic, and displays of affection) or capture legal behavior in the course of conducting public safety activities (*e.g.,* monitoring public protests, traffic, or public transportation). Most people would find it unsettling to be the subject of constant or intense surveillance.

The Legal and Policy panelists discussed locations where having CCTV may be beneficial, including venues where a large number of the public are moving through constricted spaces and where there are significant public safety concerns. Such venues include stadiums and mass transit systems. They also stressed the need to be specific about where cameras are placed, what cameras are used, what their capacity is, and what they are being used for. Many panelists agreed that these decisions should be made public and allow for public input.

The Legal and Policy panel discussed the special concerns raised in communities where law enforcement and private-sector owners of cameras have a special relationship, making the wall between the public and private sector in some instances porous or even non-existent. They suggested that there should be justification for government access to private sector, third-party surveillance records based on either incident reports or businesses that are located in designated high crime areas. Other Workshop panels also recommended that communities adopt rules justifying and limiting government use of private-sector cameras and providing protections against misuse.

The Legal and Policy panel agreed that the Fourth Amendment also covers government use of CCTV obtained from private-sector entities, whether government has access directly to a business video feed, or a business turns over surveillance tapes to the police upon police request. Some communities are now requiring, as part of the building permit approval process, that police have the ability to monitor everything in the store as a condition of operating a store (*i.e.,* continuous data feeds vs. traditional data dumps). The panel responded, however, that camera footage and images obtained through such private-public partnerships should be subject to the same data policies and limitations that apply to information collected by government cameras (*e.g.,* masking, retention periods, and limitations on dissemination.)

Most importantly, the Legal and Policy panel provided an overview of the law concerning the regulation of government surveillance. Primarily, the panel focused on the Fourth Amendment

and the right to be protected against unreasonable searches and seizures and the "reasonable expectation of privacy" test. One of the academic panelists provided the following synopsis of the current law in this area and the principles defining what constitutes a "search":

Kyllo v. the United States.[3] *Kyllo* involved the government's use of thermal imaging to discern heat differentials inside the home. The Supreme Court ultimately determined that the use of thermal imaging was a search as defined by the Fourth Amendment; however, the Court made clear that looking into a home with the naked eye from a lawful vantage point may not be a search (*e.g*., police on the sidewalk looking into the home through a picture window). The Court went further to state that it is not a search if the police use technology to duplicate what the police would see if standing on the sidewalk. The Court added that if technology "in general public use" is used to see more than the naked eye (*e.g.*, telescope, binoculars, etc.) then it is not a search. "General public use" is further defined as that which is generally available to the public.

United States v. Knotts.[4] *Knotts* involved the use of CCTV in public spaces and the police's use of a tracking device to track a car through public streets. The Court ruled such tracking was not an illegal Fourth Amendment search because there was no expectation of privacy even if the police are using enhanced technology to view what was going on in public. The Court's ruling brought up the question of "dragnet surveillance," which the court in *Knotts* said would probably be considered a search. The Court further hinted that had the surveillance been used for a long period of time, say over multiple days, then it may have constituted a Fourth Amendment search. To date, however, the Court has not considered that issue.

Katz v. United States.[5] *Katz* involved the use of audio surveillance and the bugging of a public phone booth. The Court ruled that the surveillance applies to the person and not the location and that intercepting conversations in public where the person clearly was seeking privacy, in this case, going into a phone booth, was considered a search. Therefore, according to the Legal and Policy panelists, CCTV involving audio as well as visual surveillance could well constitute a Fourth Amendment search.

A Legal and Policy panelist, quoting court dictum in a state case, further indicated that the use of CCTV could be a search under the right circumstances, *e.g*., where video surveillance is aimed indiscriminately in public places and captures lawful activities of many citizens in the hope that it will deter crime or capture what crime may occur, or where police use private agents or entities as agents."[6]

---

[3] *Kyllo v. United States* (99-8508) 533 U.S. 27 (2001) 190 F.3d 1041, reversed and remanded.
[4] *United States vs. Knotts* 460 U.S. 276 (1983)
[5] *Katz v. United States*, 389 U.S. 347 (1967)
[6] In *State of Vermont v. Michael N. Costin*, the lower court said in dictum that while in this case video surveillance was used in a narrow set of circumstances to substitute for in-person surveillance, this was not a case "where video surveillance is aimed indiscriminately at public places and captures lawful activities of many citizens in the hope that it will deter crime or capture what crime may occur." 168 Vt. 175; 720 A.2d 866 (July 31, 1998).

Indianapolis v. Edmond.[7] In this case, the Court considered a related public space issue, whether it is permissible to conduct a roadblock without a warrant and without proper cause. The Court held that such a roadblock is permissible, so long as a higher authority authorizes the roadblock and either the police who are implementing the roadblock have a reasonable suspicion to believe the person they are stopping has evidence of a crime in their vehicle or has committed a crime, or there is proof of a significant crime problem that the roadblock is designed to address.

Although the courts typically look to the Fourth Amendment in deciding public space cases, the Legal and Policy panel suggested that the use of CCTV raises other Constitutional issues. These include:

- First Amendment -- Does the use of CCTV in public spaces chill freedom of speech and/or association? If "yes," then the government may need justification in order to engage in use of cameras in public spaces.

- Due Process Clause (the right to travel and the right to repose) -- Does the use of CCTV in any way chill or infringe on the right to travel or the right to loiter? If the answer is "yes," then the government may need justification under the due process clause to engage in CCTV.

- Equal Protection Clause -- Is CCTV being used to intentionally discriminate against suspect classes on the basis of race or gender? If the answer is "yes," then its use may have constitutional implications.

The Legal and Policy panel also suggested additional factors to consider in implementing and managing CCTV systems. These include:

State Constitutions – A number of state courts have indicated that their State constitutions are more protective than the Federal Constitution and that the search and seizure provisions in their State constitution may provide a source of regulation for CCTV.

Money – If the Federal government was not providing funding through a grant process to develop camera systems, local communities may have imposed heavy regulation, or even the abolition of CCTV, due to excessive costs and questions regarding effectiveness of CCTV systems. The panel suggested that without Federal funding municipalities may have been more apt to condition funding based on the development of appropriate policies.

Wiretap Act[8] – Cameras set up by law enforcement inside a home or business is a Fourth Amendment search, and the requirements for the use of CCTV may parallel the requirements of the Wiretap Act, which require the following preconditions:

1. Normal methods of law enforcement have failed or are not worth trying;
2. A description of the non-verbal conduct to be monitored;
3. The period of interception is limited to that which is necessary to achieve the objective; and

[7] City of Indianapolis v. Edmond, 531 U.S. 32 (2000)
[8] 18 U.S.C. §§ 2510-2522.

4. The interception of conduct must be minimized.

Panel on Developing Privacy Best Practices for the Use of CCTV

The final panel of the Workshop brought together representatives from each of the prior panels to make recommendations to guide the development of best practices for the use of CCTV. First, panelists urged that DHS show fiscal responsibility and policy leadership by conducting effectiveness studies of existing CCTV programs and privacy and civil liberties impact assessments. Second, they urged DHS to show leadership by inviting communities that apply for DHS grants for CCTV projects to implement a process, prior to grant application, that includes public notice, impact assessments, authorizations by votes of elected officials, and an opportunity for the public to comment on the decision to seek CCTV funding. Following grant money awards, the Best Practices panel recommended a public process in the selected communities to determine placement and use of CCTV systems. Some panelists even urged adoption of Federal standards, enforced by law.

The Best Practices panel recommended that, following installation or before additional cameras are purchased and installed, communities enact legally-binding ordinances and require annual evaluations, involving an independent entity, of the usefulness and effectiveness of the system, with distribution to DHS and elected officials, and available to the public.

One Best Practices panelist stated that such standards would lead to better planning and structure, increase the chance for successful implementation, achieve the targeted public safety goals, and provide for a better informed public. The benefits to the public would include a balanced discussion of whether these are the strategies they want their communities to employ, an understanding of the consequences of using CCTV, and a sense that the public has been listened to by their local government.

Several panelists presented best practice principles that were based upon the FIPPs. They offered the following set of recommendations:

Principle of Transparency

- Use publicly accountable procedures to establish the system (an open and public forum).
- Use signage to alert the public to the presence of cameras.

Principle of Individual Participation

- Invite public comment as part of the process to establish the system.
- Permit public access to images pertaining to themselves to the extent possible.

Principle of Purpose Specification

- Use video surveillance only to further a clearly articulated law enforcement principle.
- Set clear, objective standards to evaluate effectiveness of the CCTV system.
- Design the system to ensure that it achieves its objective.

Principle of Data Minimization

- Determine whether video surveillance is needed to accomplish the community's law enforcement purpose.
- Compare the cost of a public video surveillance system to alternative means of addressing the stated purposes.

- Design the scope and capabilities of a public video surveillance system to minimize its negative impact on constitutional rights and values.

Principles of Use Limitation

- Prohibit sharing of public video surveillance data with third parties and set appropriate limits on sharing public video with other governmental agencies.
- Require additional specific approvals to use more intrusive technologies.
- Require additional specific approvals to use stored footage for a secondary purpose -- a law enforcement purpose other than the original purpose for which the system was designed and installed.

Principle of Data Quality and Integrity

- Provide safeguards for use of stored video surveillance data, such as requiring digital watermarks.
- Provide safeguards, such as training for personnel with access to a public video surveillance system.
- Establish data retention policies under which recorded footage lacking evidentiary value will be routinely destroyed after a determined length of time.

Principle of Security

- Provide appropriate sanctions against misuse and abuse of public video surveillance systems, as well as remedies for those harmed by such misuse or abuse.
- Create technological and administrative safeguards to reduce the potential for misuse and abuse of the system.

Principle of Accountability and Auditing

- Conduct periodic audits to assess the system's effectiveness, its impact on the community, and its adherence to the system's stated primary purpose.
- Define and enforce penalties for system violations.
- Diligently guard against "mission creep."
- Apply to any law enforcement use of privately collected video data the same standards that apply to public video data.

Workshop Conclusion

The Workshop provides a valuable record to inform policy development regarding government use of CCTV. Throughout the Workshop, panelists agreed that although camera technology cannot prevent or solve every crime, it may be a useful tool if used properly and if protections are in place to prevent abuse. As demonstrated, U.S. cities are experiencing successful implementation of new CCTV programs by taking pre-implementation steps including community involvement, transparency and, in some cases, conducting thorough studies and evaluations. Front-runners in the CCTV arena provided valuable resources and information for lessons-learned and best practices.

As demand and awareness for CCTV grows, so too does the importance of drafting a thorough set of policies to address privacy and civil liberties. The Workshop panelists recommended that such policies contain, at a minimum, the following elements:

1. Definition of appropriate use;
2. Access rights for those whose images are identified and retained;
3. Security controls governing the camera footage and images;

4. Appropriate limits on the location of cameras;
5. Monitoring for inappropriate uses;
6. Retention policies;
7. Adequate training of personnel with access to the systems; and
8. Internal and external auditing.

A number of Workshop panelists encouraged using the FIPPs to provide a framework for such policies. Moreover, if CCTV technology is going to be adopted, community involvement and public support will most likely lead to a better and more widely accepted program. Although some panelists agreed that if given the option of having police officers versus cameras, they would choose police officers, proponents of CCTV will continue to urge adoption of CCTV, particularly if the local community readily supports such efforts and funding continues to come from the Federal government. Government and community proponents of CCTV technology will garner greater public acceptance and support for the use of CCTV if they provide: (1) thoughtful planning to demonstrate a cost-benefit analysis to support the decision to employ CCTV; (2) opportunities for community involvement; and (3) written policies setting forth the elements described above.

In short, while the demand for cameras is growing throughout communities across the nation, all of the Workshop panelists cited the importance of public support from within the community about the use of cameras and strongly supported drafting and implementing policies to protect privacy and civil liberties before undertaking CCTV programs.

APPENDIX A

DECEMBER 17 and 18, 2007

CCTV: DEVELOPING PRIVACY BEST PRACTICES

Hilton Arlington

Gallery Ballroom
950 North Stafford Street, Arlington, Virginia
(Ballston Metro)

Day One – December 17, 2007 **Morning Session**	**8:30 a.m. – 12:15 p.m.**

Welcome and Introductions 8:30 a.m. – 8:45 a.m.

Hugo Teufel III, Chief Privacy Officer,
U.S. Department of Homeland Security

Daniel Sutherland, Officer for Civil Rights and Civil Liberties,
U.S. Department of Homeland Security

Technology Perspectives 8:45 a.m. – 10:30 a.m.

Moderator: Peter E. Sand, Director of Privacy Technology,
DHS Privacy Office

Panelists:

Larry S. Davis, Chair and Professor,
Department of Computer Science,
University of Maryland

Samuel J. Docknevich, National Practice Leader,
Digital Surveillance and Physical Security Services,
IBM Global Services

Randy Hoffmaster, Epsilon Systems Solution, Inc.

Jennifer King, Research Specialist,
Samuelson Law, Technology and Public Policy Clinic,
University of California-Berkeley School of Law

Larry Strach, Executive Vice President, Engineering,
Duos Technologies

Break 10:30 a.m. – 10:45 a.m.

Day One – December 17, 2007 **Morning Session, *continued***	**10:45 a.m. – 12:15 p.m.**

International Perspectives 10:45 a.m. – 12:15 p.m.

Co-Moderators: Shannon Ballard & Lauren Saadat, Associate Directors, International Privacy Policy**,** DHS Privacy Office

Panelists:

Ken Anderson, Assistant Commissioner,
Information and Privacy Commission,
Ontario Province, Canada

Wade Deisman, Professor, University of Ottawa, Canada

Phil Jones, Assistant Commissioner,
Information Commissioner's Office, United Kingdom

Clive Norris, Professor, University of Sheffield, United Kingdom

No-Host Lunch Break	**12:15 p.m. – 1:30 p.m.**

Day One – December 17, 2007 **Afternoon Session**	**1:30 p.m. – 5:00 p.m.**

Law Enforcement Perspectives 1:30 p.m. – 3:30 p.m.

Moderator: Ken Hunt, Director of Regulatory & Legislative Affairs, DHS Privacy Office

Panelists:

Mike Fergus, Project Manager, Video Evidence Projects,
International Association of Chiefs of Police

Robert Keyes, Chief of Police, Clovis, California

Nancy G. La Vigne, Senior Research Associate,
The Urban Institute

Randy Myers, Senior Attorney**,** U.S. Park Service,
Department of the Interior

Thomas J. Nestel III, Chief of Police,
Upper Moreland Township, Pennsylvania

Break 3:30 p.m. – 3:45 p.m.

Day One – December 17, 2007 **Afternoon Session, *continued***	**3:45 p.m. – 5:00 p.m.**

Community Perspectives 3:45 p.m. – 5:00 p.m.

Moderator: Timothy Keefer, Deputy Officer for Programs & Compliance, DHS Office for Civil Rights and Civil Liberties

Panelists:

Philip Berns, City Representative,
Stamford, Connecticut Board of Representatives

Norman Currie, Program Manager,
UNISYS

Donald R. Zoufal, Special Assistant to the Director,
Illinois Emergency Management Agency

Elizabeth "Beth" Hart, CCTV Manager,
Baltimore City Mayor's Office

Amy E. Lassi, Project Management Officer,
Grant Development & Administration Division,
Grant Program Directorate, FEMA, DHS

W. Randy Wright, City Council Member, Norfolk, Virginia

Eugene "Tom" Yeager, Executive Vice President,
Clean and Safe Programs, Downtown Partnership of Baltimore, Maryland

Closing Remarks for Day One	**5:00 p.m.**

Day Two - December 18, 2007 **Morning Session**	**8:30 a.m. – 12:30 p.m.**

Legal and Policy Perspectives 8:30 a.m. – 10:30 a.m.

Moderator: Toby M. Levin, Senior Advisor, DHS Privacy Office

Panelists:

Marc Jonathan Blitz, Assistant Professor,
Oklahoma City University School of Law

James Jay Carafano, Assistant Director and Research Fellow,
The Heritage Foundation

Fred Cate, Distinguished Professor and Director,
Center for Applied Cybersecurity Research,
Indiana University

Deirdre K. Mulligan, Director,
Samuelson Law, Technology & Public Policy Clinic,
Boalt Hall School of Law,
University of California - Berkeley

Christopher Slobogin, Professor,
University of Florida Law School

Break 10:30 a.m. – 10:45 a.m.

Day Two - December 18, 2007 **Morning Session,** ***continued***	**10:45 a.m. – 12:30 p.m.**

Developing Privacy Best Practices for the Use of CCTV 10:45 a.m. – 12:30 p.m.

Co-Moderators: Toby M. Levin, Senior Advisor, DHS Privacy Office and **James McNeely,** Counsel for Civil Liberties Programs**,** DHS Office for Civil Rights and Civil Liberties

Panelists:

Lillie Coney, Associate Director,
Electronic Privacy and Information Center

Sophia Cope, Staff Attorney,
Center for Democracy and Technology

Sharon Bradford Franklin, Senior Counsel,
The Constitution Project

Jennifer King, Research Scientist and Information Specialist,
Samuelson Law, Technology and Public Policy Clinic,
University of California-Berkeley

Thomas J. Nestel, III, Chief of Police,
Upper Moreland Township, Pennsylvania

Clive Norris, Professor,
University of Sheffield, United Kingdom

Nicole A. Ozer , Technology and Civil Liberties Policy Director,
ACLU of Northern California

Barry Steinhardt, Director,
Technology & Liberty Program, ACLU

Closing Remarks	**12:30 p.m.**

The Privacy Office, U.S. Department of Homeland Security, Washington, DC 20528
Telephone: 703-235-0780 Fax: 703-235-0442
privacyworkshop@dhs.gov www.dhs.gov/privacy
(Follow the links to the Workshop Section)

APPENDIX B

Best Practices for Government Use of CCTV: Implementing the Fair Information Practice Principles

Introduction

The Department of Homeland Security (DHS) Privacy Office and Office for Civil Rights and Civil Liberties are issuing *Best Practices for Government Use of CCTV: Implementing the Fair Information Practice Principles* to educate government agencies interested in building privacy, civil rights, and civil liberties considerations into Closed Circuit Television (CCTV) system design, acquisition, and operations. Government agencies are encouraged to use these best practices to build and operate CCTV systems that improve law enforcement effectiveness while preserving privacy and civil liberties. Taking such actions now can help ensure that efforts to improve security do not lead to the creation of a surveillance society.

In addition to considering implementation of these best practices, law enforcement leaders and political decision makers should carefully consider conducting a cost-benefit analysis before selecting CCTV over other tools to fight crime or improve security. A CCTV program is more likely to gather public support when the protected community understands the objectives of the program and knows that it is the result of a thoughtful analysis.

These best practices are written using the widely-accepted framework known as the Fair Information Practice Principles (FIPPs). These principles are: Transparency, Individual Participation, Purpose Specification, Data Minimization, Use Limitation, Data Quality and Integrity, Security, and Accountability and Auditing. The eight FIPPs are at the core of the Privacy Act of 1974 [5 U.S.C. § 552a] and are mirrored in the laws of many U.S. states as well as many foreign nations.

Material for drafting these best practices was also drawn from the proceedings of the DHS Privacy Office Public Workshop, *CCTV Developing Privacy Best Practices*, which was held on December 17 -18, 2007, and the comments filed in conjunction with the workshop. At that workshop, elected U.S. and international officials, law enforcement executives, public interest advocates, academics, and technologists offered a variety of opinions on best practices for implementing CCTV systems while respecting privacy and civil liberties. The discussion of best practices focused on practical recommendations for law enforcement agencies. A report of the highlights of the workshop, along with a complete transcript and comments filed, are available at www.dhs.gov/privacy.

The DHS Privacy Office and the Office for Civil Rights and Civil Liberties are undertaking the development of these best practices to fulfill their statutory duties, and the Department's mission to protect the homeland, including preserving our freedoms and our way of life. Section 222 (a)(2) of the Homeland Security Act of 2002, as amended [6 U.S.C. 552142], as amended, directs the Chief Privacy Officer of DHS to assure that the Fair Information Practice principles are implemented at the Department. The DHS Officer for Civil Rights and Civil Liberties is

directed in Section 705 (a)(3) of the Act, as amended [6 U.S.C. § 345] to "ensure that the protection of civil rights and civil liberties is appropriately incorporated into Department programs and activities." Because the Department funds the purchase of CCTV systems and analogous technology through Homeland Security Grants and other programs, DHS Privacy Office and the Office for Civil Rights and Civil Liberties believe it is important for DHS to help inform government agencies on how to implement CCTV programs in a manner that respects these fundamental rights and values.

These best practices do not take a position on the costs or benefits of CCTV, but rather provides a list of considerations a government agency should address as part of its decision making and planning. The DHS Privacy Office and the Office for Civil Rights and Civil Liberties invite the public to comment on these best practices, as they may be revised in the future as the technology evolves, and based on experience gained from its implementation and from public comments. Comments or questions regarding these best practices may be sent to privacy@dhs.gov.

Fair Information Practice Principles (FIPPs)

The privacy principles outlined here are based upon the FIPPs, a set of principles that have long served as a framework for protecting privacy within the United States and internationally. These principles were first articulated in the U.S. Department of Health, Education, and Welfare's 1973 report entitled, *Records, Computer, and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems*. The report identified eight practices, which later served as a basis for the U.S. Privacy Act of 1974.

The U.S. government has also long promoted the FIPPs internationally. In 1980, the FIPPs served as the basis for the 1980 Organization for Economic Cooperation and Development (OECD) *Guidelines on the Protection of Privacy and Transborder Flow of Personal Data*. Later in 1995, a variation of these principles was the basis of the European Union Data Protection Directive. As recently as 2004, the FIPPs were championed again by the United States in the development of the Asia-Pacific Economic Cooperation (APEC) Privacy Framework.

Section 222 of the Homeland Security Act of 2002, as amended, which is the basis for the authorities and responsibilities of the DHS Chief Privacy Officer, also recognizes the significance of the FIPPs, calling on the Chief Privacy Officer to "assur[e] that personal information contained in Privacy Act systems of records is handled in full compliance with *fair information practices* as set out in the Privacy Act of 1974." (Italics added for emphasis.) Pursuant to Section 222, the Privacy Office has applies the FIPPs in its Privacy Impact Assessment guidance and throughout its operations.

The best practices articulated below apply these widely-held principles to the privacy concerns associated with the government's use of CCTV. Each FIPPs principle is followed by examples of how to implement the principle in the context of CCTV.

Purpose Specification Principle

Each government agency should specifically articulate the authority that permits its use of CCTV and specifically articulate the law enforcement purpose(s) for which CCTV is intended to be used.

(1) Know why you want to deploy CCTV. What is your current law enforcement strategy and what role can CCTV play?
   a) To the extent feasible, conduct a study or literature review of the effectiveness of CCTV for the intended purpose. Consideration of how CCTV might be employed effectively (or how it might not be helpful) may assist in the decision making. Make the results of the study available to the public.
   b) Determine whether CCTV is intended to assist in for crime detection, crime prevention, or to assist in crime investigations, or to secure critical infrastructure from possible terrorist threat.
   c)
   d) Evaluate whether there are alternative means of addressing the stated purpose, particularly alternatives that are less intrusive on privacy and civil liberties. Alternatives may include area lighting, community policing, or crime prevention programs to address root causes.
   e) Determine whether resources will be available, long term, to properly operate the system properly. This should take into account funding, staffing, physical logistics, and maintenance, among other things.

(2) Know whether you have the legal authority to employ CCTV.
   a) Have a clearly articulated law enforcement purpose before setting up a CCTV system. Continue to ask when designing, building, and operating the system, whether it is capable of effectively achieving that purpose.
      Example: Determine whether the system will serve a crime prevention or evidentiary purpose and develop appropriate protocols for such purpose(s).

(3) The cameras and the camera network should be equipped with only those features or capabilities reasonably necessary to serve the purpose of the system. Technological features like magnification, night vision, infrared detection, and automatic identification and tracking, which pose significant dangers to privacy and other constitutional rights and liberties, should be used only where they are needed.
   a) Example: A camera network created to monitor a busy urban freeway for accidents or stopped vehicles likely does not require facial recognition technology—the use of which would increase the impact on civil liberties and increase the cost of the system without furthering its legitimate purpose.

Transparency Principle

Each government agency considering the use of CCTV should be as transparent as possible and provide notice to the public regarding its use of CCTV. There should be no secret use of CCTV. Each agency should have a written CCTV policy that governs the collection, use, maintenance, and disclosure of all camera footage or images.

(1) Where possible, involve the community in the decision making process to adopt CCTV. Establishing surveillance within a community can have major impact because even ordinary, law-abiding people may resent the presence of an "all-seeing eye."
   a) Government agencies should give community stakeholders adequate notice when considering the use of CCTV and provide an opportunity for meaningful public comment. In addition to gauging possible community response to an installed CCTV system, this presents the decision-makers with a chance to win community support, which can contribute to the success of law enforcement and security efforts in the future.
   b) The process should be public and include public notice, an assessment of how the system will likely impact privacy and civil liberties, and should state how the system will be authorized. A CCTV initiative will be better received if it is the subject of deliberations and is rolled out with the assent of politically accountable officials, such as city council members or an elected law enforcement officer.
   c) Town meetings, deliberation by the elected governance of a city or town, administrative notice and comment process, public hearings, voter referendum or neighborhood canvassing are all acceptable means of involving the public and demonstrating government accountability.
      i) Stakeholders include representatives from law enforcement, homeland security, emergency management, academic, legal, political, business, civic, religious, civil liberties protection, and technologists, as well as those citizens who wish to participate in the public process.
(2) Conduct a cost-benefit analysis as part of the decision making process and make that information available to the public.
   a) Conducting such an analysis may be difficult given that privacy and civil liberties are difficult to quantify; however, a number of factors can be evaluated: locations, number of cameras, capabilities, type of network, database design, storage retention, active or inactive monitoring, security measures, and alternatives.
(3) Prepare a written policy defining the mission of the system, how the cameras will be used, the rules of operation, and the privacy and civil liberties protections that have been provided to protect against misuse or abuse.
   a) Identify the system administrator responsible for all operational and administrative elements.
   b) Explain the system's capabilities; how it will be used, image retention, and release; and access to video center and image storage locations.
   c) Note the legal and administrative restrictions for its use.
      i) Address the privacy and civil liberties concerns discussed in this guidance.
      ii) Consider issues such as maintaining the integrity of evidence, the possible uses of CCTV footage and images (prosecution, defending against or substantiating officer abuse claims) as well as more troublesome uses (*e.g.*, subpoena by third parties attempting to prove or disprove matters at issue in unrelated civil litigation, such as divorce cases).
(4) Make as much of the agency's documentation (*e.g.*, policy, standard operating procedures, records disposition schedule, etc.) as possible publicly available.

Individual Participation Principle

Each government agency considering the use of CCTV should involve the public to the greatest extent possible in its decision to employ CCTV. Ideally, public involvement should take place before the agency applies for grant funding from the Department of Homeland Security. To the extent practical, the agency should provide notice through appropriate signage in areas where CCTV is employed and provide mechanisms for appropriate access and redress regarding the use of camera footage or images.

(1) Provide individuals a method to access images of themselves, if the camera footage or images are retained in a manner that identifies the individual and permits retrieval.
(2) Access rights, however, should not be used to justify archiving footage.
(3) Time-limited archiving is always preferable from a privacy perspective and possibly from a system management standpoint as well.
    a) Data retention and storage quickly becomes very expensive, and the stored data is frequently useless.
    b) A short retention period will reduce the number of access requests.
    c) A well-designed policy for a system that stores data should include procedures for identifying footage or images that should be retained, indexing and storing it in a retrievable manner, and establishing a chain of custody over footage or images that may be of legal significance.
(4) A policy that some CCTV system operators have found useful in this respect is permitting individuals to inspect, at any reasonable time (*e.g.*, in a non-crisis period and without compromising the security of critical infrastructure), the agency's camera monitoring operations center. In addition to permitting individual access and establishing transparency and oversight, this can serve an important public relations purpose, reassuring the community about the reasonableness of the CCTV use and the good faith of the CCTV operators. Agencies permitting this type of open access to CCTV operations report community support for monitoring.

Data Minimization Principle

Each government agency should only use CCTV to the extent relevant and necessary to accomplish the specified purpose(s) and only retain the camera footage or images for as long as is necessary to fulfill the specified purpose(s). The camera footage or images should be disposed of in accordance with a specified records disposition schedule.

(1) Design the scope and capabilities of the system to minimize its negative impact on privacy and other constitutional rights and values by limiting the data collected to the data that is likely to help accomplish the mission and limiting the data retained to the data that is necessary to accomplish the mission.
    a) Data minimization aligns with many pragmatic concerns.
        i) Excess surveillance capacity does not produce good value-for-money due to the cost of standing up and operating systems, and the cost of data storage.

ii) Excess surveillance capacity may increase the chance of improper activity by system operators. More cameras and more operators mean more chances for all types of complications.
iii) Given the bandwidth of video feeds, long term data storage can be costly, especially when useless data is retained.

(2) Data collection should be time, geographically, and technically limited to accomplish only the system's stated goals.
a) The duration that a system operates should be no longer than reasonably necessary to achieve its articulated purpose.
i) Permanent systems should be created only to address threats to public safety that are of indefinite duration.
(1) Example: CCTV system monitoring vulnerable approaches to a liquid propane gas terminal.
ii) Agencies should evaluate camera systems annually (including efficacy studies), and determine if they are still necessary.
iii) Flexible installation of cameras, permitting ready removal and reinstallation elsewhere as required, may be a cost effective way of achieving law enforcement and security goals, while limiting the amount of irrelevant data collected.
iv) Data retention and disposal policies should be decided ahead of time.
(1) Images and footage should not be permanently retained, unless there is a purpose to the retention, such as use in an ongoing investigation of specific persons or activities, or availability for court testimony in a proceeding.
(2) Retained data can be subpoenaed by outside civil litigators, for example, in divorce cases.
(3) Communities might not be receptive to CCTV programs that create a permanent record of the activities of innocent people in areas under surveillance.
(4) Data retention can still be expensive, even though costs are going down.
b) CCTV systems should be limited in geographic scope, serving as extra eyes in problem areas (*e.g.*, with law enforcement or security problems) and looking only at areas where it is permissible and non-oppressive for law enforcement officers and security personnel to look.
i) Thus far, studies indicate that CCTV systems work best when targeting specific areas that have specific problems. Cameras may create a "squish zone," moving crime off one street and into an alley, or onto the next street. Coupled with other law enforcement strategies, this may be useful. In contrast, surveilling an area of little law enforcement or security concern is without purpose, resulting in the accumulation of useless data and the unnecessary expenditure of funds.
ii) Use only enough cameras to accomplish the intended purpose.
iii) Only focus cameras on those structures or areas that require law enforcement or security scrutiny, and where observation will fit into the overall law enforcement or security strategy.
(1) Example: Surveillance of a public park may be a reasonable use, but the cameras overlooking the park should not also be able to look into the windows of an adjacent apartment building.
(2) Example: An optical camera with very high magnification provides generally observation capability in observes a public square, but it may also beis capable of

reading what an individual at an outdoor café table some distance away is writing on a note pad.

c) CCTV systems should be limited in the types of technology employed to those types of technology necessary to accomplish the goals of the system.
   i) Example: A traffic monitoring CCTV system should probably not be designed with facial recognition analysis in mind.
   ii) Example: A camera in a public space combined with audio feed for detecting gunshots should not be used to eavesdrop on conversations of passersby.
   iii) Example: If simple, visual observation of a public area like a plaza is the goal, the system should not include technology to capture and record conversations of individuals within the vicinity.
   iv) Example: Consider whether cameras should be fitted with technology that permits the ability to look through clothes or into containers in a public space.
   v) Using sensors rather than cameras can limit the amount of data collected and the impact on privacy.
      (1) Example: Law enforcement wants to partner with an oil refinery to secure a large, fairly desolate area around the plant. Instead of having dozens of cameras covering every approach at all time, several more powerful pan-tilt-zoom cameras are installed on elevated poles, which are automatically triggered to focus on a particular area when a motion sensor is triggered.
      (2) Example: A large city has problems with gun violence. Rather than installing hundreds of cameras, sensitive audio sensors calibrated to detect gunshots can be installed to alert patrol units to the location of gunfire.
      (3) Consider the privacy and civil liberties impact of installing audio sensors. Be sure that audio monitoring devices sensitive enough to detect gunshots at great distance are not used for eavesdropping.

d) To limit geographic and technical scope of CCTV systems, consider the following safeguards:
   i) Fixed camera installation can prevent the camera from being re-targeted into private areas.
   ii) Physical "blinders" can be installed to reduce the camera's field of vision to prevent cameras from being panned, tilted, or zoomed into private areas that raise no law enforcement or security concern.
   iii) Software "blur" spots can permit pan, tilt, and zoom operation, but render privacy areas too blurry for a viewer to interpret. Technical capability to unmask the blurring may be considered necessary to assist in a specific law enforcement investigation.

e) Consider emergency uses in CCTV design and build in enough flexibility to deal with such situations.
   i) Example: A pan/tilt/zoom (PTZ) camera that routinely monitors a public square surrounded by housing may need to be refocused on private housing to follow an armed robber who has fled. Such cameras can be software limited to an ordinary sweep, but permit an operator to log in and view areas that would ordinarily not be examined. The log in would leave an audit trail, that would discourage impermissible uses and cause the operator to consider whether the planned camera use is permissible.

(3) Legal considerations such as state privacy laws and the U.S. Constitution will also counsel data minimization.

a) Example: Political demonstrators hold a peaceful demonstration in a public square observed by CCTV. The demonstration is uneventful. Whether it amounts to a violation of the First Amendment is unclear, but retaining footage or images of the event could have a chilling effect on the exercise of First Amendment rights, and should be avoided if possible. Such retention, as discussed above, may also be a waste of money and system resources.

Use Limitation Principle

Each government agency should use CCTV solely for the purpose(s) specified in the notice given to the public. Disclosing camera footage or images outside the agency should only be pursuant to a written policy and for a valid public safety or law enforcement purpose.

(1) As a general matter, limit data sharing to those individuals and agencies with a legitimate need-to-know. More specifically, limit the number of individuals with access, the type and quantity of data shared, and the time that those individuals are permitted to retain the data.
(2) Using camera footage or images for a purpose other than those stated in the public policy for the system, should only be done under special process to safeguard against abuse. Additional safeguards regarding secondary uses could include obtaining written authorization from a senior agency or law enforcement official or seeking permission from a local magistrate where constitutional or other individual rights questions arise.
   a) Example: Assume a CCTV system includes audio monitoring for the purposes of gunshot detection, which passively monitors loud sounds and uses a vectoring process, similar to sonar, to determine where gunshots occurred. Generally, no monitoring of conversations or other noise by law enforcement occurs since the monitors are automated and tuned to detect gunshots. However, if law enforcement officers wish to eavesdrop on a meeting of two criminal conspirators scheduled for a public place under CCTV observation and request that the audio feed from the sensitive gunshot monitors be made available to them, state law may require the law enforcement officers to seek a warrant, and it may also be prudent under Federal Constitutional law to seek a warrant based on probable cause.
   b) Example: Assume that a camera system with the stated purpose of monitoring a public plaza will sweep or be aimed toward a nearby park where a potentially violent political demonstration will occur. Because the use is planned and outside of the stated uses of the system, and additionally because significant individual rights issues are implicated, such use should require a senior law enforcement officer authorization.
   c) No additional approval should be required for incidental use of a system.
      i) Example: A system installed for crime control purposes should be available for use in assisting fire and rescue personnel in responding to a building fire or a plane crash. Similarly, exigent circumstances, such as monitoring fleeing suspects, should be permissible, subject to reasonable oversight measures.
      ii) The types of incidental uses of the system that are permissible should be made clear to operators in training and in written policies.
      iii) Data obtained during incidental/exigent use of the camera system should be reviewed by supervisors as soon as practical after the incidental use to determine if the data should be retained or purged.

d) Secondary use of archived and "pre-archival" stored video footage or images should require the administrative approval of senior personnel.
    i) Example: The police academy wishes to use crowd shots in training as background footage, or to illustrate some point relating to law enforcement technique, such as conducting an arrest. Whether such secondary uses would be permissible is a decision that should be reserved to accountable, senior decision-makers.

(3) Release of footage or images should only occur upon written request through a designated chain of command, acting in accordance with relevant privacy laws.
(4) Operators should not be able to make copies of footage or images without supervisor authorization.
(5) Private-sector footage or images should be treated as if they had been recorded initially on a government-run camera once they come into government hands. For privacy and data integrity purposes, the footage or images should be considered government footage or images once they are in government hands.
(6) There is generally no legal expectation of privacy in things in plain view; but if a yard is fenced off, or window curtains are drawn, and technical surveillance is capable of breaching those privacy measures, probable cause or a warrant may be required.
    i) Certain "public" areas require special attention from legal counsel since individuals may have an expectation of privacy in those areas - consider changing rooms at a public pool or gym, and restrooms.

Data Quality and Integrity Principle

Each government agency should, to the extent practical, ensure that the camera footage or images are accurate, relevant, timely, and complete, within the context of its use.

(1) Safeguard and authenticate the stored camera data using appropriate physical, personnel, and technical security measures. Consider using digital watermarks, encryption, or other security and authentication techniques to secure the data.
(2) Consider how the system design may be used to authenticate and establish chain-of-custody for data that will potentially be used as evidence.
(3) Establish a data retention policy that requires the purging of recorded footage or images that lack evidentiary value or other value for a stated purpose of the system.
(4) Provide for procedures (a) to identify and secure data that should be retained as evidence or for other stated purposes;, (b) to conductfor regularly scheduled review of all retained data;, and (c) for the routine destruction/purging of data that does not have to be retained.
(5) Determine ahead of time how requests for stored data potentially related to third-party litigation will be handled. While agencies must comply with specific subpoena and court orders, there is no objection to having a data storage policy that routinely eliminates stored data after its operational (law enforcement or security) usefulness has ended.

Security Principle

Each government agency should protect the CCTV system through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

(1) Security measures should be layered. The agency should not rely on one particular security measure to safeguard data but should employ several measures that functionally overlap to ensure the security of data and the overall CCTV system.
(2) Network security is critical, particularly for wireless systems.
(3) Other security measures include: physical security of the network and of any viewing and data storage centers; personnel security ensuring those who have access to the system are appropriately vetted; and other security measures as appropriate.
(4) Implement information security practices and safeguards to enforce all privacy policies. Use technology, such as encryption and access controls, to ensure that the system is only used as authorized and that the camera footage and images are protected against unauthorized use.
(5) Ensure that those who have access to the system are appropriately trained to maintain the data. Training should be provided for all levels of system operations, from technical personnel to administrator and oversight personnel.
    a) Training should address Constitutional issues, case law, search and seizure regulations, state and local legislation, ethical considerations, and departmental policy.
    b) Training should occur prior to assignment to operate a CCTV system and include refresher training at least yearly to reinforce the importance of acceptable behavior.
    c) The importance of proper training and regular refresher training should be highlighted when potential liability issues are considered. Liability may arise under state privacy or tort law if information is mishandled or misused, and prosecutions and security efforts may be undermined by data corruption or mishandling.
(6) Oversight of system operators to ensure compliance with policies and good practices may act as another layer of security and may serve to improve system function and reduce potential agency liability, even as it ensures the integrity and utility of the CCTV system.

Accountability and Auditing Principle

Each government agency should be accountable for complying with these principles, providing training to all employees and contractors who use the CCTV system, and auditing the actual use of the CCTV system to demonstrate compliance with these principles and all applicable privacy protection requirements.

(1) Provide adequate supervision at all times when the CCTV system is operational to reduce the risk of misuse or abuse.
(2) Establish a control log that documents the names and hours of personnel working each shift; names, times and purpose of entry into the CCTV center by non-assigned personnel; all requests for footage or images; and any noteworthy incidents. To some extent this may be done in automated fashion by the measures suggested in item 3, below.
(3) Use automated operator logon, access control, and other standard audit features to ensure a clear audit trail is maintained. This enables tracking of abusive use of CCTV assets back to the individual who violated a policy.
(4) Implement appropriate encryption, watermarking, and other chair-of-custody processes to ensure that camera footage and images are appropriately handled.
(5) Conduct periodic audits of the system to ensure that all policies are adhered to. Preferably, professional boards or outside government agencies should conduct independent audits.

(6) Provide sanctions against misuse and abuse of CCTV systems, as well as remedies for people who may be harmed by those types of abuse and misuse. Create technological and administrative safeguards, such as digital masking of people whose images are incidentally captured, but who are not the actual criminal suspects.
(7) Define consequences for misuse or abuses of the system as part of the written policy and ensure that all users receive training regarding these consequences.
(8) A useful oversight measure, and one that can help build community trust in the law enforcement agency and in the CCTV system, is to permit public inspection of the CCTV operations center/viewing room at any reasonably appropriate (*e.g.*, non-crisis) time.

APPENDIX C

Template

Privacy Impact Assessment for the Use of CCTV

By

DHS Programs

Overview

The overview should include:

- The system or program's technical and commonly referred-to name and the Department of Homeland Security (DHS) Component and program responsible for its implementation and oversight.
- The name of the Federal, state, local, or other entities that operate, oversee, or have access to the system and program
- The objective of the program and how it relates to the mission of the program and DHS.
- A general description of the technology, the system, and the program.
    - Technology: for example, a description of the camera and recording technologies, with model numbers, vendors, and functions.
    - System: for example, a description of the network of surveillance devices—where and how they are installed, the number of devices, the system for collecting and, if applicable, monitoring the visual information.
    - Program: for example, a description of the law enforcement program that oversees or uses the surveillance technology – its development, funding, purpose, and limitations.

A clear and concise overview provides the reader the context in which to view the remainder of the PIA.

<< ADD Overview Here >>

Section 1.0 The System and the Information Collected and Stored Within the System

The following questions are intended to define the scope of the information collected, as well as the reasons for its collection as part of the program being developed. The term "information" includes all images and footage captured by the camera system and any information associated with those images that can be linked to individuals. If the images are viewed but not stored, please indicate that process below.

1.1 What information is to be collected?

(Please check the following if applicable)
The System's technology enables it to record:

☐ Video
    Static Range:
    Zoom Range:
    Pan from one angle to another:
☐ Tracking
    ☐ Automatic (for example, triggered by certain movements, indicators)
    ☐ Manual (controlled by a human operator)
☐ Sound
    Frequency Range:

Provide a description of what the camera is intended to view.
<<ADD Answer Here>>

The System typically records:

- ☐ Passersby on public streets.
- ☐ Textual information (such as license plate numbers, street and business names, or text written on recorded persons' belongings).
- ☐ Images not ordinarily available to a police officer on the street:
  - ☐ Inside commercial buildings, private homes, etc.
  - ☐ Above the ground floor of buildings, private homes, etc.

☐ The System does not record or store the images.

Sample screenshots of a typical recording may be a helpful item to include in an appendix to the PIA.

1.1.1 If the activity or program seeks any specific information or types of information, please specify what is being sought.

<< ADD Answer Here>>

1.1.2 Is the information obtained from the CCTV monitoring combined with any other information; and if so, please describe the other information.

<<ADD Answer Here>>

1.2 From whom is the information collected?

- ☐ General public in the monitored areas.
- ☐ Targeted populations, areas, or activities (please describe).
- ☐ Program personnel are directed to focus on particular people, activities, or places.

1.2.1 Describe any training, guidance, or policies given to program personnel that direct them to focus on particular people, activities, or places.

<< ADD Answer Here >>

1.3 Why is the information being collected? Identify all that apply.

- ☐ For traffic-control purposes
- ☐ Crime prevention
- ☐ Crime detection
- ☐ To aid in criminal prosecution
- ☐ Threat identification
- ☐ Terrorism investigation
- ☐ Terrorism prevention

☐ Other (please specify)

1.3.1 Policy Rationale

Provide a brief description stating why cameras are necessary to the program and to the governmental entity's mission. Description may address one or more of the following:

- ☐ Crime prevention rationale: (For example: (1) Crimes in-progress may only be prevented if the cameras are monitored in real-time. (2) A clearly visible camera alerting the public that they are monitored may deter criminal activity, at least in the monitored area.)
- ☐ Crime investigation rationale: (For example: A hidden camera may be investigative, providing after-the-fact records of persons and locations that may be subpoenaed.)
- ☐ Terrorism rationale: (For example: Video footage is collected to compare against information contained in terrorist databases.)

1.3.2 Detail why the particular cameras, their specific placement, the exact monitoring system and its technological features were selected to advance the program's mission. For example, describe how low-light technology was selected to combat illegal border crossing at night. It is not sufficient to merely state the general purpose of the system.

<< ADD Answer Here >>

1.3.3 Are you using the cameras to track and/or to identify individuals?

<<ADD Answer Here>>

1.4 How is the information collected?

- ☐ Real-time monitoring, with footage streamed, but not stored.
- ☐ Real-time monitoring with footage stored.
- ☐ Footage not monitored, only stored.

1.5 Operating Policies and Procedure

Describe the policies governing how the records can be deleted, altered or enhanced, either before or after storage. Are there access control policies limiting who can see and use the video images and for what purposes? Are there auditing mechanisms to monitor who accesses the records, and to track their uses, and if so, are these mechanisms a permanent and unalterable part of the entire system? What training was conducted for officials monitoring or accessing the technology?

<< ADD Answer Here >>

1.6 Effectiveness

Describe how the program will evaluate the camera system's performance. Are there specific metrics established for evaluation? Is there a specific timeline for evaluation?

<< ADD Answer Here >>

1.7 Cost Comparison

Has the program done a cost comparison of the camera system to alternative means of addressing the system's purposes that may have less of an impact on privacy? If so, provide a summary of such cost comparison. (For example, compare the cost of the camera system to adding law enforcement personnel to patrol the area.)

<< ADD Answer Here >>

1.8 What specific legal authorities, arrangements, and/or agreements govern the camera system?

The section should include a description of the legislative authorization of DHS, as well as any executive or law enforcement decision authorizing the system. In addition, provide a list of the limitations or regulations controlling the use of the camera system. This may include existing law enforcement standards, such as subpoenas and warrants, or surveillance-specific rules. For example, is a warrant required for tracking or identifying an individual?

<< ADD Answer Here >>

1.9 The Decision Making Process

Describe the decision making process that led to the purchase of the camera system.

- ☐ Decision-making process included public comment or review
- ☐ The Program making the decision relied on:
  - ☐ case studies
  - ☐ research
  - ☐ hearings
  - ☐ recommendations from camera vendors
  - ☐ information from other localities
  - ☐ other (please specify)

<< ADD Answer Here >>

1.10 Privacy Impact Analysis

Given the amount and type of data collected, and the system's structure, purpose and use, discuss what privacy risks were identified and how they were mitigated. If during the system design or technology selection process, decisions were made to limit the scope of surveillance or increase accountability, include a discussion of this decision.
Relevant privacy risks you can discuss include:

- **Privacy rights**. For example, cameras can capture individuals entering places or engaging in activities where they do not expect to be identified or tracked. Such situations may include entering a doctor's office, or an Alcoholics Anonymous, social, political, or religious meeting.
- **Freedom of speech and association**. Cameras may give the government records of what individuals say, do, and read in the public arena, for example documenting the individuals at a particular rally or associations between individuals. Such recording may chill constitutionally-protected expression and association.

- **Government accountability and procedural safeguards**. While the expectation is that law enforcement and other authorized personnel will use the technology legitimately, the program design should anticipate and safeguard against unauthorized uses, including creating a system of accountability for all uses.
- **Equal protection and discrimination**. Government surveillance, because it makes some policing activities invisible to the public, poses heightened risks of misuse, such as profiling by race, citizenship status, gender, age, socioeconomic level, sexual orientation, or otherwise. Decisions about camera placement, and dynamic decisions about camera operation, should be the product of rationale, non-discriminatory processes and inputs. System decisions should be scrutinized with fairness and non-discrimination concerns in mind.

  << ADD Answer Here >>

Section 2.0 – Uses of the System and Information

2.1 Describe uses of the footage or images derived from the cameras.

Please describe in detail how the footage or images are used, as well as how the footage or images may be used in the future.

<< ADD Answer Here >>

2.2 Privacy Impact Analysis

Describe any types of controls that are in place to ensure that the footage or images is handled in accordance with the above described uses. For example, is appropriate use of the information covered in training for all users of the system? Are audit logs regularly reviewed? What disciplinary programs are in place if an individual is found to be inappropriately using the technology or records?

<< ADD Answer Here >>

Section 3.0 – Retention

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What is the retention period for the information in the system (i.e., how long are footage or images stored)?

- ☐ 24-72 hours
- ☐ 72 hours – 1 week
- ☐ 1 week – 1 month
- ☐ 1 month – 3 months
- ☐ 3 months – 6 months
- ☐ 6 months – 1 year
- ☐ more than 1 year (please describe)

☐ indefinitely

3.1.1 Describe any exemptions for the retention period (i.e. Part of an investigation or review)

<< ADD Answer Here >>

3.2 Retention Procedure

☐ Footage or images are automatically deleted after the retention period expires
☐ System operator required to initiate deletion
☐ Under certain circumstances, officials may override detention period:
  ☐ To delete the footage or images before the detention period
  ☐ To retain the footage or images after the detention period
  ☐ Please describe the circumstances and official process for override

3.3 Privacy Impact Analysis:

Considering the purpose for retaining the information, explain why the information is maintained for the designated period.

<< ADD Answer Here >>

Section 4.0 – Internal Sharing and Disclosure

The following questions are intended to describe the scope of sharing *within* the program's operation, for example, sharing with various units or divisions within the Component or DHS. *External sharing with outside entities will be addressed in the next section.*

4.1 With what internal entities and types of personnel will the information be shared?

Internal Entities
☐ Investigations unit
☐ Auditing unit
☐ Financial unit
☐ DHS enforcement unit
☐ Other (please specify)
☐ None

Types of Personnel
☐ Command staff (please specify which positions)
☐ Middle management (please specify)
☐ Entry-level employees
☐ Other (please specify)

4.2 For the internal entities listed above, what is the extent of the access each receives (i.e. what records or technology is available to them, and for what purpose)?

<< ADD Answer Here >>

4.2.1 Is there a written policy governing how access is granted?

- ☐ Yes (please detail)
- ☐ No

4.2.2 Is the grant of access specifically authorized by:

- ☐ Statute (please specify which statute)
- ☐ Regulation (please specify which regulation)
- ☐ Other (please describe)
- ☐ None

4.3 How is the information shared?

4.3.1 Can personnel with access obtain the information:

- ☐ Off-site, from a remote server
- ☐ Via copies of the video distributed to those who need it
- ☐ Only by viewing the video on-site
- ☐ Other (please specify)

4.4 Privacy Impact Analysis:

Considering the extent of internal information sharing, discuss what privacy risks were identified and how they were mitigated. For example, discuss any access controls, encryption, training, regulations, or disciplinary procedures that will ensure only legitimate uses of the system within the department.

<< ADD Answer Here >>

Section 5.0 – External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to your operation – including other Federal agencies, State and Local Government, as well as private entities and individuals.

5.1 With which external entities is the information shared?

List the name(s) of the external entities with whom the footage or images and related information will be shared. The term "external entities" refers to individuals or groups outside your organization.

- ☐ Local government agencies (please specify)
- ☐ State government agencies (please specify)
- ☐ Federal government agencies (please specify)

- ☐ Private entities:
  - ☐ Businesses in monitored areas
  - ☐ Insurance companies
  - ☐ News outlets
  - ☐ Other (please specify)
- ☐ Individuals:
  - ☐ Crime victims
  - ☐ Criminal defendants
  - ☐ Civil litigants
  - ☐ General public via Public Records Act or Freedom of Information Act requests
  - ☐ Other (please specify)

5.2 What information is shared and for what purpose?

5.2.1 For each entity or individual listed above, please describe all of the following:

- ☐ The purpose for disclosure
- ☐ The rules and regulations governing disclosure
- ☐ Conditions under which information will not be disclosed
- ☐ Citations to any specific authority authorizing sharing of the camera footage or images

5.3 How is the information transmitted or disclosed to external entities?

- ☐ Discrete portions of camera footage or images are shared on a case-by-case basis
- ☐ Certain external entities have direct access to camera footage or images
- ☐ Real-time feeds of footage or images between agencies or departments
- ☐ Footage or images are transmitted wirelessly or downloaded from a server
- ☐ Footage or images are transmitted via hard copy
- ☐ Footage or images may only be accessed on-site

5.4 Is a Memorandum of Understanding (MOU), contract, or agreement in place with each external organization with whom information is shared, and does the MOU reflect the scope of the information currently shared?

- ☐ Yes
- ☐ No

If an MOU is not in place, explain steps taken to address this omission.

5.5 How is the shared information secured by the recipient?

For each interface with a system outside your operation:

☐ There is a written policy defining how security is to be maintained during the information sharing
☐ One person is in charge of ensuring the system remains secure during the information sharing (please specify)
☐ The external entity has the right to further disclose the information to other entities
☐ The external entity does not have the right to further disclose the information to other entities
☐ Technological protections such as blocking, face-blurring or access tracking remain intact one information is shared
☐ Technological protections do not remain intact once information is shared

5.6 Privacy Impact Analysis:

Given the external sharing, what privacy risks were identified? Describe how they were mitigated. For example, if a sharing agreement is in place, what safeguards (including training, access control or assurance of technological privacy protection) have been implemented to ensure information is used appropriately by agents outside your program/component?

<< ADD Answer Here >>

Section 6. 0 – Technical Access and Security

6.1 Who will be able to delete, alter or enhance records either before or after storage?

☐ Program leadership
☐ Operation personnel
☐ Persons outside the program who will have routine or ongoing access to the system (please specify)
☐ Other (please specify)

6.1.1 Are different levels of access granted according to the position of the user? If so, please describe.

☐ All authorized users have access to real-time footage or images
☐ Only certain authorized users have access to real-time footage or images (please specify which users)
☐ All authorized users have access to stored footage or images
☐ Only certain users have access to stored footage or images (please specify which users)
☐ All authorized users can control the camera functions (pan, tilt, zoom)
☐ Only certain authorized users can control the camera functions
☐ All authorized users can delete or modify footage or images

☐ Only certain authorized users can delete or modify footage or images (please specify which users)

6.1.2 Are there written procedures for granting access to users for the first time?

☐ Yes (please specify)
☐ No

6.1.3 When access is granted:

☐ There are ways to limit access to the relevant records or technology (please specify)
☐ There are no ways to limit access

6.1.4 Are there auditing mechanisms:

☐ To monitor who accesses the records?
☐ To track their uses?

6.1.5 Training received by prospective users includes discussion of:

☐ Liability issues
☐ Privacy issues
☐ Technical aspects of the system
☐ Limits on system uses
☐ Disciplinary procedures
☐ Other (specify)
☐ No training

The training lasts:

☐ None
☐ 0-1 hours
☐ 1-5 hours
☐ 5-10 hours
☐ 10-40 hours
☐ 40-80 hours
☐ More than 80 hours

The training consists of:

☐ A course
☐ A video
☐ Written materials
☐ Written materials, but no verbal instruction
☐ None
☐ Other (please specify)

6.2 The system is audited:

- ☐ When an employee with access leaves the organization
- ☐ If an employee is disciplined for improper use of the system
- ☐ Once a week
- ☐ Once a month
- ☐ Once a year
- ☐ Never
- ☐ When called for

6.2.1 System auditing is:

- ☐ Performed by someone within the organization
- ☐ Performed by someone outside the organization
- ☐ Overseen by an outside body (for example a city council or other elected body – please specify)

6.3 Privacy Impact Analysis:

Given the sensitivity and scope of information collected, what privacy risks related to security were identified and mitigated?

<< ADD Answer Here >>

Section 7.0 – Notice

7.1 Is notice provided to potential subjects of camera recording that they are within view of a camera?

- ☐ Signs posted in public areas inform the public of recording by cameras
- ☐ Signs in multiple languages
- ☐ Attached is a copy of the wording of such notice signs
- ☐ Notice is not provided
- ☐ Other (please describe)

Section 8.0 – Technology

The following questions are directed at analyzing the selection process for any technologies used by the camera system, including cameras, lenses, and recording and storage equipment.

8.1 Were competing technologies evaluated to compare their ability to achieve system goals, including privacy protection?

- ☐ Yes
- ☐ No

8.2 What design choices were made to enhance privacy?

- ☐ The system includes face-blurring technology
- ☐ The system includes blocking technology

☐ The system limited location to address privacy
☐ The system has other privacy-enhancing technology (Please specify)
☐ None (Please specify)

Section 9.0 – Attachments to the PIA

☐ Authorizing legislation
☐ Grant documents
☐ Transcript of public hearing or legislative session
☐ Press release announcing the CCTV program
☐ Program manuals outlining the system's rules and regulations
☐ Other (please specify)

Responsible Officials

<< ADD Privacy Officer/Project Manager>>

Approval Signature

_____

Chief Privacy Officer
Department of Homeland Security

APPENDIX D

Template

Privacy Impact Assessment for the Use of CCTV

By

State and Local Entities

Overview

The overview should include:

- The system or program's technical and commonly referred-to name and the organization responsible for its implementation and oversight.
- The name of the Federal, state, local, or other entities that operate, oversee, or have access to the system and program
- The objective of the program and how it relates to the governmental entity's mission
- A general description of the technology, the system, and the program.
    - Technology: for example, a description of the camera and recording technologies, with model numbers, vendors, and functions.
    - System: for example, a description of the network of surveillance devices—where and how they are installed, the number of devices, the system for collecting and, if applicable, monitoring the visual information.
    - Program: for example, a description of the law enforcement program that oversees or uses the surveillance technology – its development, funding, purpose, and limitations.

A clear and concise overview provides the reader the context in which to view the remainder of the PIA.

<< ADD Overview Here >>

Section 1.0 The System and the Information Collected and Stored Within the System

The following questions are intended to define the scope of the information collected, as well as the reasons for its collection as part of the program being developed. The term "information" includes all images and footage captured by the camera system and any information associated with those images that can be linked to individuals. If the images are viewed but not stored, please indicate that process below.

1.1 What information is to be collected?

(Please check the following if applicable)
The System's technology enables it to record:

☐ Video
    Static Range:
    Zoom Range:
    Pan from one angle to another:
☐ Tracking
    ☐ Automatic (for example, triggered by certain movements, indicators)
    ☐ Manual (controlled by a human operator)
☐ Sound
    Frequency Range:

Provide a description of what the camera is intended to view.

<<ADD Answer Here>>

The System typically records:

- ☐ Textual information (such as license plate numbers, street and business names, or text written on recorded persons' belongings).
- ☐ Images not ordinarily available to a police officer on the street:
  - ☐ Inside commercial buildings, private homes, etc.
  - ☐ Above the ground floor of buildings, private homes, etc.

☐ The System does not record or store the images.

Sample screenshots of a typical recording may be a helpful item to include in an appendix to the PIA.

1.1.1 If the activity or program seeks any specific information or types of information, please specify what is being sought.

<< ADD Answer Here>>

1.1.2 Is the information obtained from the CCTV monitoring combined with any other information; and if so, please describe the other information.

<<ADD Answer Here>>

1.2 From whom is the information collected?

- ☐ General public in the monitored areas.
- ☐ Targeted populations, areas, or activities (please describe).
- ☐ Program personnel are directed to focus on particular people, activities, or places.

1.2.1 Describe any training, guidance, or policies given to program personnel that direct them to focus on particular people, activities, or places.

<< ADD Answer Here >>

1.3 Why is the information being collected? Identify all that apply.

- ☐ For traffic-control purposes
- ☐ Crime prevention
- ☐ Crime detection
- ☐ To aid in criminal prosecution
- ☐ Threat identification
- ☐ Terrorism investigation
- ☐ Terrorism prevention
- ☐ Other (please specify)

1.3.1 Policy Rationale

Provide a brief description stating why cameras are necessary to the program and to the governmental entity's mission. Description may address one or more of the following:

- ☐ Crime prevention rationale: (For example: (1) Crimes in-progress may only be prevented if the cameras are monitored in real-time. (2) A clearly visible camera alerting the public that they are monitored may deter criminal activity, at least in the monitored area.)
- ☐ Crime investigation rationale: (For example: A hidden camera may be investigative, providing after-the-fact records of persons and locations that may be subpoenaed.)
- ☐ Terrorism rationale: (For example: Video footage is collected to compare against information contained in terrorist databases.)

1.3.2 Detail why the particular cameras, their specific placement, the exact monitoring system and its technological features were selected to advance the governmental entity's mission. For example, describe how low-light technology was selected to combat crime at night. It is not sufficient to merely state the general purpose of the system.

<< ADD Answer Here >>

1.3.3 Are you using the cameras to track and/or to identify individuals?

<<ADD Answer Here>>

1.4 How is the information collected?

- ☐ Real-time monitoring, with footage streamed, but not stored.
- ☐ Real-time monitoring with footage stored.
- ☐ Footage not monitored, only stored.

1.5 Operating Policies and Procedure

Describe the policies governing how the records can be deleted, altered or enhanced, either before or after storage. Are there access control policies limiting who can see and use the video images and for what purposes? Are there auditing mechanisms to monitor who accesses the records, and to track their uses, and if so, are these mechanisms a permanent and unalterable part of the entire system? What training was conducted for officials monitoring or accessing the technology?

<< ADD Answer Here >>

1.6 Effectiveness

Describe how the governmental entity will evaluate the camera system's performance. Are there specific metrics established for evaluation? Is there a specific timeline for evaluation?

<< ADD Answer Here >>

1.7 Cost Comparison

Has the governmental entity done a cost comparison of the camera system to alternative means of addressing the system's purposes that may have less of an impact on privacy? If so, provide a summary of such cost comparison. (For example, compare the cost of the camera system to adding law enforcement personnel to patrol the area.)

<< ADD Answer Here >>

1.8 What specific legal authorities, arrangements, and/or agreements govern the camera system?

The section should include a description of the legislative authorization at the Federal, State, and/or local level, as well as any executive or law enforcement decision authorizing the system. In addition, provide a list of the limitations or regulations controlling the use of the camera system. This may include existing law enforcement standards, such as subpoenas and warrants, or surveillance-specific rules. For example, is a warrant required for tracking or identifying an individual?

<< ADD Answer Here >>

1.9 The Decision Making Process

Describe the decision making process that led to the purchase of the camera system.

- ☐ Decision-making process included public comment or review
- ☐ Entity making the decision relied on:
  - ☐ case studies
  - ☐ research
  - ☐ hearings
  - ☐ recommendations from camera vendors
  - ☐ information from other localities
  - ☐ other (please specify)

<< ADD Answer Here >>

1.10 The Funding

- ☐ DHS Grant
- ☐ General revenues
- ☐ Law enforcement budget
- ☐ Other (please specify)
- ☐ Funding has limited duration (please specify)
- ☐ Funding renewal is contingent on program evaluation

<< ADD Answer Here >>

1.11 Privacy Impact Analysis

Given the amount and type of data collected, and the system's structure, purpose and use, discuss what privacy risks were identified and how they were mitigated. If during the system design or

technology selection process, decisions were made to limit the scope of surveillance or increase accountability, include a discussion of this decision.
Relevant privacy risks you can discuss include:

- **Privacy rights**. For example, cameras can capture individuals entering places or engaging in activities where they do not expect to be identified or tracked. Such situations may include entering a doctor's office, or an Alcoholics Anonymous, social, political, or religious meeting.
- **Freedom of speech and association**. Cameras may give the government records of what individuals say, do, and read in the public arena, for example documenting the individuals at a particular rally or associations between individuals. Such recording may chill constitutionally-protected expression and association.
- **Government accountability and procedural safeguards**. While the expectation is that law enforcement and other authorized personnel will use the technology legitimately, the program design should anticipate and safeguard against unauthorized uses, including creating a system of accountability for all uses.
- **Equal protection and discrimination**. Government surveillance, because it makes some policing activities invisible to the public, poses heightened risks of misuse, such as profiling by race, citizenship status, gender, age, socioeconomic level, sexual orientation, or otherwise. Decisions about camera placement, and dynamic decisions about camera operation, should be the product of rationale, non-discriminatory processes and inputs. System decisions should be scrutinized with fairness and non-discrimination concerns in mind.

  << ADD Answer Here >>

Section 2.0 – Uses of the System and Information

2.1 Describe uses of the footage or images derived from the cameras.

Please describe in detail how the footage or images are used, as well as how the footage or images may be used in the future.

<< ADD Answer Here >>

2.2 Privacy Impact Analysis

Describe any types of controls that are in place to ensure that the footage or images is handled in accordance with the above described uses. For example, is appropriate use of the information covered in training for all users of the system? Are audit logs regularly reviewed? What disciplinary programs are in place if an individual is found to be inappropriately using the technology or records?

<< ADD Answer Here >>

Section 3.0 – Retention

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What is the retention period for the information in the system (i.e., how long are footage or images stored)?

- ☐ 24-72 hours
- ☐ 72 hours – 1 week
- ☐ 1 week – 1 month
- ☐ 1 month – 3 months
- ☐ 3 months – 6 months
- ☐ 6 months – 1 year
- ☐ more than 1 year (please describe)
- ☐ indefinitely

3.1.1 Describe any exemptions for the retention period (i.e. Part of an investigation or review)

<< ADD Answer Here >>

3.2 Retention Procedure

- ☐ Footage or images are automatically deleted after the retention period expires
- ☐ System operator required to initiate deletion
- ☐ Under certain circumstances, officials may override detention period:
  - ☐ To delete the footage or images before the detention period
  - ☐ To retain the footage or images after the detention period
  - ☐ Please describe the circumstances and official process for override

3.3 Privacy Impact Analysis:

Considering the purpose for retaining the information, explain why the information is maintained for the designated period.

<< ADD Answer Here >>

Section 4.0 – Internal Sharing and Disclosure

The following questions are intended to describe the scope of sharing *within* the program's operation, for example, sharing with various units or divisions within the police department in charge of the camera system. *External sharing with outside entities will be addressed in the next section.*

4.1 With what internal entities and types of personnel will the information be shared?

Internal Entities

- ☐ Investigations unit
- ☐ Auditing unit
- ☐ Financial unit
- ☐ Property-crimes unit
- ☐ Street patrols

☐ Command unit
☐ Other (please specify)
☐ None

Types of Personnel
☐ Command staff (please specify which positions)
☐ Middle management (please specify)
☐ Entry-level employees
☐ Other (please specify)

4.2 For the internal entities listed above, what is the extent of the access each receives (i.e. what records or technology is available to them, and for what purpose)?

<< ADD Answer Here >>

4.2.1 Is there a written policy governing how access is granted?

☐ Yes (please detail)
☐ No

4.2.2 Is the grant of access specifically authorized by:

☐ Statute (please specify which statute)
☐ Regulation (please specify which regulation)
☐ Other (please describe)
☐ None

4.3 How is the information shared?

4.3.1 Can personnel with access obtain the information:

☐ Off-site, from a remote server
☐ Via copies of the video distributed to those who need it
☐ Only by viewing the video on-site
☐ Other (please specify)

4.4 Privacy Impact Analysis:

Considering the extent of internal information sharing, discuss what privacy risks were identified and how they were mitigated. For example, discuss any access controls, encryption, training, regulations, or disciplinary procedures that will ensure only legitimate uses of the system within the department.

<< ADD Answer Here >>

Section 5.0 – External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to your operation – including Federal, State and Local Government, as well as private entities and individuals.

5.1 With which external entities is the information shared?

List the name(s) of the external entities with whom the footage or images and related information will be shared. The term "external entities" refers to individuals or groups outside your organization.

- ☐ Local government agencies (please specify)
- ☐ State government agencies (please specify)
- ☐ Federal government agencies (please specify)
- ☐ Private entities:
  - ☐ Businesses in monitored areas
  - ☐ Insurance companies
  - ☐ News outlets
  - ☐ Other (please specify)
- ☐ Individuals:
  - ☐ Crime victims
  - ☐ Criminal defendants
  - ☐ Civil litigants
  - ☐ General public via Public Records Act or Freedom of Information Act requests
  - ☐ Other (please specify)

5.2 What information is shared and for what purpose?

5.2.1 For each entity or individual listed above, please describe all of the following:

- ☐ The purpose for disclosure
- ☐ The rules and regulations governing disclosure
- ☐ Conditions under which information will not be disclosed
- ☐ Citations to any specific authority authorizing sharing of the camera footage or images

5.3 How is the information transmitted or disclosed to external entities?

- ☐ Discrete portions of camera footage or images are shared on a case-by-case basis
- ☐ Certain external entities have direct access to camera footage or images
- ☐ Real-time feeds of footage or images between agencies or departments
- ☐ Footage or images are transmitted wirelessly or downloaded from a server
- ☐ Footage or images are transmitted via hard copy
- ☐ Footage or images may only be accessed on-site

5.4 Is a Memorandum of Understanding (MOU), contract, or agreement in place with each external organization with whom information is shared, and does the MOU reflect the scope of the information currently shared?

☐ Yes
☐ No

If an MOU is not in place, explain steps taken to address this omission.

5.5 How is the shared information secured by the recipient?

For each interface with a system outside your operation:

☐ There is a written policy defining how security is to be maintained during the information sharing
☐ One person is in charge of ensuring the system remains secure during the information sharing (please specify)
☐ The external entity has the right to further disclose the information to other entities
☐ The external entity does not have the right to further disclose the information to other entities
☐ Technological protections such as blocking, face-blurring or access tracking remain intact one information is shared
☐ Technological protections do not remain intact once information is shared

5.6 Privacy Impact Analysis:

Given the external sharing, what privacy risks were identified? Describe how they were mitigated. For example, if a sharing agreement is in place, what safeguards (including training, access control or assurance of technological privacy protection) have been implemented to ensure information is used appropriately by agents outside your department/agency?

<< ADD Answer Here >>

Section 6. 0 – Technical Access and Security

6.1 Who will be able to delete, alter or enhance records either before or after storage?

☐ Command staff
☐ Shift commanders
☐ Patrol officers
☐ Persons outside the organization who will have routine or ongoing access to the system (please specify)
☐ Other (please specify)

6.1.1 Are different levels of access granted according to the position of the user? If so, please describe.

- ☐ All authorized users have access to real-time footage or images
- ☐ Only certain authorized users have access to real-time footage or images (please specify which users)
- ☐ All authorized users have access to stored footage or images
- ☐ Only certain users have access to stored footage or images (please specify which users)
- ☐ All authorized users can control the camera functions (pan, tilt, zoom)
- ☐ Only certain authorized users can control the camera functions
- ☐ All authorized users can delete or modify footage or images
- ☐ Only certain authorized users can delete or modify footage or images (please specify which users)

6.1.2 Are there written procedures for granting access to users for the first time?

- ☐ Yes (please specify)
- ☐ No

6.1.3 When access is granted:

- ☐ There are ways to limit access to the relevant records or technology (please specify)
- ☐ There are no ways to limit access

6.1.4 Are there auditing mechanisms:

- ☐ To monitor who accesses the records?
- ☐ To track their uses?

6.1.5 Training received by prospective users includes discussion of:

- ☐ Liability issues
- ☐ Privacy issues
- ☐ Technical aspects of the system
- ☐ Limits on system uses
- ☐ Disciplinary procedures
- ☐ Other (specify)
- ☐ No training

The training lasts:

- ☐ None
- ☐ 0-1 hours
- ☐ 1-5 hours
- ☐ 5-10 hours
- ☐ 10-40 hours

☐ 40-80 hours
☐ More than 80 hours

The training consists of:
☐ A course
☐ A video
☐ Written materials
☐ Written materials, but no verbal instruction
☐ None
☐ Other (please specify)

6.2 The system is audited:

☐ When an employee with access leaves the organization
☐ If an employee is disciplined for improper use of the system
☐ Once a week
☐ Once a month
☐ Once a year
☐ Never
☐ When called for

6.2.1 System auditing is:

☐ Performed by someone within the organization
☐ Performed by someone outside the organization
☐ Overseen by an outside body (for example a city council or other elected body – please specify)

6.3 Privacy Impact Analysis:

Given the sensitivity and scope of information collected, what privacy risks related to security were identified and mitigated?

<< ADD Answer Here >>

Section 7.0 – Notice

7.1 Is notice provided to potential subjects of camera recording that they are within view of a camera?

☐ Signs posted in public areas inform the public of recording by cameras
☐ Signs in multiple languages
☐ Attached is a copy of the wording of such notice signs
☐ Notice is not provided
☐ Other (please describe)

Section 8.0 – Technology

The following questions are directed at analyzing the selection process for any technologies used by the camera system, including cameras, lenses, and recording and storage equipment.

8.1 Were competing technologies evaluated to compare their ability to achieve system goals, including privacy protection?

☐ Yes
☐ No

8.2 What design choices were made to enhance privacy?

☐ The system includes face-blurring technology
☐ The system includes blocking technology
☐ The system limited location to address privacy
☐ The system has other privacy-enhancing technology (Please specify)
☐ None (Please specify)

Section 9.0 – Attachments to the PIA

☐ Authorizing legislation
☐ Grant documents
☐ Transcript of public hearing or legislative session
☐ Press release announcing the CCTV program
☐ Program manuals outlining the system's rules and regulations
☐ Other (please specify)

Responsible Officials

<< ADD Project Manager>>

APPENDIX D

Civil Liberties Impact Assessment
for the

DATE

Contact Point

Reviewing Official

Officer for Civil Rights and Civil Liberties

(202) XXX- XXXX

Introduction

[Include a summary of the program being reviewed. Include a statement of the statutory and/or regulatory authority for this program.]

Potential Civil Liberties Impacts

Impact on Particular Groups or Individuals

1. *Is the program intended to have a direct impact on certain racial or ethnic groups? Even if it is not, might the program have an effect on certain racial or ethnic groups that might reasonably be perceived to be intentional?* If a program singles out one or more racial, ethnic, or national origin groups, *or is intended to do so*, the program must satisfy stringent Constitutional requirements. *See Loving v. Virginia*, 388 U.S. 1 (1967) (strict scrutiny standard of review applies where government action classifies individuals on the basis of race). If the program indirectly or unintentionally impacts upon minorities, the Constitutional standards for evaluating it are much less stringent, *requiring only a lawful, rational basis for the program, but the impact on minorities* should still be considered. *See Washington v. Davis*, 426 U.S. 299 (1976) (applying a rational basis standard of review to government regulation with disparate impact on minorities); *see also Pers. Adminr. v. Feeney*, 442 U.S. 256 (1979) (intentional discrimination, not merely discriminatory effect, is required to trigger heightened review).

2. *Would the program further the Constitutional principle of race-neutral government action, or would it encourage or depend upon a government official categorizing people by race?* Generally, an agency creating a program that singles out one or more racial or ethnic groups must show that it has narrowly tailored its program to further a compelling government interest. When the government treats certain categories of people differently than other categories, it generally must do so according to categories other than race or ethnicity (such as geography or socioeconomic status). *See, e.g., Adarand Const., Inc. v. Pena*, 515 U.S. 200, 235 (1995); *Bolling v. Sharpe*, 347 U.S. 497 (1954).

3. *How would the program affect people with disabilities?* Certain regulatory programs may work a greater hardship on persons with disabilities. If this possibility is anticipated with respect to a particular regulation, we should ask whether this aspect of the proposed rule is justified and whether the hardship can be ameliorated in the implementation of the rule. *Cf.* Rehabilitation Act of 1973, 29 U.S.C. § 794 (prohibiting discrimination on the basis of disability in programs conducted by federal agencies).

4. *How would the program affect those attempting to exercise a particular religion?* Programs identifying particular religious beliefs must be assessed strictly under the First Amendment. Generally-applicable rules that do not refer to any particular religion, but which may have an adverse effect on religious adherents'

exercise of their religion, will be assessed under a less onerous constitutional test, *see Employment Division, Dept. of Human Resources v. Smith*, 494 U.S. 872 (1990), but federal statutes may require a heightened justification for even generally-applicable rules. *See O'Bryan v. Bureau of Prisons*, 349 F.3d 399 (7th Cir. 2003) (discussing applicability of the Religious Freedom Restoration Act , 42 U.S.C. § 2000bb-1, to internal operations of the federal government). *Cf.* Religious Land Use and Institutionalized Persons Act of 2000, 42 U.S.C. § 2000cc *et seq*. (providing protection for the exercise of religion by institutionalized persons). Agencies should consider whether their programs affect the exercise of religion and whether the agency could make reasonable accommodations to avoid a negative effect.

5. *How would the program affect people with limited English language proficiency?* Title VI of the Civil Rights Act of 1964 prohibits discrimination based on national origin by recipients of federal funds. Department of Justice regulations interpret this to mean that these recipients must take reasonable steps to provide persons with limited English proficiency meaningful access to programs and services. Executive Order No. 13,166 requires the executive agencies of the federal government to meet the same standard in their own programs.

Influence of Government

6. *Would the program increase the authority, control, or influence of the federal government in its relationship with private citizens?* Specifically:

   A. *Would the program require or authorize the federal government to collect more information about private citizens?* The collection of data on law-abiding citizens reduces their control over personal information and thereby reduces their liberty. The agency should consider whether it has a sound basis for concluding that collection of the additional information is necessary to effectively carry out an important agency function. If the agency expects that obtaining the information will be beneficial, but cannot foresee with certainty whether the expected benefits will materialize, the agency could consider adding sunset provisions or provisions that commit the agency to a periodic reassessment of the benefits associated with the information collection.

   B. *Would the program require or authorize the federal government to centralize the collection of information that was previously dispersed?* While federal, state, and local government agencies collect a great deal of information on American citizens, limited permanent residents, and non-U.S. citizens, it is currently dispersed in many places, both in paper records and in databases. While it is important in many circumstances for the Department to organize the collection of data, it is also important to recognize that the federal government's centralization of information is generally met with public suspicion even when the centralized collection of information meets all legal requirements (e,g., CAPPS II and Total

Information Awareness). Centralizing information into organized government databases also increases the risk that the information collected will be used for a purpose other than that for which it was collected (commonly referred to as, "mission creep"). It also compounds the risk that compilations of information could be accessed by unauthorized persons. For these reasons, regulatory analysis of such programs should include a discussion of the civil liberties impact of centralization as opposed to a decentralized, federated or distributed approach to data collection. *See United States Dept. of Justice v. Reporters Comm. for Freedom of the Press*, 489 U.S. 749, 764 (1989) ("Plainly there is a vast difference [in terms of personal privacy] between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information.").

7. *Would the program increase the authority, control, or influence of the federal government in its relationship with state or local governments?* The Constitution creates a delicate balance between federal and state governments, which helps to prevent the accumulation of excessive power in either the States or our National Government. These structural constraints on government protect our civil liberties. *See Atascadero State Hosp. v. Scanlon*, 473 U.S. 234, 242 (1985) ("The constitutionally mandated balance of power between the States and the Federal Government was adopted by the Framers to ensure the protection of our fundamental liberties.") (quotation marks and citation omitted); *Garcia v. San Antonio Metro. Transit Auth.*, 469 U.S. 528, 572 (1985) (Powell, J., dissenting) ("The Framers believed that the separate sphere of sovereignty reserved to the States would ensure that the States would serve as an effective 'counterpoise' to the power of the Federal Government."). When authority is dispersed between the various levels of government, it is less likely that a single agency can accumulate unhealthy power over our individual lives. *See also* Exec. Order No. 13,132 (1999) ("The people of the States created the national government and delegated to it enumerated governmental powers. All other sovereign powers, save those expressly prohibited the States by the Constitution, are reserved to the States or to the people.").

8. *Would the program increase the authority, control, or influence of the federal government in its relationship with the private sector?* A robust private sector also serves as a check to the authority of the government. Associations of individuals in the private sector allow for the free flow of ideas and programs that can advance the interests of individuals. The gradual layering of regulations stifles this creativity. *See* 2 Alexis de Tocqueville, *Democracy in America* 319 (Phillips Bradley ed., Vintage Books 1990) (1840) (describing what a despotic government would look like in a democratic society, and stating that such a government would "cover[] the surface of society with a network of small complicated rules, minute and uniform, through which the most original minds and the most energetic characters cannot penetrate, to rise above the crowd. . . . Such a power does not destroy, but it prevents existence; it does not tyrannize, but

it compresses, enervates, extinguishes, and stupefies a people, till [the] nation is reduced to nothing better than a flock of timid and industrious animals, of which the government is the shepherd").

9. *Would the program require or authorize the federal government to share information about private citizens with third parties outside the federal government?* If so, the legal authorities permitting the information to be shared need to be identified.

10. *Does the program include an intelligence or surveillance component? Will the program be governed by the provisions of Executive Order 12333 and/or the National Security Act of 1947?*

Notice and Redress

11. *Does the public receive notice of the program, and have the ability to file comments on it?*

12. *Are procedures available for redress of alleged violations of civil rights and civil liberties? If so, how will the public be informed of these redress procedures? Do the redress procedures provide for data corrections to be sent to all entities with which the information has been shared?*

Alternatives

13. *Is the program the least burdensome alternative with respect to civil liberties? Could the agency formulate other alternatives to accomplish the same goal while minimizing the impacts on civil liberties?* Executive Order No. 12,866 (1993), amended by Exec. Order No. 13,258 (2002), requires agencies to identify and assess alternative forms of regulation.

14. *Could the agency alter the proposed regulatory plan to enhance civil liberties?* This may involve removing established regulatory burdens when those burdens have not produced significant benefits. For example, if an agency seeks to improve security by employing a new surveillance technique where a different surveillance technique is currently in place, the agency should consider discontinuing the first surveillance technique rather than simply adding the new to the old.

15. *Will any impositions on liberty created by the program be voluntarily incurred?*

16. *Is any imposition on civil rights and civil liberties equally distributed, randomly distributed, or focused on identifiable groups?*

17. *Is any imposition on civil rights and civil liberties brief or extended?*

Safeguards

18. *Would effective implementation of the program be dependent, in whole or in part, on government employees having a heightened awareness of Constitutional rights, federal laws or regulations, or Departmental policies as they carry out their duties?* If so, the promulgating agency should consider the need to increase or strengthen training with regard to the protection of civil rights and civil liberties.

19. *Would the program increase or decrease the discretion of those employees or agents implementing the regulation?* It is possible that an increase in discretionary authority could provide the means for obscuring improper enforcement motives at times. On the other hand, additional discretionary authority may allow for special consideration in some circumstances to ease the regulatory burden on disadvantaged individuals or groups.

20. *Does the program have embedded legal counsel or ready access to legal counsel?* The active involvement of the Office of General Counsel will assist programs to avoid violations of law.

21. *Are reports to Congress, or Congressionally-mandated audits, required, and if so are they one-time or periodic in nature?* Congressional oversight provides another level of oversight for a program.

Other Rights

22. *Could the program limit protected political or religious expression? Could the program implicitly chill open discourse or a person's ability to express their beliefs in writing that does not threaten or amount to shouting fire in a theater?* There are numerous other civil liberties recognized in our founding documents and supported by legislation, regulations, court decisions and policy. While these may be less likely to placed in jeopardy by DHS programs, they nonetheless deserve mention here and should not escape the attention of program leadership. The interpretation of rights inherent in the First Amendment, such as free speech, freedom of the press, right to assemble, and the right to petition, is mostly settled. Yet, in the realm of security policy, the application of these rights requires careful scrutiny.

23. *Could the program lead to some restriction on property ownership, such as real, personal or intellectual property, firearms, or would it grant an unfair advantage to a particular business entity? Will the program have an impact on voting rights? Does the program take the least restrictive approach possible to regulating travel, including the travel of United States citizens? Does the program take away a freedom without affording proper due process?* Other liberties that a program should be evaluated against include: the right to keep and bear arms, due process rights, private property rights, rights of the accused, voting rights, the right to travel, and the presumption of innocence.

Conclusion

Responsible Officials_____, _____

Program Manager:

Approval Signature Page

_____

Officer for Civil Rights and Civil Liberties
Department of Homeland Security