CITY AND COUNTY OF SAN FRANCISCO

DENNIS J. HERRERA
City Attorney

OFFICE OF THE CITY ATTORNEY

LINDA M. ROSS
General Counsel, Mayor's Office

DIRECT DIAL: (415) 554-4724
E-MAIL: linda.ross@sfgov.org

MEMORANDUM

TO: Laura Adleman
Public Information Officer
Office of Emergency Services

FROM: Linda M. Ross
General Counsel, Mayor's Office

DATE: September 15, 2006

RE: **Guidelines for Redacting Information from Plans Created By The City To Anticipate and Respond to Emergencies Created By Terrorist or Other Criminal Activity.**

Question Presented

Various City departments, as coordinated by the City's Office of Emergency Services/Homeland Security ("OES"), created plans to anticipate and respond to emergencies, including emergencies created by terrorist acts or other criminal activity. These plans are housed at OES's offices in the Emergency Operations Center. You have received Sunshine Ordinance requests for these plans and asked what legal bases there may be for redacting information from the plans that presents serious security concerns.

Short Answer

Generally, all records in the possession of a public agency such as OES are public records subject to disclosure, unless a specific provision of law exempts them from disclosure. State and local laws place great weight on the right of the people to know what their government is doing, and that includes how well prepared the government is for emergencies. Still, the law recognizes limited exceptions for information that if made public could jeopardize the security of the government and the people it serves. Listed below is a summary of the provisions of the San Francisco Sunshine Ordinance, California Public Records Act, and federal law that may provide a legal basis for redacting certain information from emergency plans created by City agencies to respond to emergencies.

The provisions that may provide a basis for redacting information, depending on the particular facts and circumstances, to protect against serious security risks include: (1) the exemption for certain "security procedures" and "security files," contained in California Government Code Section 6254(f); (2) the exemption for documents prepared for closed session to assess "vulnerability to terrorist attack or other criminal attacks," contained in Government Code Section 6254(aa); (3) information that would create liability for the City if released, as

Memorandum

TO: Laura Adleman
Public Information Officer
Office of Emergency Services
DATE: September 15, 2006
PAGE: 2
RE: **Guidelines for Redacting Information from Plans Created By The City To Anticipate and Respond to Emergencies Created By Terrorist or Other Criminal Activity.**

acknowledged in San Francisco Administrative Code Section 67.27(c); (4) "critical infrastructure information" submitted to the federal Department of Homeland Security under 6 U.S.C. Sections 131-133; (5) "critical infrastructure information" submitted to the California Office of Homeland Security under Government Code Section 6254(bb); (6) private information such as employee home phone numbers or addresses, under California Constitution Article I, Section 1 (right of privacy) and Government Code Section 6254(c); and (7) "recommendations of the author" contained in certain drafts or memos, under San Francisco Administrative Code Section 67.24(a).

The City's Sunshine Ordinance does not permit the City to withhold a document based on the balancing test contained in Government Code Section 6255, or based on an assertion "that the public interest in withholding the information outweighs the public interest in disclosure," which is essentially the balancing test set forth in Section 6255. (SF Admin. Code § 67.24(g),(i).) Therefore, any withholding based on security concerns must be justified under another exemption contained in the state Public Records Act or the City's Sunshine Ordinance.

The decisions to redact information in reliance on the above provisions must be made on a case-by-case basis depending on the content of a particular document.

A. Legal Background, Emergency Plans.

San Francisco's Administrative Code Section 7.3 created the "City and County Disaster Council." Section 7.4(a) empowered the Disaster Council, among other things, to "develop a plan for meeting any emergency, such plan to provide for the effective mobilization of all the resources of the community, both public and private; …." Section 7.5 declared that "[a]ll officers and employees of the City and County" together with others "shall constitute the City and County of San Francisco Emergency Services organization." Under that section: "The structure, organization, duties, and functions of the City and County Emergency Services shall be set forth in the emergency plan duly recommended for approval by the Disaster Council and approved and promulgated by the Mayor." [Emphasis added.]

Administrative Code Section 7.7 created "the office of Director of Emergency Services who shall be appointed by the Mayor." The Mayor "as chair of the Disaster Council and Commander of Emergency Services" shall employ a "Director of Emergency Services" whose duty, among other things, is to "develop and manage an emergency plan of the City and County, to coordinate all protective and relief services for the City and County, the training of all personnel connected therewith and the operation and implementation of all emergency plans and activities." [Emphasis added.]

Under Administrative Code Section 7.9, the "emergency functions of the Emergency Services organization shall be set forth in the Emergency Operations Plan of the City." Designated department heads "shall formulate functional emergency plans" which become "an annex to the Emergency Operations Plan." (*Ibid.*) [Emphasis added.]

Memorandum

TO: Laura Adleman
Public Information Officer
Office of Emergency Services
DATE: September 15, 2006
PAGE: 3
RE: **Guidelines for Redacting Information from Plans Created By The City To Anticipate and Respond to Emergencies Created By Terrorist or Other Criminal Activity.**

OES is now known as the Office of Emergency Services/Homeland Security, because it administers federal Homeland Security Funds. Federal grants require the City to take action to prevent and respond to a possible terrorist attack.

OES has possession of numerous emergency plans created by OES and other departments under these provisions.

B. State, Local and Federal Laws That Provide A Legal Basis For Redacting Certain Information From The Emergency Plans.

1. Security procedures and security files.

Under the California Public Records Act, Government Code Section 6254(f), the City is entitled to withhold:

> Records of complaints to, or investigations conducted by, or records of intelligence information or security procedures of, the office of the Attorney General and the Department of Justice, and any state or local police agency, or any investigatory or security files compiled by any other state or local police agency, or any investigatory or security files compiled by any other state or local agency for correctional, law enforcement purposes or licensing purposes …. (Emphasis added.)

Here, Section 6254(f) provides two separate possible exemptions: (1) "security procedures of … any … local police agency" or (2)"security files compiled by any … local agency for … law enforcement purposes." The California Public Records Act does not contain definitions of "security procedures," "security files," or "law enforcement purposes." And we have found no California case specifically addressing the disclosure of information from emergency plans that were created to combat terrorism or other criminal activity. But California case law makes it clear that the exemptions in Section 6254(f) are not limited to documents created as part of a criminal investigation or prosecution.

Information that is "independently exempt" under Section 6254(f) (and not exempt just because it is contained in an "investigatory …file") is not subject to a requirement that it relate to a "concrete and definite prospect of enforcement proceedings." (See *Haynie v. Superior Court* (2001) 26 Cal.4th 1061, 1069 ["[r]ecords of … investigations" need not relate to a "concrete and definite prospect of an enforcement proceeding"]; *American Civil Liberties Union Foundation v. Deukmejian* (1982) 32 Cal.3d 440, 449 ["records of intelligence information" need not relate to a "concrete and definite prospect of an enforcement proceeding"].) Records of "security procedures" are "independently exempt" under Section 6254(f). Therefore, there is no requirement that these records relate to a specific criminal prosecution to be exempt.

Memorandum

TO: Laura Adleman
Public Information Officer
Office of Emergency Services
DATE: September 15, 2006
PAGE: 4
RE: **Guidelines for Redacting Information from Plans Created By The City To Anticipate and Respond to Emergencies Created By Terrorist or Other Criminal Activity.**

Moreover, under the Act, the term "security files" is distinct from the term "investigatory files" and does not on its face necessarily involve a particular enforcement action.

Consistent with this principle, recent cases decided under the federal Freedom of Information Act have broadly defined the FOIA exemption for records created for "law enforcement purposes." (See 5 U.S.C. § 552(b)(7).) Courts have applied this exemption to information compiled to *protect against* violations of the law, or information revealing *vulnerability* of infrastructure or protective systems, not just materials created for investigation and prosecution of a violation of law. As stated above, the term "law enforcement purposes" is not defined in the California Public Records Act. Although the federal and state Acts do not contain identical provisions, the "judicial construction and legislative history of the federal act serve to illuminate the interpretation of its California counterpart." (*ACLU, supra*, 32 Cal.3d at p. 447.)

In *Living Rivers, Inc. v. United States Bureau of Reclamation*, 272 F.Supp.2d 1313 (D. Utah 2003), the court held that Bureau "inundation maps" showing "which downstream areas would be flooded in the event of a dam failure attack" could be withheld under FOIA because they were compiled for law enforcement purposes. (*Id*. at 1319.) The Bureau had offered proof that it used "the inundation maps to develop its Emergency Action Plans and to protect and alert potentially threatened people in the vicinity of the dams." (*Ibid*.) the court held that the maps "could reasonably be expected to endanger the life or physical safety of any individual" (a FOIA requirement) based on representations that "[t]errorists could use the inundation maps to estimate the extent of flooding that would be occasioned by attacking individual features of the dam. Terrorists could also use the inundation maps to compare the amount of flooding and damage that would result from attacking one dam as compared to attacking another dam." (*Id*. at 1321.)

Similarly, in *Coastal Delivery Corp v. United States Custom Service*, 272 F.Supp.2d 958 (C.D.Cal. 2003), the court held that the Custom Service could withhold the number of containers inspected at the Los Angeles/Long Beach seaport because "this information combined with other information – i.e., the number of containers examined at other ports … could reasonably be used to circumvent law enforcement practices." (*Id.* at 966.)

See also *U.S. News & World Report v. Dep't of Treasury*, No. 84-2303, 18686 U.S. Dist. LEXIS 27634, at 5 (D.D.C. Mar. 26, 1986) (unpublished decision) [Secret service properly withheld specifications and other information relating to the purchase of two armored presidential limousines, even though such information did not relate to an investigation of a specific violation of the law]; *Larouch v. Webster*, 75 Civ. 6010, 1984 WL 1061, at 8 (S.D.N.Y. October 23, 1984 [Withholding FBI lab report describing manufacture of home-made machine gun to protect law enforcement personnel from encounters with criminals armed with home-made weapons].

Memorandum

TO: Laura Adleman
Public Information Officer
Office of Emergency Services
DATE: September 15, 2006
PAGE: 5
RE: **Guidelines for Redacting Information from Plans Created By The City To Anticipate and Respond to Emergencies Created By Terrorist or Other Criminal Activity.**

Depending on their content, the City's emergency plans may contain "security procedures" or "security files" of any state or local police agency, or "security files compiled by any other state or local agency" for "law enforcement purposes."

As explained above, the City's Charter charges the Disaster Council and OES with creation of an overall emergency plan for the City, and various department heads are charged with creating functional annexes to that plan. These plans involve coordination of all City personnel and resources, which include local police agencies such as the San Francisco Police Department and the San Francisco Sheriff's Department.

These local police agencies, in conjunction with other City agencies, have developed "security procedures" in case of an emergency caused by terrorists or other criminal conduct. Moreover, OES and other local agencies have developed "security files" for "law enforcement purposes" in case of such an emergency. As demonstrated above, "law enforcement purposes" includes plans to *both prevent and respond* to a terrorist attack.

Some information about protecting against or responding to terrorism already is in the public domain, particularly on the internet, or is a matter of common sense. It would be difficult to justify redaction of this type of information. Therefore, City officials and employees knowledgeable about security must decide the information to be redacted on a case-by-case basis.

Some possible categories of information that may be subject to redaction include:

- Evaluation of particular terrorist threats, weapons or strategies.
- Identification of internal communications channels that need to remain free in the event of an emergency including a terrorist attack.
- Descriptions or analyses that show the particular vulnerability of infrastructure or protective systems to possible attack.

Again, City officials must make decisions on redaction on a case-by-case basis.

2. Documents prepared to assess vulnerability to terrorist attack or other criminal acts for distribution or consideration at a closed session.

Under Government Code Section 6254(aa), the City is entitled to withhold: "A document prepared by or for a state or local agency that assesses its vulnerability to terrorist attack or other criminal acts intended to disrupt the public agency's operations and that is for distribution or consideration in a closed session."

Memorandum

TO: Laura Adleman
Public Information Officer
Office of Emergency Services
DATE: September 15, 2006
PAGE: 6
RE: **Guidelines for Redacting Information from Plans Created By The City To Anticipate and Respond to Emergencies Created By Terrorist or Other Criminal Activity.**

Both state and City open meeting laws recognize the need to hold closed sessions to consider matters posing a threat to the security of public buildings, to essential public services, or the public's right of access to public services or facilities.

Under the state Brown Act, Government Code Section 54957(a): "Nothing contained in this chapter shall be construed to prevent the legislative body of a local agency from holding closed sessions with the Attorney General, district attorney, agency counsel, sheriff, or chief of police, or their respective deputies, or a security consultant or a security operations manager, on matters posing a threat to the security of public buildings, a threat to the security of essential public services, including water, drinking water, wastewater treatment, natural gas service, and electric service, or a threat to the public's right of access to public services or public facilities." [Emphasis added.]

Under San Francisco Administrative Code Section 67.10(a): "A policy body may, but is not required to, hold a closed session: (a) With the Attorney General, district attorney, sheriff, or chief of police, or their respective deputies, on matters posing a threat to the security of public buildings or a threat to the public's right of access to public services or public facilities." [Emphasis added.]

3. Information that would create serious liability for the City.

The City may face potential liability as a result of disclosure of certain information, if it is used by a terrorist or other criminal to harm an individual. San Francisco Administrative Code Section 67.27(c) of the Sunshine Ordinance acknowledges this consideration as a basis for withholding or redacting a document. Under the Sunshine Ordinance, Administrative Code Section 67(c): "A withholding on the basis that disclosure would incur civil or criminal liability shall cite any specific statutory or case law, or any other public agency's experience, supporting that position."

There have been a number of lawsuits against private and governmental entities in the wake of the September 11, 2001 attack on the World Trade Center in New York City. These lawsuits claim that these entities breached a duty to protect the public against the terrorist attack. (See, e.*g., In re September 11 Litigation* (S.D.N.Y. 2003) 2003 WL 22251325; *Gaff v. Port Authority* (S.D.N.Y. 2003) 2003 WL 22232949.) In the event of a terrorist attack, an injured party may bring a claim based on the assertion that the City negligently disclosed information that facilitated the attack. At this point, it is impossible to predict whether a court or jury would find that the City had a duty of nondisclosure, or that the nondisclosure was the legal cause of the injury. But the City's potential liability cannot be discounted.

The type of information that may be exempt under this section includes the examples listed in Section B(1).

Memorandum

TO: Laura Adleman
Public Information Officer
Office of Emergency Services
DATE: September 15, 2006
PAGE: 7
RE: **Guidelines for Redacting Information from Plans Created By The City To Anticipate and Respond to Emergencies Created By Terrorist or Other Criminal Activity.**

4. Law enforcement information.

The Sunshine Ordinance exempts from public disclosure certain categories of information contained in law enforcement files even after it is clear that there will be no prosecution by the District Attorney for criminal activities. (SF Admin. Code § 67.24(d).) These categories include: "The identity of a confidential source," "Secret techniques or procedures," and "Information whose disclosure would endanger law enforcement personnel." (*Id.* §§ 67.24(d.)(4), (5), (6).)

This section appears to apply to information from a particular criminal investigation and not to information created to protect against a potential crime. The City's emergency plans probably do not contain information connected to a particular criminal prosecution. Therefore, this section may not be strictly applicable to the plans. But the concerns expressed in this section, in particular the need to protect information about "secret techniques or procedures" and "information whose disclosure would endanger law enforcement personnel" involve the types of information that would also fall under the exception discussed in Section B(1) above relating to "security procedures" or "security files." As discussed above, that exception may apply to information in the City's emergency plans.

5. Critical infrastructure information submitted as confidential to the Department of Homeland Security.

Information about "critical infrastructure information" or a "protected system" voluntarily submitted to the federal Department of Homeland Security, and marked as confidential as prescribed by the Act, is not subject to state or local public disclosure laws. (See Sections 212-214 of the federal Homeland Security Act (6 U.S.C. §§ 131-133).)

The federal definition of "critical infrastructure information" is very broad. It means "information not customarily in the public domain and related to the security of critical infrastructure or protected systems." (6 U.S.C. § 131(3).) This definition covers "either physical or computer-based attack" that "violates Federal, State or local law, harms interstate commerce of the United States, or threatens public health or safety; the ability to resist such an attack;" or any "problem or solution." (*Ibid*.)

The term "protected system" is also broad. It means "any service, physical or computer-based system … that … affects the viability of a facility of critical infrastructure" and "any physical or computer-based system …." (6 U.S.C. § 131(6).)

This law was enacted to encourage private industry to "share critical infrastructure information with the federal government" and address industry's concern "that the information will not be adequately protected from disclosure to the public." (Federal Register/Vol 69, No. 34, Feb. 20, 2004/Rules and Regulations) The Act has very strict requirements for submission of information marked as confidential and acceptance by the federal government

Memorandum

TO: Laura Adleman
Public Information Officer
Office of Emergency Services
DATE: September 15, 2006
PAGE: 8
RE: **Guidelines for Redacting Information from Plans Created By The City To Anticipate and Respond to Emergencies Created By Terrorist or Other Criminal Activity.**

---

before information is protected from disclosure. (See 6 U.S.C.A § 133(e); 6 C.F.R. 29.5 [Requirements for protection].)

If the federal government shares "critical infrastructure information" or "protected system" information with a state or local government or government agency, the information cannot "be made available pursuant to any State or local law requiring disclosure of information or records." (6 U.S.C. § 133(a)(1)(E)(i).) The state Public Records Act exempts disclosure of "[r]ecords the disclosure of which is exempted or prohibited pursuant to federal or state law, …" (Cal. Gov. Code 6254(k).) Accordingly, if the City has any information that comes under the protection of the Act, it would not be subject to disclosure.

But even if the City's "critical infrastructure information" or "protected system" is not strictly covered by this federal law exception, it may come under the state Public Records Act exception discussed in Section B(1) for "security procedures" or "security files."

6. Critical infrastructure information submitted voluntarily to the California Office of Homeland Security.

The state Public Records Act exempts from disclosure "critical infrastructure information" as defined under federal law that is "voluntarily submitted to the California Office of Homeland Security …." (Cal. Gov. Code 6254(bb).) That section provides an exemption for:

> Critical infrastructure information, as defined in Section 131(3) of title 6 of the United State Code, that is voluntarily submitted to the California Office of Homeland Security for use by that office including the identity of the person who or entity that voluntarily submitted the information. As used in this subdivision, "voluntarily submitted" means submitted in the absence of the office exercising any legal authority to compel access to or submission of critical infrastructure information. This subdivision shall not affect the status of information in the possession of any other state or local government agency.

This measure was enacted: "In order to ensure that important economic infrastructure, including, but not limited to, the manufacturing, transportation, refining, and processing industries, is protected from terrorist attack …." (Section 2, Stats.2005, c. 476 (A.B.1495).)

The term "critical infrastructure information," taken from federal law, is broad as explained above. But this section of the California Public Records Act does not "affect the status of information in the possession of any other state or local government agency." There is no case law interpreting this provision, and it is unclear how it would affect information held by San Francisco that the City had not sent to the California Office of Homeland Security.

Memorandum

TO: Laura Adleman
Public Information Officer
Office of Emergency Services
DATE: September 15, 2006
PAGE: 9
RE: **Guidelines for Redacting Information from Plans Created By The City To Anticipate and Respond to Emergencies Created By Terrorist or Other Criminal Activity.**

But even if the City's "critical infrastructure information" is not strictly covered by this particular exception, it may come under the state Public Records Act exception discussed in Section B(1) for "security procedures" or "security files."

7. Private information.

Government Code 6254(c) exempts from disclosure: "Personnel, medical or similar files, the disclosure of which would constitute an unwarranted invasion of personal privacy."

If the emergency plans contain personal information, such as private home telephone numbers or home addresses of City employees, that information should be redacted under the state constitutional right to privacy, Article I, Section 1 of the California Constitution.

8. Drafts and memoranda: Recommendations of the author.

Under Government Code 6254(a), a governmental entity may withhold: "Preliminary drafts, notes, or interagency or intra-agency memoranda that are not retained by the public agency in the ordinary course of business, provided that the public interest in withholding those records clearly outweighs the public interest in disclosure." The City's Sunshine Ordinance, Administrative Code Section 67.24(a)(1) limits that exemption. It states that:

> Except as provided in subparagraph (2), no preliminary draft or department memorandum, whether in printed or electronic form, shall be exempt from disclosure under Government Code Section 6254, subdivision (a) or any other provision. If such a document is not normally kept on file and would otherwise be disposed of, its factual content is not exempt under subdivision (a). Only the recommendation of the author may, in such circumstances, be withheld as exempt.

The emergency plans may involve a "preliminary draft or department memorandum" that is "not normally kept on file and would otherwise be disposed of." In such a case, its "factual content" would not be exempt, but "recommendation of the author may, in such circumstances, be withheld as exempt."

Conclusion

OES has possession of numerous emergency plans created by various City departments. OES has received Sunshine Ordinance requests for these plans. The following legal provisions may provide a basis for redacting certain information from these plans before they are disclosed:

(1) the exemption for certain "security procedures" and "security files," contained in California Government Code Section 62354(f)"; (2) the exemption for documents prepared for

Memorandum

TO: Laura Adleman
Public Information Officer
Office of Emergency Services
DATE: September 15, 2006
PAGE: 10
RE: **Guidelines for Redacting Information from Plans Created By The City To Anticipate and Respond to Emergencies Created By Terrorist or Other Criminal Activity.**

closed session to assess "vulnerability to terrorist attack or other criminal attacks," contained in Government Code Section 6254(aa); (3) information that would create liability for the City if released, as acknowledged in San Francisco Administrative Code Section 67.27(c); (4) "critical infrastructure information" submitted to the federal Department of Homeland Security under 6 U.S.C. Sections 131-133; (5) "critical infrastructure information" submitted to the California Office of Homeland Security under Government Code Section 6254(bb); (6) private information such as employee home phone numbers or addresses, under California Constitution Article I, Section 1 (protection of privacy) and Government Code Section 6254(c); and (7) "recommendations of the author" contained in certain drafts or memos, under San Francisco Administrative Code Section 67.24(a).

Decisions on redaction should be made on a case-by-case basis by City officials or employees knowledgeable about the City's emergency plans and security concerns.