

Date: January 8, 2008

Item No. 12

File No. 07082

SUNSHINE ORDINANCE TASK FORCE

AGENDA PACKET CONTENTS LIST*

<input checked="" type="checkbox"/>	Complaint by: Wayne Lanier vs DTIS
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	

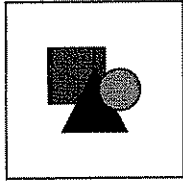
Completed by: Frank Darby

Date: January 2, 2008

***This list reflects the explanatory documents provided**

~ Late Agenda Items (documents received too late for distribution to the Task Force Members)

** The document this form replaces exceeds 25 pages and will therefore not be copied for the packet. The original document is in the file kept by the Administrator, and may be viewed in its entirety by the Task Force, or any member of the public upon request at City Hall, Room 244.



DENNIS J. HERRERA
City Attorney

ERNEST H. LLORENTE
Deputy City Attorney

DIRECT DIAL: (415) 554-4236
E-MAIL: ernest.llorente@sfgov.org

MEMORANDUM

December 26, 2007

*WAYNE LANIER V. DEPARTMENT OF TELECOMMUNICATIONS AND
INFORMATION SERVICES (07082)*

COMPLAINT

THE COMPLAINANT ALLEGES THE FOLLOWING FACTS:

On April 11, 2007, Complainant Wayne Lanier made a public records request to Chris Vein of DTIS for any policy, procedure, guideline or other controlled instruction used by DTIS to maintain public records in electronic form; backup such records; and recover such records in event of loss of the original records. On April 16, 2007, Chris Vein responded and cited 67.25(b) and California Public Records Act section 6253(c) for an extension of time to respond to the request. The extension period elapsed and Wayne Lanier claims that DTIS did not comply with the requests.

COMPLAINANT FILES COMPLAINT:

On October 10, 2007, Wayne Lanier filed a complaint against the DTIS alleging violations of section 67.21, 67.25(b), 67.29-7(a) and 67.34 of the Sunshine Ordinance.

THE RESPONDENT AGENCY STATES THE FOLLOWING:

On December 11, 2007, Barry Fraser, DTIS representative, appeared before the Complaints Committee and acknowledged that the SOTF had subject matter jurisdiction over the complaint and that the department will present its defense before the full task force.

APPLICABLE STATUTORY SECTIONS:

1. Sunshine Ordinance, San Francisco Administrative Code Section 67.1 addresses Findings and Purpose.
2. Sunshine Ordinance, San Francisco Administrative Code Section 67.21 addresses general requests for public documents.
3. Sunshine Ordinance, San Francisco Administrative Code Section 67.24 public information that must be disclosed.

Memorandum

4. Sunshine Ordinance, San Francisco Administrative Code Section. 67.26 deals with withholding kept to a minimum.
5. Sunshine Ordinance, San Francisco Administrative Code Section. 67.27 deals with justification for withholding.
6. Sunshine Ordinance, San Francisco Administrative Code Section. 67.29-7 covers correspondence and records of the Mayor and Department Heads.
7. Sunshine Ordinance, San Francisco Administrative Code Section. 67.34 deals with willful failure to comply with the requirements of the Sunshine Ordinance and the comparable state statutes to be Official Misconduct.
6. California Public Records Act, Government Code Section 6253.9 deal with information in an electronic format.
7. California Public Records Act, Government Code Section 6253 deals with public records open to inspection; agency duties and time limits.
8. California Public Records Act, Government Code Section 6255 deals with justification for withholding of records.
9. California Constitution, Article I, Section 3 addresses Assembly, petition, open meetings.

APPLICABLE CASE CASE LAW:

none

ISSUES TO BE DETERMINED**1. FACTUAL ISSUES****A. Uncontested Facts:**

- Wayne Lanier made a public records request for records.
- DTIS responded and exercised its prerogative for an extension to comply with the request.

B. Contested facts/ Facts in dispute:

The Task Force must determine what facts are true.

i. Relevant facts in dispute:

Memorandum

•

QUESTIONS THAT MIGHT ASSIST IN DETERMINING FACTS;

LEGAL ISSUES/LEGAL DETERMINATIONS;

- Were sections of the Sunshine Ordinance (Section 67.21), Brown Act, Public Records Act, and/or California Constitution Article I, Section three violated?
- Was there an exception to the Sunshine Ordinance, under State, Federal, or case law?

CONCLUSION

THE TASK FORCE FINDS THE FOLLOWING FACTS TO BE TRUE:

THE TASK FORCE FINDS THAT THE ALLEGED VIOLATIONS TO BE TRUE OR NOT TRUE.

Memorandum

THE CALIFORNIA CONSTITUTION AS AMENDED BY PROPOSITION 59 IN 2004 PROVIDES FOR OPENNESS IN GOVERNMENT.

Article I Section 3 provides:

- a) The people have the right to instruct their representative, petition government for redress of grievances, and assemble freely to consult for the common good.
- b)(1) The people have the right of access to information concerning the conduct of the people's business, and therefore, the meetings of public bodies and the writings of public officials and agencies shall be open to public scrutiny.
- 2) A statute, court rule, or other authority, including those in effect on the effective date of this subdivision that limits the right of access shall be adopted with findings demonstrating the interest protected by the limitation and the need for protecting that interest.
- 3) Nothing in this subdivision supersedes or modifies the right of privacy guaranteed by Section 1 or affects the construction of any statute, court rule, or other authority to the extent that it protects that right to privacy, including any statutory procedures governing discovery or disclosure of information concerning the official performance or professional qualifications of a peace officer.
- 4) Nothing in this subdivision supersedes or modifies any provision of this Constitution, including the guarantees that person may not be deprived of life, liberty, or property without due process of law, or denied equal protection of the laws, as provided by Section 7.
- 5) This subdivision does not repeal or nullify, expressly or by implication, any constitutional or statutory exception to the right of access to public records or meetings or public bodies that is in effect on the effective date of this subdivision, including, but not limited to, any statute protecting the confidentiality of law enforcement and prosecution records.
- 6) Nothing in this subdivision repeals, nullifies, supersedes, or modifies protections for the confidentiality of proceedings and records of the Legislature, the Members of the Legislature, and its employees, committee, and caucuses provided by Section 7 of Article IV, state law, or legislative rules adopted in furtherance of those provisions: nor does it affect the scope of permitted discovery in judicial or administrative proceedings regarding deliberations of the Legislature, the Members of the Legislature, and its employees, committees, and caucuses.

Memorandum**ATTACHED STATUTORY SECTIONS FROM CHAPTER 67 OF THE SAN
FRANCISCO ADMINISTRATIVE CODE (THE SUNSHINE ORDINANCE)
UNLESS OTHERWISE SPECIFIED****Section 67.1 addresses Findings and Purpose**

The Board of Supervisors and the People of the City and County of San Francisco find and declare:

- (a) Government's duty is to serve the public, reaching its decisions in full view of the public.
- (b) Elected officials, commissions, boards, councils and other agencies of the City and County exist to conduct the people's business. The people do not cede to these entities the right to decide what the people should know about the operations of local government.
- (c) Although California has a long tradition of laws designed to protect the public's access to the workings of government, every generation of governmental leaders includes officials who feel more comfortable conducting public business away from the scrutiny of those who elect and employ them. New approaches to government constantly offer public officials additional ways to hide the making of public policy from the public. As government evolves, so must the laws designed to ensure that the process remains visible.
- (d) The right of the people to know what their government and those acting on behalf of their government are doing is fundamental to democracy, and with very few exceptions, that right supersedes any other policy interest government officials may use to prevent public access to information. Only in rare and unusual circumstances does the public benefit from allowing the business of government to be conducted in secret, and those circumstances should be carefully and narrowly defined to prevent public officials from abusing their authority.
- (e) Public officials who attempt to conduct the public's business in secret should be held accountable for their actions. Only a strong Open Government and Sunshine Ordinance, enforced by a strong Sunshine Ordinance Task Force can protect the public's interest in open government.
- (f) The people of San Francisco enact these amendments to assure that the people of the City remain in control of the government they have created.
- (g) Private entities and individuals and employees and officials of the City and County of San Francisco have rights to privacy that must be respected. However, when a person or entity is before a policy body or passive meeting body, that person, and the public, has the right to an open and public process.

Memorandum

Section 67.21 addresses general requests for public documents.

This section provides:

- (a) Every person having custody of any public record or public information, as defined herein, ... shall, at normal times and during normal and reasonable hours of operation, without unreasonable delay, and without requiring an appointment, permit the public record, or any segregable portion of a record, to be inspected and examined by any person and shall furnish one copy thereof upon payment of a reasonable copying charge, not to exceed the lesser of the actual cost or ten cents per page.
- (b) A custodian of a public record shall as soon as possible and within **ten days** (emphasis added) following receipt of a request for inspection or copy of a public record, comply with such request. Such request may be delivered to the office of the custodian by the requester orally or in writing by fax, postal delivery, or e-mail. If the custodian believes the record or information requested is not a public record or is exempt, the custodian shall justify withholding any record by demonstrating, in writing as soon as possible and within ten days following receipt of a request, that the record in question is exempt under express provisions of this ordinance.

Section 67.24:

Notwithstanding a department's legal discretion to withhold certain information under the California Public Records Act, the following policies shall govern specific types of documents and information and shall provide enhanced rights of public access to information and records:

- a) Drafts and Memoranda....
- b) Litigation Material....
- c) Personnel Information...
- d) Law Enforcement Information....
- e) Contracts, Bids and Proposals...
- f) Budgets and Other Financial Information...

Section 67.27 provides:

Any withholding of information shall be justified in writing, as follows:

- a.) A withholding under a specific permissive exemption in the California Public Records Act, or elsewhere, which permissive exemption is not forbidden to be asserted by this ordinance, shall cite that authority.

Memorandum

- b.) A withholding on the basis that disclosure is prohibited by law shall cite the specific statutory authority in the Public Records Act of elsewhere.
- 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 litigation experience, supporting that position.
- d.) When a record being requested contains information, most of which is exempt from disclosure under the California Public Records Act and this Article, the custodian shall inform the requester of the nature and extent of the nonexempt information and suggest alternative sources for the information requested, if available.

Section 67.34 addresses willful failure as official misconduct.

The willful failure of any elected official, department head, or other managerial city employee to discharge any duties imposed by the Sunshine Ordinance, the Brown Act or the Public Records Act shall be deemed official misconduct. Complaints involving allegations of willful violations of this ordinance, the Brown Act or the Public Records Act by elected officials or department heads of the City and County of San Francisco shall be handled by the Ethics Commission.

The California Public Records Act is located in the state Government Code Sections 6250 et seq. All statutory references, unless stated otherwise, are to the Government Code.

Section 6253 provides for the process of public records inspection:

- a.) Public records are open to inspection at all times during the office hours of the state or local agency and every person has a right to inspect any public record, except as hereafter provided. Any reasonably segregable portion of a record shall be available for inspection by any person requesting the records after deletion of the portions that are exempted by law.
- b.) Except with respect to public records exempt from disclosure by express provisions of law, each state or local agency, upon a request for a copy of records that reasonably describes an identifiable record or records, shall make the records promptly available to any person upon payment of fees covering direct costs of duplication, or a statutory fee if applicable. Upon request, an exact copy shall be provided unless impracticable to do so.
- c.) Each agency, upon a request for a copy of records, shall within 10 days from receipt of the request, determine whether the request, in whole or in part, seeks copies of disclosable public records in the possession of the agency and shall promptly notify the person making the request of the determination and the reasons therefore....

Memorandum

Section 6255(a) provides for the process for justifying the non-disclosure of records.:

a.) The agency shall justify withholding any record by demonstrating that the record in question is exempt under express provisions of this chapter or that on the facts of the particular case the public interest served by not disclosing the record clearly outweighs the public interest served by disclosure of the record.

b.) A response to a written request for inspection or copies of public records that includes a determination that the request is denied, in whole or in part, shall be in writing.



Wayne Lanier
<w_lanier@pacbell.net>
12/07/2007 02:18 PM

To SOTF Members and SOTF Administrator <sotf@sfgov.org>
Ron Vinson DTIS <Ron.Vinson@sfgov.org>, Barry Fraser
cc <Barry.Fraser@SFGOV.ORG>, Doug Comstock
<Dougcoms@aol.com>, Richard Knee
bcc
Subject Documents attached for Complaint #07082

TO: All SOTF Members and SOTF Administrator Frank Darby

Please find five [5] attached Adobe Acrobats [PDF] Documents submitted in support of Complaint #07082. These are:

Disaster Recovery Pt. 1 - mostrecent.pdf
Redaction Test 071207 UNredacted.pdf
Redaction Test 071207 REDACTEDinPDF.pdf
Redaction Test 071207 REDACTEDinWord.pdf
e-mail_to_SOTF_Documents_attached_Complaint_07082_sent071207.pdf

Please provide these documents to all SOTF Members. A copy of this e-mail was simultaneously sent to DTIS [see Cc: first two names].

DTIS did provide me with a PDF Copy of the Introduction to the DTIS Disaster Recovery Plan, as requested. See the first attachmenty, **Disaster Recovery Pt. 1 - mostrecent.pdf**.

I have written comments on the original PDF document sent to me and that commented version is attached. That document was created from a file scan, thus could not be searched. It was still heavily redacted. Redactions were indicated in marker. No description of the material redacted was provided. No specific reasons for redaction were given, other than a note in the covering e-mail that redactions were for security reasons.


I believe we should discuss this heavily-redacted copy in a hearing before the full SOTF Membership. First, because I believe we should address redaction, *absent explanation of specifically what was redacted and the specific reason for redaction* . Second, because we should address the *limits of redaction for "Security Reasons"* . Third, because we should address *redaction as a "reason" for claiming excessive labor to provide requested documents by first printing, then scanning, then redacting by whiteout and pen, then scanning the redacted version, then printing to PDF and providing as un-searchable PDF documents* .

To this end, I have provided as exhibits three [3] **Searchable** PDF documents, one an **unREDACTED** pdf copy; one **REDACTED in PDF**; and one **REDACTED in WORD** then printed to PDF. These are examples of how DTIS could have avoided labor AND provided a Searchable PDF document, as well as examples of how PDF comments can be used to explain what was redacted and why it was redacted, as per Chapter 67.


Finally, I have provided a PDF version of this e-mail.

Administrator: In providing these documents electronically, provide the original PDF - NOT a scanned version. *You defeat the example if you provide "scanned" unsearchable non-dynamic versions* . In providing these documents on paper, print from the original PDF, not a scanned version.

Thank you,

 Wayne Lanier, PhD <w_lanier@pacbell.net> Disaster Recovery Pt. 1 - mostrecent.pdf

 Redaction Test 071207 UNredacted.pdf  Redaction Test 071207 REDACTEDinPDF.pdf

 Redaction Test 071207 REDACTEDinWord.pdf  e-mail_to_SOTF_Documents_attached_Complaint_07082_sent071207.pdf

To: SOTF Members and SOTF Administrator <sotf@sfgov.org>
From: Wayne Lanier <w_lanier@pacbell.net>
Subject: Documents attached for Complaint #07082
Cc: Ron Vinson DTIS <Ron.Vinson@sfgov.org>, Barry Fraser <Barry.Fraser@SFGOV.ORG>, Doug Comstock <Dougcoms@aol.com>, Richard Knee <rak0408@earthlink.net>, Erica Craven <elc@lrolaw.com>, Bruce Wolfe <sotf@brucewolfe.net>, Harrison Sheppard <hjslaw@jps.net>, Kristin Chu <kristin@chu.com>
Bcc:
Attached: D:\POLITICS\SunshineFiles\DTIS\Disaster Recovery Pt. 1 - mostrecent.pdf;
D:\POLITICS\SunshineFiles\DTIS\Redaction Test 071207 UNredacted.pdf;
D:\POLITICS\SunshineFiles\DTIS\Redaction Test 071207 REDACTEDinPDF.pdf;
D:\POLITICS\SunshineFiles\DTIS\Redaction Test 071207 REDACTEDinWord.pdf;
D:\POLITICS\SunshineFiles\DTIS\e-mail_to_SOTF_Documents_attached_Complaint_07082_sent071207.pdf;

TO: All SOTF Members and SOTF Administrator Frank Darby

Please find five [5] attached Adobe Acrobats [PDF] Documents submitted in support of Complaint #07082. These are:

- Disaster Recovery Pt. 1 - mostrecent.pdf
- Redaction Test 071207 UNredacted.pdf
- Redaction Test 071207 REDACTEDinPDF.pdf
- Redaction Test 071207 REDACTEDinWord.pdf
- e-mail_to_SOTF_Documents_attached_Complaint_07082_sent071207.pdf

Please provide these documents to all SOTF Members. A copy of this e-mail was simultaneously sent to DTIS [see Cc: first two names].

DTIS did provide me with a PDF Copy of the Introduction to the DTIS Disaster Recovery Plan, as requested. See the first attachment, Disaster Recovery Pt. 1 - mostrecent.pdf.

I have written comments on the original PDF document sent to me and that commented version is attached. That document was created from a file scan, thus could not be searched. It was still heavily redacted. Redactions were indicated in marker. No description of the material redacted was provided. No specific reasons for redaction were given, other than a note in the covering e-mail that redactions were for security reasons.

I believe we should discuss this heavily-redacted copy in a hearing before the full SOTF Membership. First, because I believe we should address redaction, *absent explanation of specifically what was redacted and the specific reason for redaction*. Second, because we should address the *limits of redaction for "Security Reasons"*. Third, because we should

address redaction as a "reason" for claiming excessive labor to provide requested documents by first printing, then scanning, then redacting by whiteout and pen, then scanning the redacted version, then printing to PDF and providing as un-searchable PDF documents.


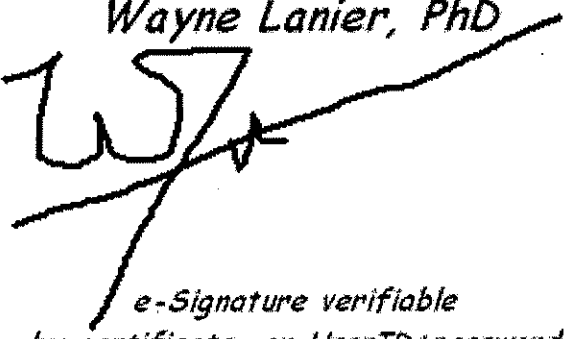
To this end, I have provided as exhibits three [3] Searchable PDF documents, one an unREDACTED pdf copy; one REDACTED in PDF; and one REDACTED in WORD then printed to PDF. These are examples of how DTIS could have avoided labor AND provided a Searchable PDF document, as well as examples of how PDF comments can be used to explain what was redacted and why it was redacted, as per Chapter 67.

Finally, I have provided a PDF version of this e-mail.

Administrator: In providing these documents electronically, provide the original PDF - NOT a scanned version. *You defeat the example if you provide "scanned" unsearchable non-dynamic versions.* In providing these documents on paper, print from the original PDF, not a scanned version.

Thank you,

Wayne Lanier, PhD <w_lanier@pacbell.net>

 Wayne Lanier, PhD

e-Signature verifiable
by certificate, or UserID+password.

Digitally signed by
Wayne Lanier, PhD
Date: 2007.12.07
14:20:02 -08'00'
Reason:
SUBMISSION OF
DOCUMENTS TO
SOTF FOR
HEARING
Location: 250
Ashbury, San
Francisco, CA
94117

EXAMPLE OF REDACTION

This document was written using Microsoft WORD v97.

This is a standard Word Application. The operating system was Windows 2000 Professional, v. 5.0.

This document will be printed to Portable Document Format [PDF] using Adobe Acrobat v. 5.0 "Professional".


This is ordinary WORD text that, when this document is printed to PDF, will be preserved.

REDACTION Example:

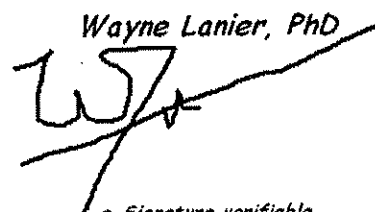

This server has been configured to permit activating the complete disk data deletion. To carry out this process, select the Tools Option "DISK DELETE".

1. Upon the prompt, enter your User ID + Password and either press [NEXT] or [ABORT]. Pressing [NEXT] will continue the "DISK DELETE" sequence. Pressing [ABORT] will cancel "DISK DELETE".

2. Upon the prompt, enter the following CODE:


and either press [DISK DELETE] or [ABORT]. Pressing [ABORT] will cancel "DISK DELETE".

Wayne Lanier, PhD


Wayne Lanier, PhD

*e-Signature verifiable
by certificate, or UserID+password.*

Digitally signed
by Wayne
Lanier, PhD
Date: 2007.12.07
12:54:58 -08'00'
Reason:
DEMONSTRATI
ON OF
REDACTION IN
WORD BEFORE
PDF
Location: 250
Ashbury, San
Francisco, CA
94117

EXAMPLE OF REDACTION

This document was written using Microsoft WORD v97.

This is a standard Word Application. The operating system was Windows 2000 Professional, v. 5.0.

This document will be printed to Portable Document Format [PDF] using Adobe Acrobat v. 5.0 "Professional".

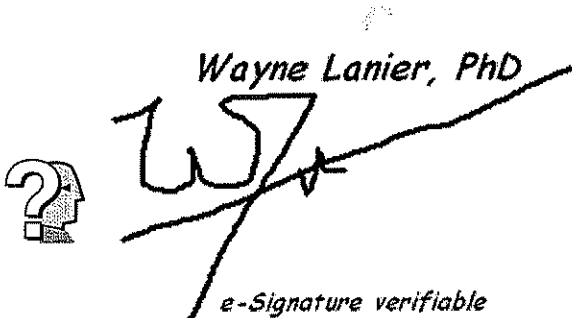
This is ordinary WORD text that, when this document is printed to PDF, will be preserved.

REDACTION Example:

This server has been configured to permit activating the complete disk data deletion. To carry out this process, select the Tools Option "DISK DELETE".

1. Upon the prompt, enter your User ID + Password and either press [NEXT] or [ABORT]. Pressing [NEXT] will continue the "DISK DELETE" sequence. Pressing [ABORT] will cancel "DISK DELETE".
2. Upon the prompt, enter the following CODE:
31415926
and either press [DISK DELETE] or [ABORT]. Pressing [ABORT] will cancel "DISK DELETE".

Wayne Lanier, PhD


*e-Signature verifiable
by certificate, or UserID+password.*

Digitally signed
by Wayne Lanier,
PhD
Date: 2007.12.07
13:23:25 -08'00'
Reason:
UN-Redacted in
either WORD or
PDF [signed in
PDF].
Location: 250
Ashbury, San
Francisco, CA
94117

WHAT TO DO IN A DISASTER



Make Preliminary Assessment

1. Make a brief determination of the following:

- What happened?
- Was anyone injured?
- Have Police/Fire/Ambulance been notified?
- What is the extent of the damage?
- When did it occur?
- What actions have the onsite personnel or others already taken?
- How long does the problem reporter estimate it will take to recover?
- What will the onsite personnel do next?
- How can the problem reporter be reached for further information or coordination?

2. Begin logging your actions and what you learn.

Be specific. Include in your log:

- **When** – The time of each entry, beginning with the time of the initial report of the incident.
- **What** – What happened or what you learned or did.
- **Who** – Who reported the item. Who was injured. Who called 911.

See Appendix x for log sheets.



Address Life Safety Issues

- For police, fire, medical emergencies..... → Call 911
- For help with what to do after requesting emergency services..... → Look in your Emergency Procedures manual.
- For help with first aid → Look in the first aid handbooks in the earthquake survival kits.
See diagrams on page x for locations of survival kits.
→ Look in the Pacific Bell phone book (white pages), under "Customer Guide" for first aid information.

NOTE: Take any steps needed to assure that injuries are dealt with, that employees and the public are not exposed to risk of injury, and further damage to equipment and property is prevented.

Enlist the aid of floor monitors, emergency personnel (fire, police, ambulance, PG&E, etc.), as appropriate. Delegate tasks wherever possible so that you can function in an overall management capacity to the maximum degree permitted by the circumstances.



Activate the Plan

1. Determine whether to activate the plan:

- If it is *probable or certain* that the disaster will interrupt services to DTIS clients for 48 hours or more, activate the disaster recovery plan.
- If it is *not clear* whether the disaster will interrupt services for 48 hours or more, do one of the following:
 - Convene the IMRT to decide whether to activate the plan based on the combined judgement of the members,
and/or
 - gather more information until you can make a reasonable judgement,
and/or
 - activate the plan.

In any event, if the incident remains *unresolved for more than 8 hours* and does not have a confidently predictable time for *resolution within 48 hours* of the original occurrence, *activate the plan*.

Illustrations

- **You would activate the plan if there is a regional disaster or if the incident caused any of the following:**

- CPU damaged
- Long term power disruption
- Facility damaged
- Access to facility denied
- Building damaged

- **You may need to activate the plan if the incident caused any of the following:**

- Software or data lost or damaged
- Threat of loss or damage to software or data
- Peripheral equipment damaged, including DASD, communications equipment, or terminals.

- **You probably would not activate the plan if:**

- Data and equipment are only minimally affected
- Damaged data and equipment are restorable within 24 hours.

2. Designate the Disaster Recovery Control Center:

Decide which location will serve as the Control Center for this incident based on information you have about the location and extent of damages.

- Depending on circumstances, verify that the room is accessible and usable by calling someone working nearby.
- If neither site is accessible, arrange another location to meet in based on your knowledge of the nature and extent of the damage.

Primary Disaster Recovery Control Center:

[]

Alternate Disaster Recovery Control Center:

[]

3. Convene the Incident Management Recovery Team (IMRT), as follows:

- a. Contact the Primary Members of the IMRT.
 - If a Primary Member cannot be reached, call that Member's Alternate.
- b. Tell the member that a disaster has occurred and the IMRT is being activated.
- c. Tell them which Control Center you have selected.



Notify the Hotsite

1. Call IBM Customer Service → []
 - Select the Business Recovery Services option.
 - Select Option #1 "Declare a Disaster"
2. Give the IBM recovery services coordinator the following information when asked. (Information may not be requested in this order):
 - Your area code and phone number..... → Give your normal work phone number.
 - Your customer number..... → []
 - Your contract numbers and machine information, as requested
 - []
 - For the mainframe
Contract number: BF20109
Machine type: 2066-oX2
Machine serial number: 83-002642A
 - For the TESS server
Contract number: CFT4HSG
Machine type: Compaq Proliant ML570 servers
 - For the HP 9000 (Retirement)
Contract number: CFTP9JI
Machine type: HP9000 K580
 - For the SUN server
Contract number: BJ04213
Machine type: Sun Ultra Enterprise 250
 - For the AS400 (Assessor)
Contract number: CFTTLGH
Machine type: AS/400

→ For the RS/6000 (Port)

Contract number: CFT44DE

Machine type: RS/6000Model H50

→ For the Shared Network (activate with Mainframe, TESS and/or AS400)

Contract number: CFT7MPG

Machine type: Cisco 7513 and PRI's

• Service you are requesting

→ If this is an actual disaster, say:

"I am reporting an *actual disaster*."

OR

If this is a potential emergency, say: "I am reporting a *potential emergency*," and explain the situation.

Request that the recovery be handled at the [] hotsite if possible.

Request that the [] be made available to us. []

• Phone number where an IBM representative can call you back.....

→ Give a phone number where an IBM representative can contact you with an action plan.

If you don't know where you will be:

a. Say, "I cannot be contacted by phone at this time," AND

b. Call IBM back when you have a number where a representative can contact you.

4. Remain near (or go to) the phone number you gave IBM and wait for a representative to contact you.

5. When you hear from the IBM representative:

a. Write down the action-plan information you are given, including the address and phone number of the IBM recovery center we have been assigned to for this disaster

→ If we are assigned to the [] Recovery Center, verify that the address is []

Phone: []

→ If we are assigned to the Recovery Center, verify that the address is:

IBM Business Recovery Services

→ If we are assigned to an *alternate* recovery center, enter the address and phone number here:

b. Obtain the CPU type and serial number of the system we will be using and record them here

CPU Type: _____

Serial No. _____

6. Provide the CPU type and serial number to the Operating Systems Recovery Team.



Notify Iron Mountain

1. Determine which Iron Mountain account(s) to activate, as follows:

Account []

→ Mainframe backups in []

This account covers:

- *mainframe backups – both application and systems backups*

These tapes are kept in [] and are stored on open shelves

Use this account if the mainframe is inoperable and backup data is to be shipped to the recovery center.

Iron Mountain will ship either the latest generation of each dataset stored at the [] Iron Mountain site or the specific reel numbers you request.

Account []

→ Mainframe Backups in []

(Systems Backups only).

This account covers:

- *mainframe backups – systems backups only (including CICS)*
- *CDs, floppy diskettes, etc. needed to initialize servers or as documentation (see Appendix L).*

These tapes are kept in [] and are stored on open shelves.

Use this account if the mainframe is inoperable and systems datasets are to be shipped to the recovery center.

Iron Mountain will ship the last received containers stored at the [] Iron Mountain facility.

Account { } → Disaster Recovery Manual and LAN Backups.

This account covers:

- *The latest copy of this manual*
- *Backups for LANs (DTIS and several client departments)*

This material is kept in {
is stored in containers.

Use this account if a disaster occurs involving the mainframe *or* LAN backup tape is needed.

Ask Iron Mountain to ship *only* the container containing the manual to the hot site. Three copies of the manual rotate through Iron Mountain. Ask Iron Mountain to send the container of these three that they received most recently.

The container numbers are:

{
{ }
}

Container numbers for LAN backups are in Appendix L.

Account { } → TESS Payroll Front-End Backups

This account covers:

- *Backups from the TESS server*

These tapes are sent to { } and
are stored in containers.

Use this account if the TESS server is inoperable.

Iron Mountain will ship the last received container stored at the { } site to the TESS server recovery location.

Account []

→ **AS400 Backups**

This account covers:

- **AS400 backups supporting the INPACT property system**

These tapes are kept in [] and are stored on open shelves.

Use this account if the AS400 is inoperable.

Iron Mountain will ship the last received container stored at the [] site to the AS400 recovery location.

Account []

→ **HP 9000 Backups**

This account covers:

- **HP9000 backups supporting the Retirement retiree payroll system**

These tapes are kept in [] are stored on open shelves

Use this account if the HP9000 is inoperable.

Iron Mountain will ship the last received container stored at the [] site to the HP9000 recovery location.

2. Call Iron Mountain []

→ []

3. Tell the Iron Mountain contact that the City and County of San Francisco is activating the disaster recovery plan for one or more accounts, and give the following information:

- The account(s) to activate.
- Information requested to identify you as an authorized caller.

NOTE: DTIS senior staff and Operations senior managers are authorized to activate disaster recovery plans.

- The IBM recovery center address and phone number..... → Obtained during hotsite notification, above. Get this from the person who notified IBM of the disaster. (See page 1-5.)



Notify Recovery Teams

1. Place a message on the DTIS Main Message Mailbox

Compose a message covering the nature and extent of the disaster and what action the caller should take. Follow the procedure in Appendix M to record the message in the DTIS Main Mailbox.

If appropriate, add messages to the Division mailboxes to provide specific information and instructions employees in those divisions.

2. Begin contacting other members of the IRMT and then the team leaders for each of the recovery teams.

Refer to Sections 3 and 4 for the team leaders' names. Look in Appendix K for home phone numbers and Appendix J for cell phone and pager numbers.

2. Meet with operators of low income housing developments
3. Design fiber network to reach developments
4. Identify non-profit partners to deploy and maintain access networks within buildings
5. Deploy fiber to building and access networks within buildings

V. Wireless Network(s) for Internal City Needs

Estimated Time to Complete: 24 Months

Beginning date: January 1, 2008

Target Completion Date: December 31, 2010

Estimated Cost: \$12,000,000 - \$18,000,000

1. Identify specifications for public safety oriented network with ECD, Police, Fire
2. Identify sources of funding
3. Identify opportunities for additional municipal uses, e.g., field work such as, permitting, building inspection, assessment, and metering, e.g., parking meters, etc.
4. Issue request for proposal
5. Select private partner
6. Deploy municipal network

VI. Facilitate Entry of Private Wireless Networks

Estimated Time to Complete: 12 Months

Beginning date: January 1, 2008

Target Completion Date: December 31, 2010

1. Identify potential City owned "mounting assets" for radios, e.g., roof tops, light poles, City radio towers
2. Identify and to the extent possible, "pre-address" environmental issues



Wayne Lanier
<w_lanier@pacbell.net>

12/09/2007 08:01 PM

Please respond to
w_lanier@pacbell.net

To SOTF Members and SOTF Administrator <sotf@sfgov.org>

cc Ron Vinson DTIS <Ron.Vinson@sfgov.org>, Barry Fraser
<Barry.Fraser@SFGOV.ORG>, Doug Comstock
<Dougcoms@aol.com>, Richard Knee

bcc

Subject CORRECTION TO Documents attached for Complaint
#07082

TO: All SOTF Members and SOTF Administrator Frank Darby

Please find one [1] attached Adobe Acrobat [PDF] Document. **This is a correction.**

Among the five [5] documents originally submitted on 2007.12.07 in support of Complaint
#07082 was:

"Redaction Test 071207 REDACTEDinPDF.pdf"

This was not the correct file, intended for submission.

The correct file is attached:

Redaction Test 071207 REDACTEDinPDF_locked_signed.pdf

My apologies for this error.

Thank you,



Wayne Lanier, PhD Redaction Test 071207 REDACTEDinPDF_locked_signed.pdf

EXAMPLE OF REDACTION

This document was written using Microsoft WORD v97.

This is a standard Word Application. The operating system was Windows 2000 Professional, v. 5.0.

This document will be printed to Portable Document Format [PDF] using Adobe Acrobat v. 5.0 "Professional".

This is ordinary WORD text that, when this document is printed to PDF, will be preserved.

REDACTION Example:

This server has been configured to permit activating the complete disk data deletion. To carry out this process, select the Tools Option "DISK DELETE".

1. Upon the prompt, enter your User ID + Password and either press [NEXT] or [ABORT]. Pressing [NEXT] will continue the "DISK DELETE" sequence. Pressing [ABORT] will cancel "DISK DELETE".
2. Upon the prompt, enter the following CODE:
31415926
and either press [DISK DELETE] or [ABORT]. Pressing [ABORT] will cancel "DISK DELETE".

Wayne Lanier, PhD



Wayne Lanier, PhD

*e-Signature verifiable
by certificate, or UserID+password.*

Digitally signed by
Wayne Lanier,
PhD
Date: 2007.12.09
11:58:53 -08'00'
Reason: Signing a
locked document
Location: 250
Ashbury, San
Francisco, CA
94117



Doris Legaspi/DTIS/SFGOV
12/31/2007 11:29 AM

To frank.darby@sfgov.org, sotf@sfgov.org
cc Barry Fraser/DTIS/SFGOV@SFGOV, Ron Vinson
bcc
Subject SOTF Complaint No. 07082_Wayne Lanier v. DTIS - January 8, 2008

History: This message has been forwarded.

Mr. Darby,

DTIS is providing the attached response letter and three attachments in the matter of complaint No. 07082_Wayne Lanier v. DTIS. Please distribute these documents to all Task Force Members prior to the January 8, 2008 meeting.

If you have any questions please don't hesitate to contact me.



Response to Lanier.pdf



Attachment 1 - LA V42.pdf



Attachment 2 - 110807 .pdf



Attachment 3 - 111607 .pdf

Doris Legaspi
Executive Secretary
Telecommunications & Information Services
One So. Van Ness, 2nd Floor,
San Francisco, CA 94103
Tel. No. (415) 581-3988
Fax No. (415) 581-3970

CITY AND COUNTY OF SAN FRANCISCO



Chris Vein
Executive Director

Telephone: (415) 581-4001

**DEPARTMENT OF TELECOMMUNICATIONS
AND INFORMATION SERVICES**

Ron Vinson
Chief Administrative Officer

Telephone: (415) 554-0803 Fax: (415) 581-4003

December 31, 2007

City and County of San Francisco
Sunshine Ordinance Task Force
c/o Mr. Frank Darby
1 Dr. Carlton B. Goodlett Place
Room 244
San Francisco, CA 94102-4689

RE: #07082_Wayne Lanier v. DTIS

Dear Mr. Darby:

This is a response by the Department of Telecommunications and Information Services (DTIS) to Complaint # 07082, submitted by Dr. Wayne Lanier, scheduled for hearing before the Task Force on January 8, 2008. Please deliver this response to the members of the Task Force.

As a preliminary matter, we admit that we were very late in providing the records in response to Dr. Lanier's initial public records request, made on April, 11, 2007. On April 16, 2007, we sent Dr. Lanier an email acknowledging his request and asking for a time extension to respond. Unfortunately, DTIS was inundated with many special projects during that period, in addition to being in the midst of organizing a major office move to occur later in the year, so the response was delayed for several months. We have addressed this problem by assigning additional staff to respond to Sunshine requests. As a result, we have significantly improved our response time for such requests.

With respect to Dr. Lanier's original request, we believe that we have now complied in every respect. This request stated:

Please [Reply] to this e-mail by Friday, May 11th, 2007, attaching a Portable Document Format [PDF] copy of any procedure, policy, guideline, SOP, or other controlled instruction [herein called "procedure"] used by your Office or Department to:

- Maintain Public Records in electronic form;
- Back-up such electronic Public Records; and,
- Recover such back-up electronic Public Records in event of loss of the original records.

We provided three PDF documents to Mr. Lanier: two documents that consist of the Table of Contents and Chapter One of the DTIS Disaster Recovery Manual (Manual); and a copy of DTIS email backup and recovery procedure, contained in our client Service Level Agreement (Attachment 1).

We provided the excerpts from the Manual to Dr. Lanier with the clear understanding that the materials were an introduction and overview of the full document, which consists of several hundred pages. The full Manual provides detailed instructions for the recovery of backed-up data and systems applications for dozens of servers operating as part of the City's data network. The full manual includes comprehensive procedures for the verification, validation and identification of backup data retrieved in the recovery process.

Dr. Lanier agreed that he would review the excerpts and then determine whether access to the rest of the Manual was necessary. Dr. Lanier never requested any additional information from DTIS.¹

Only one document, Chapter One of the Manual, remains at the heart of this dispute. This document contains information that, if disclosed to the public, would create a significant risk of unauthorized access to essential City records, including records that are exempt from disclosure. Therefore, when we provided the document to Dr. Lanier we redacted only the portions of the documents that posed such a risk.

We have discussed this document with Dr. Lanier by phone on two separate occasions. We have carefully considered his concerns and, upon further consideration, removed some of our previous redactions. In addition, each redaction has been clearly indicated with brackets ([]). We also provided Mr. Lanier with a detailed email on November 8, 2007 (Attachment 2) that clearly identified the types of information redacted and provided a clear reference to the appropriate justifications for withholding this information. We sent Dr. Lanier a follow-up email on November 16, 2007, asking if he needed to meet and discuss the documents or clarification of any of the redactions (Attachment 3). However, Dr. Lanier never responded until we received a copy of his email to the Task Force on December 7, 2007.

Dr. Lanier's December 7 email stated two general concerns with DTIS' redaction decisions, and also raised a third entirely new concern. First, Dr. Lanier asks the Task Force to "address redaction, ***absent explanation of specifically what was redacted and the specific reason for redaction.***" Second, he asks the Task Force to "address the ***limits of redaction for 'Security Reasons'***". Third he asks the Task Force to "address ***redaction as a "reason" for claiming excessive labor to provide requested documents by first printing, then scanning, then redacting by whiteout and pen, then scanning the redacted version, then printing to PDF and providing as un-searchable PDF documents.***" (emphasis in original)

I. Specific Redactions and Reasons for Redaction

DTIS has answered these questions about our decision to redact portions of Chapter One of the Manual in our email of November 8, 2007. We explained that the Manual is one way in which DTIS fulfills the public interest, as described in San Francisco Administrative Code Section 8.9, in preserving "records which would be essential to the continuity of government and the protection of rights and interests of individuals in event of a major disaster . . . against possible destruction by fire, earthquake, flood, enemy attack or other cause." The Manual includes detailed security information that authorized City personnel would use to gain access to these essential records that have been stored in off-site facilities, as well as information pinpointing the location of off-site storage and recovery facilities that contain these back-up records.

¹ For this reason, we are puzzled by Dr. Lanier's assertion that important information is missing from the records provided by DTIS, such as how the recovery is verified and validated. There is considerable additional information of this nature in the full Manual, which Dr. Lanier expressly told DTIS he did not wish to see. See the email from Dr. Wayne Lanier to SOTF dated November 2, 2007 (at pp. 39-40 of the SOTF file in this matter).

The off-site records addressed in the Manual include the essential records of many City departments and offices, including the Office of the District Attorney, the Police Department, the Port of San Francisco, the Office of the Treasurer and Tax Collector, the Human Services Agency, the San Francisco Employee Retirement System, DTIS and many others. These records contain a host of information that is exempt from disclosure under state and local law, including law enforcement investigatory or security files (California Government Code Section 6254(f)); attorney-client privileged information (California Government Code Section 6254(k) and California Evidence Code Section 954); trade secret information submitted by entities doing business with the City (California Government Code Section 6254(k), California Evidence Code Section 1060 and California Civil Code Section 3426 *et seq.*); proprietary financial information submitted by entities seeking contracts with the City (San Francisco Administrative Code Section 67.24(e)); confidential taxpayer information (San Francisco Business and Tax Regulations Code Section 6.22-1); and personnel records the disclosure of which would constitute an unwarranted invasion of personal privacy and other private information such as social security numbers (California Government Code Section 6254(c)). Legislators have authorized these exemptions despite the presumption that government records should be open to the public because they understand that important public policy reasons exist for governments to maintain the confidentiality of certain records.

Unauthorized access to this exempt information would undermine the City's ability to carry out numerous critical functions, including law enforcement, legal affairs, tax administration, personnel administration, and business affairs with outside entities.

The excerpts from the Manual contain some information that, if disclosed to the public, would create a significant risk of unauthorized access to these essential records, including records that are exempt from disclosure. In particular, the documents contain detailed security procedures for accessing these essential records in a disaster, including passwords, account numbers, phone numbers, and container numbers for the record repositories. In addition, the documents include information about the precise physical locations of the back-up records and the "hotsites" at which essential City data operations would be conducted in the event of a crippling disaster.

Disclosure of these security procedures and locations would provide a road map to allow unauthorized persons or entities to gain access to all of the City's essential records that are addressed in the Manual, including all of the exempt information listed above. Accordingly, we have made limited redactions only as necessary to remove this road map information, to prevent the disclosure of information that is exempt from disclosure.

For example, we disclosed the names of the vendors used to provide backup storage and hotsite services, but we withheld the precise locations of the storage facilities and hotsites. Dr. Lanier points out that a review of the public domain will provide a listing of multiple sites used for such purposes. However, the actual site used by the City cannot be determined by such a review.² Likewise, Dr. Lanier claims that vendor telephone numbers are publicly available and must therefore be disclosed. However, the specific call-in number used by the City to activate a hotsite or initiate a data recovery is not a public record. This information is part of the authentication process and therefore is similar to a password or user access identifier. This

² For example, IBM marketing materials assert that the company operates 150 business recovery centers worldwide, and the addressees and general phone numbers of those centers are public record. However, no publicly available documents indicate which of these centers would be used by the City in the event of a disaster.

information is not necessary to derive an understanding of how the City's data recovery process works. However, it could be used to compromise the City's data security processes.

Any information that we make available in response to a public records request must be disclosed in response to any similar future request, regardless of the purpose of the future request. Although we are confident that Dr. Lanier is motivated by good intentions in making this request, we cannot be certain that future requesters would have the same good intentions. As a result, we must be mindful of the risk that a person could use the redacted information to gain unauthorized access to City records.

II. Limits of Redaction for Security Reasons

As discussed above, we have limited our redactions to two categories of information (1) detailed security procedures for accessing backup records in a disaster, including passwords, account numbers, phone numbers, and container numbers for the record repositories; and (2) information about the precise physical locations of the records and the "hotsites" at which essential City data operations would be conducted in the event of a major disaster.

Disclosure of these security procedures and location information would provide a road map to allow unauthorized persons or entities to gain access to all of the City's essential records that are addressed in the Manual. Such information could be used to compromise the City's data security process, either by a bad actor intentionally tampering with a critical recovery event, or by hackers attempting to "spoof" a data recovery event by contacting the data recovery center and posing as City staff. DRIS simply cannot disclose the information at issue in this case without a substantial risk that the information may be used to compromise the security and integrity of the City's back up systems.

In short, information that may reasonably lead to unauthorized access to protected City records, especially when the information is only incidental to the understanding of the contents of the document, should be protected from disclosure.

III. Method of Redaction

As a final matter, Dr. Lanier, in his December 7 email, raises a new issue. He requests the Task Force to review this request "because we should address **redaction as a "reason" for claiming excessive labor to provide requested documents by first printing, then scanning, then redacting by whiteout and pen, then scanning the redacted version, then printing to PDF and providing as un-searchable PDF documents.**" (emphasis in original) Dr. Lanier goes on to suggest an alternative method for redacting protected information in documents subject to Sunshine requests.

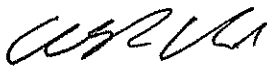
We note that the redacted document in this case (as in many cases for public records) was most readily available in paper format. Dr. Lanier's procedure would not be feasible for records stored only on paper.

In addition, while Dr. Lanier's redaction methods may or may not have merit, he only raised this issue with DTIS on December 7, 2007, and we have not had adequate opportunity to thoroughly review and test his suggestions. DTIS would welcome the opportunity to undertake such a review. Above and beyond the question of adequacy as a redaction solution will be the issue of cost to each department to purchase software licensing to allow wide scale use of the required software throughout City departments. Initial investigation suggests that the software is costly compared with other methods of redaction.

With all due respect, the purpose of this hearing is simply to determine whether DTIS has responded to Dr. Lanier's Sunshine request, not to determine the appropriateness of specific choices of software applications, system security safeguards or back up and recovery procedures employed by DTIS. Dr. Lanier has indicated to us on several occasions that he believes that certain data back up and recovery procedures employed by DTIS can be improved upon. In our conversations, he has repeatedly provided suggestions for improving these procedures. We welcome Dr. Lanier's input on these matters. However, the decision to implement those recommendations remains solely with DTIS, and is outside of the scope of this hearing.

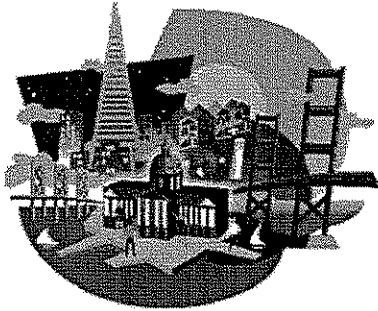
If you have any questions regarding this response, please feel free to contact me.

Sincerely,



**Ron Vinson
Chief Administrative Officer
Department of Telecommunications and Information Services**

Enclosures



San Francisco
Department of Telecommunications
& Information Services

Service Level Agreement
For Enterprise Messaging Services

Version 4.0

June 12, 2007

Approvals of the Agreement

DEPARTMENT :

[Name], [Department], Department Head	Date
---------------------------------------	------

[Name], [Department], IT Manager	Date
----------------------------------	------

[Name], [Department], Help Desk Manager	Date
---	------

DEPARTMENT OF TELECOMMUNICATIONS AND INFORMATION SERVICES:

Chris Vein, DTIS, Chief Information Officer	Date
---	------

Rod Loucks, DTIS, Chief Technology Officer	Date
--	------

Scott Melendez, DTIS, Manager, Enterprise Messaging	Date
---	------

DTIS, Customer Service Manager	Date
--------------------------------	------

TABLE OF CONTENTS

APPROVALS OF THE AGREEMENT	I
DEPARTMENT :	
.....	I
DEPARTMENT OF TELECOMMUNICATIONS AND INFORMATION SERVICES:	I
SERVICE LEVEL AGREEMENT TERMS	1
PURPOSE	1
TERM OF AGREEMENT	1
CHANGE AND REVIEW PROCESS FOR THE AGREEMENT.....	1
E-MAIL SYSTEM BUDGET	2
E-MAIL SYSTEM PERFORMANCE AND DTIS SERVICES	3
HOURS OF OPERATION	3
POPULATION TO BE SUPPORTED.....	3
SERVICES TO BE PROVIDED	3
SERVICES/SYSTEMS NOT SUPPORTED	3
E-MAIL SYSTEM PERFORMANCE	4
MESSAGING SYSTEM INTRANET SITE.....	4
E-MAIL SYSTEM MAINTENANCE AND RETENTION.....	4
RESTORATION OF USER'S MAILBOX DATABASE	5
TECHNICAL SUPPORT.....	5
PRIORITY (SEVERITY) LEVELS.....	5
PRIORITY (SEVERITY) LEVEL RESPONSE TIMES.....	8
ESCALATION PATH FOR PROBLEM REPORTING	8
PROBLEM REPORTING	10
STAMP TICKETS AND TYPES:.....	10
E-MAIL/INTRANET ASSISTANCE	11
CONTACTING DTIS HELP DESK	11
BACKUP AND RECOVERY	11
USER DATA BACKUPS	11
SYSTEM BACKUPS.....	13
E-MAIL SYSTEM RECOVERY	15
INFRASTRUCTURE MAINTENANCE	15
CUSTOMER RESPONSIBILITIES	17
CUSTOMER LEVEL SUPPORT	17
ENTERPRISE EMAIL SLA.DOC	PAGE I

LOCAL NOTES ADMINISTRATOR DUTIES	17
SYSTEM REQUIREMENTS	17
IBM NOTES CLIENT 6.5.X:.....	17
DOMINO WEB ACCESS (FORMERLY KNOWN AS INOTES):	18
IBM SAMETIME (INSTANT MESSAGING):.....	18
DOMINO/PDA SYNCHRONIZATION:.....	18
OTHER MESSAGING SERVICES:.....	18
PROBLEM REPORTING & CONTACT LIST	19
PROBLEM REPORTING	19
CONTACT LIST	19
NOTIFICATION LIST	19
E-MAIL SYSTEM VIRUS/SPAM PREVENTION.....	19
 APPENDIX A	 21
DTIS ESCALATION SUPPORT LIST.....	21
 APPENDIX B	 22
VENDOR SUPPORT CONTACT INFORMATION	22
SOFTWARE: IBM LOTUS NOTES/DOMINO SUPPORT INFO	22
HARDWARE: IBM AS/400 ISERIES SUPPORT INFO	22
AS/400 ISERIES SERIAL NUMBERS	22

Service Level Agreement Terms

Purpose

This document describes the services the Department of Technology and Information Services (DTIS) provides for the Enterprise Electronic Messaging and Calendar System (the E-Mail System). These services will be provided for the elected officials and employees of the City and County of San Francisco (City).

This document defines the standard and optional aspects of the E-Mail System services, explains the procedures that City Departments (a.k.a. Customers) must follow to take full advantage of the services offered, and clarifies the responsibilities of both the Customer and DTIS.

DTIS's commitment is to make available E-Mail System services that are user-friendly, reliable, powerful, and fully compatible with emerging technologies, backed by the most comprehensive and beneficial support services possible. In addition, DTIS seeks maximum value for taxpayers' money. DTIS's services are meant to ensure the integrity of the E-Mail System and to minimize the potential for serious problems.

Term of Agreement

The term of this agreement is for the duration of time that the Customer utilizes the Enterprise Email System, or until such time as the agreement is revised.

Change and Review Process for the Agreement

This agreement will be reviewed annually at a renewal meeting of City department representatives with DTIS.

Either DTIS or individual departments may initiate a review of the agreement outside the regular cycle by contacting the signing parties and arranging a discussion. Factors that may initiate a need for review and modification of the agreement include changes in the amount or type of services required; feedback that indicates service issues, significant changes in workload projections, and/or changes in funding. Changes will be incorporated into the Service Level Agreement (SLA) through addenda.

E-Mail System Budget

The Customer will provide the appropriate work orders and budget funding in the annual DTIS budget. E-Mail System charges will be budgeted in each department's annual service budget with DTIS.

E-Mail System Performance and DTIS Services

Hours of Operation

The Enterprise Electronic Messaging and Calendar System is operational 24 hours a day, 365 days a year, except those times as published in the sections on *System Backups* and *Infrastructure Maintenance*.

Population to be Supported

- All City and County Departments
- All City and County Commissions
- Approved specific community-based and/or affiliated agencies

Services to be Provided

- Provide a Help Desk staff available 7 AM to 6 PM, Monday through Friday, and secondary support staff after hours
- Priority level problem reporting (see **Technical Support** for details)
- E-Mail for City owned and installed workstations within the City's wide area network (WAN)
- Remote access to E-Mail System via secure (VPN) workstation
- E-Mail mailbox database maintenance on all E-mail System servers
- Security & privacy of E-Mail System
- Maintain daily backup of E-Mail System
- Anti-virus and spam protection for E-Mail System
- Enterprise E-Mail web site with system availability/status, news, and message board(s)
- Provide a Notification via e-mail to designated persons in the departments in the event of system-wide problems
- Business Continuity Support

Services/Systems Not Supported

- Non-IBM approved clients
- Non-AS/400 local servers (Exception: DTIS will support the Exchange-Domino Connector between DPH and UCSF)
- Any departmental owned and/or maintained WAN, LANs, servers, workstations, or other telecommunications equipment or peripherals.

E-Mail System Performance

System Performance will not be defined in this SLA because performance can be impacted by many factors including server workload and bandwidth available across the WAN at any given point in time. DTIS will ensure that E-Mail routing occurs continuously (24x7) by configuring the Domino servers to deliver e-mail on an **immediate** basis with no queuing of email for subsequent delivery, except in the event of a severe Messaging System problem.

Messaging System Intranet Site

DTIS maintains an Intranet site (<http://intranet/messaging>) that has system status, downloads, user guides, and more. All departmental administrators are urged to consult this site regularly.

E-Mail System Maintenance and Retention¹

DTIS encourages all City Department employees of the Enterprise Messaging System to routinely archive and/or dispose of e-mail messages in their mailbox in order to maximize the amount of space available. DTIS will establish a quota system, consisting of the following:

- A warning threshold of 80 megabytes (Mb);
- A ceiling of 150 Mb.²

DTIS believes this is sufficient allocation of space to accommodate most users. Departments with their own instance can allocate this space on a different methodology, but based on an allocation of 100Mb per user, e.g., a

¹ From Sunshine Ordinance Task Force memorandum dated March 1, 2001; *E-Mail*: Under the Sunshine Ordinance and state law, any e-mail that is created or received in connection with the transaction of public business and which (1) the department retains as evidence of the department's activities, or (2) relates to the legal or financial rights of the City or of persons directly affected by the activities of the City, must be retained in accordance with the department's record retention schedule. The standard for determining, if e-mail is a record that must be retained is identified to the standard applies to any document. Government Code § 62.52(e); Administrative code § 67.20(b). If the e-mail must be retained, it should be printed out and the hard copy retained in the appropriate file unless the department can reliably retain and retrieve the e-mail in electronic format.

² Exceptions will be made for senior management within departments.

department with 100 users will have a 10 Gb allotment. It will be up to individual department IT managers then to set individual quotas on their users or otherwise manage mailboxes. Department IT managers will be responsible for reducing the size of user mail files if the storage capacity levels of the iSeries servers reaches certain threshold levels. DTIS will monitor this and provide these reports to the customer.

Restoration of User's Mailbox Database

The Department Administrator in the user's department or individual user can request a restoration of a user's e-mail database or their own e-mail database, respectively. The ability to restore a user's mailbox database will depend on the availability of the back-up tape. Data restoration of a user's e-mail database may take up to 48 hours.

Technical Support

Unless otherwise indicated below, **the first level of contact for user and system issues is the Department Local Help Desk or designated Local Notes Administrator and/or Mentor within each department!** The DTIS Help Desk will ask if that step has been done before entering an incident.

The technical support provided by DTIS is primarily with regard to system availability. It is not technical support to answer user 'how-to' questions. It is the responsibility of the Department's Local Help Desk or Notes Administrators or Mentors to handle user questions/problems. If Department Local Help Desk or Notes Administrator/Mentor is unavailable, the DTIS Help Desk can provide user assistance at (415) 554-5700. Telephone support is available from 7 AM to 6 PM, Monday through Friday (except Holidays and weekends). A Messaging system administrator is on-call 7x24; see table below for response time.

Priority (Severity) Levels

At the time the problem is logged, either the Department Local Help Desk or DTIS Help Desk will establish the priority based on *Priority Determination Table* below.

Priority Determination Table

Priority 1 (Critical)	Priority 2 (High)	Priority 3 (Medium)	Priority 4 (Low)
Business and Financial Exposure			
Failure creates a critical business and financial exposure.	Failure creates a serious business and financial exposure.	Failure creates a low business and financial exposure.	Failure creates a minimal business and financial exposure.
Work Outage			
<p>The e-mail application failure causes the Customer to be unable to work or perform some significant portion of their job.</p> <p>System is unavailable, not responding, or not accessible.</p>	<p>The e-mail application failure causes the Customer to be unable to work or perform some significant portion of their job.</p>	<p>The e-mail application failure causes the Customer to be unable to perform some small portion of their job, but they are still able to complete most other tasks.</p> <p>May also include questions and requests for information.</p>	<p>The e-mail application failure causes the Customer to be unable to perform a minor portion of their job, but they are still able to complete most other tasks.</p>
Number of Customers Affected			
The e-mail application failure affects the <i>majority</i> of Customers.	The e-mail application failure affects a <i>large</i> number of Customers.	The e-mail application failure affects a <i>small</i> number of Customers.	The e-mail application failure may only affect one or two Customers.
Workaround [This bullet carries the heaviest weighting of the characteristics for Priority 1 and 2.]			
No acceptable and implemented workaround exists (i.e., the job cannot be done in some other way).	An acceptable and implemented workaround exists (i.e., the job can be done in some other way).	An acceptable workaround may exist.	An acceptable workaround may exist.

Priority (Severity) Level Response Times

The following table displays the Response Time and Resolution Time goals for each severity level.³

Priority 1 (Critical)	Priority 2 (High)	Priority 3 (Medium)	Priority 4 (Low)
Response Time			
From DTIS Help Desk: Within one hour, 24x7. From Messaging Team: Within an hour after being notified	Within 90 minutes: 10x5 After Hours: Within 2 1/2 hours	From DTIS Help Desk: Within eight hours or by next business day, 10x5.	Within twenty-four hours or next business day, 10x5.
Resolution Time			
The maximum acceptable resolution time is 24 continuous hours, after initial response time. Updated status will be provided to all Customers contacts, if problem has not been resolved after 24 hours.	The maximum acceptable resolution time is up to five (5) business days.	The maximum acceptable resolution time is 20 business days.	The maximum acceptable resolution time is 90 calendar days.

Escalation Path for Problem Reporting

If problem persists or is labeled "Priority 1" by Department Local Help Desk or trained Notes Administrator(s), the issue should be escalated as per below.

Support Level	Role	Action
0	User	Call Mentor or Departmental Help Desk (see Appendix A)

³ In any event, a call to the DTIS Help Desk will result in a STAMP ticket creation.

1	Mentor	Resolve problem OR Call Department Help Desk for resolution (see Appendix A)
2	Department Help Desk or Lotus Notes Administrator	Resolve problem OR Call DTIS Help Desk for resolution or update
3	DTIS Help Desk	Resolve problem OR Escalate to Second Tier Support

Problem Reporting

The DTIS Help Desk is staffed 7 AM to 6 PM, Monday through Friday (except on Holidays and weekends). The secondary support staff is available after hours.

The DTIS Help Desk and secondary support staff can be reach at (415) 554-5700.

In any event, customers will receive STAMP ticket to follow up.

Priority Level 1:

DTIS Help Desk duties:

- 1) Log all Priority 1 issues, which are dispatched for immediate review by the e-mail service technicians.
- 2) Provide First-Tier troubleshooting
- 3) Escalate to DTIS Messaging Group or Manager
- 4) Follow-up with the Customer to confirm resolution of issue.
- 5) Provide back-up support by technical staff at DTIS's One Market location.

Priority Levels 2, 3, and 4:

DTIS Help Desk duties:

- 1) Log all Priority 2, 3, and 4 issues, which are dispatched for immediate review by DTIS Messaging group..
- 2) Follow-up with the Customer to confirm status or resolution of issue.

STAMP Tickets and Types:

When a call is logged, the DTIS Help Desk will issue a STAMP ticket. There are two types of STAMP tickets: Incidents and Requests.

Generally, an Incident is an issue that is impacting the customer immediately. Examples would be:

- Inability to access Mail
- Non-delivery or receipt of an expected email
- Customer receiving "Server Not Responding" errors

These are issues that require immediate resolution.

A Request is an issue that may involve some research, procurement, or other tasks that might take some time. Examples of Requests:

- Creation of a mail-in database
- Moving users between departments
- Procurement of software

E-Mail/Intranet Assistance

E-Mail/Intranet assistance: Self-help is available 24 hours on the DTIS Messaging Intranet site (<http://messaging>). On this site, you will find a variety of documents, tips, techniques, and other helpful information.

Contacting DTIS Help Desk

Method	Procedure
Telephone	DTIS Help Desk (415) 554-5700
E-Mail	If a Customer would like to e-mail a request or question, send to dtis.helpdesk@sfgov.org
Fax	Address faxes to the DTIS Help Desk, and fax to (415) 554-4730.

Backup and Recovery

The following procedures are for Enterprise Servers residing in DTIS locations, and will be performed by DTIS staff. Backup, offsite tape rotation, and restore procedures for servers that reside at One Market Plaza, Department of Public Health Department of Human Services, and City Hall, that will be performed primarily by DTIS Department staff, will be mutually agreed upon by the Department and DTIS, in an addendum to the SLA. IBM's Backup Recovery Media Services (BRMS) software is used to perform backups.

User Data Backups

Data is backed-up to tapes, which are rotated to a secure offsite location. The IBM Domino system is still available during scheduled user data backups.

Frequency	Data Type	Day Performed ³	Start Time ³	Retention
Daily (incremental, which is changed data only)	Mail databases (*.nsf), mail templates (*.ntf) and mailboxes (*.box)	Monday – Friday	11:00 PM	14 days
Weekly (full, which is all user data)	Mail databases (*.nsf), mail templates (*.ntf) and mailboxes (*.box)	Sunday	11:00 PM	63 days (9 weeks)

⁴ DTIS has defined backup scheduling. However, the specify day and start time may vary based the on the server location and customer needs (Refer to Appendix C). DTIS reserves the right to modify “Day Performed and Start Time” parameters based on change in volume of user data.

System Backups

System back-up tapes are rotated offsite. Routine system backups will not happen simultaneously at all sites to reduce downtime. System Backup restores are performed under the direction of the DTIS Messaging Operation staff.

NOTE: The IBM Domino system will not be available during system backup described below.

System	Frequency	Data	Day Performed ²	Start Time ²	Retention
Domino	Monthly	All Domino configuration objects and user data	Last Sunday of every month, except December. Also done before and after: Installing new software or releases. Maintenance updates are applied, including quarterly maintenance release (QMR)	6:00 AM	90 days
IBM Operating System & Notes/Domino Software	Quarterly	All License Program Procedures and Operating system	Last Saturday of every quarter. Also done after installation Also done after PTF (program	To Be Scheduled by Operations	90 days

³ DTIS has defined backup scheduling. However, the specify day and start time may vary based the on the server location and customer needs (Refer to Appendix C). DTIS reserves the right to modify "Day Performed and Start Time" parameters based on change in volume of user data.

System	Frequency	Data	Day Performed ²	Start Time ²	Retention
			temporary fix) has been applied		5 years
Domino	Annually	All Domino configuration objects and user data	Last Sunday of the calendar year. Runs in place of the December Monthly	6:00 AM	

The Full annual backup represents a snapshot of the IBM Domino user and system data as of the last day of that calendar year.

E-Mail System Recovery

User data backups occur once a day. Therefore, due to the timing of each backup, DTIS cannot restore e-mail messages that were deleted before the backups occur. DTIS will make every effort to restore user data and/or system data that has successfully been backed up to recoverable media.

Infrastructure Maintenance

While DTIS would like to provide 24x7x365 access to E-Mail, DTIS occasionally will need to take the E-Mail System off-line in order to:

1. Apply fixes to software problems on the Operating System or on Domino.
2. Upgrade the Operating System or upgrade Domino.
3. Replace hardware that has failed.
4. Install additional hardware (i.e., additional memory, processors, etc.)

DTIS will maintain system status on the City Intranet site at <http://intranet/messaging>. DTIS will use the following guidelines when scheduling maintenance and/or repairs that cause the E-Mail System to be unavailable:

1. Customers will receive 2-weeks notice on any planned outages. In the event of an emergency outage, DTIS will notify departmental administrators and post information on the Intranet site.
2. Hardware and software upgrade implementations (Operating System and Domino) will be scheduled over a weekend. The size and significance of the upgrade may require a period of unavailability as long as Friday evening 11PM to Monday morning 6 AM. DTIS will make every effort to keep the window as small as possible.
3. If at all possible, fixes, including hardware repairs, will be installed either on weekends or if necessary during the evening after 7 PM.
4. Fixes to Operating System software and Domino system software (called "Hotfixes") that resolve problem(s) impacting Enterprise E-Mail will be installed as soon as possible. Depending upon the severity of the problem, the software fix may be applied during the prime time (M-F 8 AM - 5 PM). Operating system upgrades and Domino Server upgrades generally will not be installed until the upgrade has been available for a minimum of 4 months. This is to insure that any bugs in the new upgrade are resolved before the City attempts its upgrade. All upgrades will be applied in accordance with DTIS' internal Change Control procedures.

5. Major Domino Server updates will be planned in advance and will be discussed with customers. DTIS will never install a ".0" release on a production server.
6. Not all operating system upgrades may be installed. DTIS will evaluate the necessity of each upgrade, taking into consideration the following:
 - To enable Lotus Notes/Domino to function properly
 - To maintain continuous ongoing IBM technical support
 - To maintain capability with Lotus Notes/Domino
7. Not all Domino Server Upgrades may be installed. DTIS will work with departments to evaluate whether and when to implement upgrades, based upon various criteria including (but not limited to):
 - To resolve an outstanding issue/shortcoming or provide a feature/function deemed necessary by the City and County of San Francisco
 - To maintain continuous ongoing IBM/Lotus support
 - To provide new features deemed desirable by most departments

Customer Responsibilities

Customer Level Support

The Customer will designate from the departmental staff, a Local Notes Administrator(s) and a Local Notes Mentor(s). For small departments, these contacts can be the same person. Small departments also may choose to have DTIS provide Local Notes Administrative support. Local Notes Administrators are responsible for creating, maintaining, and deleting e-mail accounts, and managing message space for the end-users in their department. Local Notes Mentors provide first-line assistance to end-users in the use of the System.

The Customer is responsible for sending the Local Notes Administrator(s) and the Local Notes Mentor(s) to the appropriate training, which is provided by the DTIS Technology Learning Center.

Local Notes Administrator Duties

The Local Notes Administrator will be responsible for the following duties:

- Create and modify users
- Create and modify groups
- Remote console access to review the various (logical server) logs
- Monitor mailbox usage
- Password recovery
- Run ad hoc database compacts (although a system-wide database compact will be regularly scheduled by DTIS)
- Administer remote access

System Requirements⁵

The Customer will ensure that all City standard workstations have these system requirements for the following services:

IBM Notes Client 6.5.x:

Windows:

- Pentium III or above running 2000/XP Pro
- 128 Mbytes of RAM or above

⁵ With the latest releases of the Notes client, IBM is no longer supporting the following OSes: Windows 95, NT, Mac OS 9.

- 300 Mbytes of available hard drive space or more

Macintosh system requirements:

- G4 or later processor
- OS X 10.3 or later
- 128 Mb RAM

Domino Web Access (formerly known as iNotes):

Windows:

Internet Explorer 6.0 with security patches.

Domino Web Access, as of 6.5.1 and beyond, will unofficially support the following browsers:

- Safari (Mac OS X)
- Firefox (Windows, Mac OS X)

You may use these browsers, but some issues may be encountered.

IBM Sametime (Instant Messaging):

To access the IBM Sametime Instant Messaging system, you must be running the Notes 6.5.1 or later client for Windows. Macintosh users can access Sametime via *Sametime Browser Connect*, using Internet Explorer 5.2.3. Contact the DTIS Help Desk for details. (Mac OS X users can also use third-party clients; search <http://versiontracker.com>. DTIS will NOT support these clients!)

Domino/PDA Synchronization:

DTIS provides LIMITED support for PDA synchronization software. Departments can purchase IBM EasySync through DTIS. This is the ONLY synchronization software we “support” – the Help Desk cannot take calls on any other third-party software.

Other Messaging Services:

8. Any other Domino-related messaging services will be evaluated on a case-by-case basis, via a STAMP Request.

Problem Reporting & Contact List

Problem Reporting

When reporting problems to the DTIS Help Desk, the Customer will provide all of the following:

1. A contact name, the site, and call back number
2. The problem being experienced
3. When it occurred
4. What activity was being performed at the time
5. Any other relevant information requested by service provider
6. The device (computer type and location) upon which it occurred

Contact List

DTIS Help Desk will maintain the current list of the known departmental Local Notes Mentor(s) and Local Notes Administrator(s) on the Enterprise Electronic Messaging and Calendar Intranet site. Customers will regularly monitor and verify the accuracy of this information and notify DTIS of any changes in a timely manner.

Notification List

Customers will provide DTIS the name(s), SMTP email address, and phone number(s) of designated person(s) to be notified via e-mail in case of system wide problems with the Messaging System.

E-Mail System Virus/Spam Prevention

The Enterprise Messaging Servers automatically scan any file attachments and "tag" spam received. The anti-virus software is configured to check the vendor's web site for new patterns on a regular basis. However, DTIS advises departments that they should still have employees scan all e-mail attachments from outside the City for viruses, worms, etc. using the department's LAN based anti-virus software before launching an attachment. If an infected file is distributed, employees must inform their Local Administrator or Local Help Desk and the DTIS Help Desk (415) 554-5700 immediately or follow their departmental published procedures or training material.

By law, we cannot block spam. Our gateway servers "tag" spam, and it is delivered to the user's Spam folder. The Domino servers are set to delete the

contents of the Spam folder every 7 days. There are also tools that allow users to submit suspected spam messages, as well as mark mistakenly “tagged” spam messages.

Appendix A

DTIS Escalation Support List

The following represents DTIS Escalation On-Call Support List for the Enterprise E-Mail System. Department local technical support or Department Local Help Desk's first point of contact is the DTIS Help Desk when reporting a problem of the Enterprise E-Mail System.

Functional Area	Manager
DTIS Help Desk Local (415) 554-5700 Fax (415) 554-4730	Frank Augustine, Customer Service Manager (business hours) Office: 415-554-5700
IBM Lotus Domino/Notes AS/400 and Backup Recovery Media Services (BRMS)	Scott Melendez Office: 415-554-0844 Mobile: 415-999-9383

Appendix B

Vendor Support Contact Information

The following is informational only. Support vendor information is used by the DTIS Help Desk and Technical support to escalation priority "1" problems and to support Departments.

SOFTWARE: IBM Lotus Notes/Domino Support Info

DTIS maintains a 24 x 7x 365 support contract with IBM on all licensed IBM IBM Notes/Domino software components.

HARDWARE: IBM AS/400 iSeries Support Info

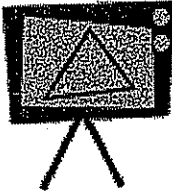
DTIS maintains a 24 x 7x 365 support contract with IBM on registered hardware & software.

Locations of AS/400 iSeries Servers for City and County of San Francisco are:

- DTIS Operations - One Market Plaza (OMP)
- Department of Public Health (DPH) - 1380 Howard
- City Hall - 1 Dr. Carlton B. Goodlett Place
- Department of Human Services – 170 Otis St.

AS/400 iSeries Serial Numbers

- 105N69M - Model 840 at OMP
- 105N6CM - Model 820 at DHS
- 105N6DM - Model 820 at DPH
- 105N6BM - Model 820 at DPH
- 105N6AM - Model 820 at City Hall



Barry Fraser/DTIS/SFGOV

11/08/2007 11:15 AM

To Wayne Lanier <w_lanier@pacbell.net>

cc Ron Vinson <Ron.Vinson@sfgov.org>, Thomas Long/CTYATT@CTYATT

bcc

Subject RE: DTIS Disaster Recovery Plan: In the matter of Complaint #07082 Lanier v DTIS

Dear Dr. Lanier,

As we discussed by phone on Tuesday, I have attached two documents that are excerpts from a Department of Telecommunications and Information Services (DTIS) Disaster Recovery Manual (Manual). We have carefully considered your response to the previous versions of these documents that we have disclosed to you. Upon further consideration, we have removed some of our previous redactions. However, for reasons that are explained below, we must continue to redact certain limited information from these documents. For your convenience, I have clearly indicated each redaction with brackets ([]).

The Manual is one way that DTIS fulfills the public interest, as described in San Francisco Administrative Code Section 8.9, in preserving "records which would be essential to the continuity of government and the protection of rights and interests of individuals in event of a major disaster . . . against possible destruction by fire, earthquake, flood, enemy attack or other cause." The Manual includes detailed security information that authorized City personnel would use to gain access to these essential records that have been stored in off-site facilities, as well as information pinpointing the location of off-site storage and recovery facilities that contain these back-up records.

The off-site records addressed in the Manual include the essential records of many City departments and offices, including the Office of the District Attorney, the Police Department, the Port of San Francisco, the Office of the Treasurer and Tax Collector, the Human Services Agency, the San Francisco Employee Retirement System, DTIS and many others. These records contain a host of information that is exempt from disclosure under state and local law, including law enforcement investigatory or security files (California Government Code Section 6254(f)); attorney-client privileged information (California Government Code Section 6254(k) and California Evidence Code Section 954); trade secret information submitted by entities doing business with the City (California Government Code Section 6254(k), California Evidence Code Section 1060 and California Civil Code Section 3426 *et seq.*); proprietary financial information submitted by entities seeking contracts with the City (San Francisco Administrative Code Section 67.24(e)); confidential taxpayer information (San Francisco Business and Tax Regulations Code Section 6.22-1); and personnel records the disclosure of which would constitute an unwarranted invasion of personal privacy and other private information such as social security numbers (California Government Code Section 6254(c)). Legislators have authorized these exemptions despite the presumption that government records should be open to the public because they understand that important public policy reasons exist for governments to maintain the confidentiality of certain records.

The attached documents from the Manual contain some information that, if disclosed to

the public, would create a significant risk of unauthorized access to these essential records, including records that are exempt from disclosure. In particular, the documents contain detailed security procedures for accessing these essential records in a disaster, including passwords, account numbers, phone numbers, and container numbers for the record repositories. In addition, the documents include information about the precise physical locations of the records and the "hotsites" at which essential City data operations would be conducted in the event of a crippling disaster.

Disclosure of these security procedures and location information would provide a road map to allow unauthorized persons or entities to gain access to all of the City's essential records that are addressed in the Manual, including all of the exempt information listed above. Accordingly, we have made limited redactions only as necessary to remove this road map information, to prevent the disclosure of information that is exempt from disclosure. Unauthorized access to this exempt information would undermine the City's ability to carry out numerous critical functions, including law enforcement, legal affairs, tax administration, personnel administration, and business affairs with outside entities.

Please be aware that any information that we make available in response to your public records request must be disclosed in response to any similar future request, regardless of the purpose of the future request. Although we are aware of the good intentions that motivate your request, we cannot be certain that future requesters would have the same good intentions. As a result, we must be mindful of the risk that a person could use the redacted information to gain unauthorized access to City records.

Also, I remind you that we are moving offices over this weekend, and appreciate your willingness to send an email to SOTF agreeing to a continuance of Item #07082 at Tuesday's meeting.

If you have any questions regarding this response, please feel free to contact me. Please note my new contact information below, effective November 13, 2007.

Barry Fraser
Policy Analyst
City and County of San Francisco
Department of Telecommunications and Information Services (DTIS)
875 Stevenson St. 5th Floor
San Francisco, CA 94103

(415) 554-4076
(415) 554-0854 FAX

Please note my new address and phone number, effective November 13:

One South Van Ness, 2nd Floor
San Francisco, CA 94103

Phone: 415-581-7105



Disaster Recovery TOC.pdf



Disaster Recovery Pt. 1.pdf



Barry Fraser/DTIS/SFGOV

11/16/2007 02:44 PM

To Wayne Lanier <w_lanier@pacbell.net>

cc Ron Vinson <Ron.Vinson@sfgov.org>

bcc

Subject Re: Continuance of November 13th Complaint Committee

Dr. Lanier,

Thank you for agreeing to a continuance of this matter. I wanted you to know that we remain willing to discuss any outstanding issues you may have with this sunshine request.

Next week is the Thanksgiving holiday, so I propose that we touch bases the week of November 26. If you have ongoing concerns, we will make ourselves available for a phone conference during that week. That will give us time to attempt a resolution of any remaining issues before the Complaint Committee meets again.

Regards,

Barry Fraser

DTIS has moved! Please note my new address and phone number, effective November 13:

**Barry Fraser
Policy Analyst
City and County of San Francisco
Department of Telecommunications and Information Services (DTIS)
One South Van Ness, 2nd Floor
San Francisco, CA 94103**

Phone: 415-581-3976

Wayne Lanier <w_lanier@pacbell.net>



Wayne Lanier
<w_lanier@pacbell.net>

11/09/2007 11:34 PM

To Ron Vinson <Ron.Vinson@sfgov.org>, Frank Darby
<Frank.Darby@sfgov.org>, SOTF <sotf@sfgov.org>
cc Barry Fraser <Barry.Fraser@SFGOV.ORG>

Subject Re: Continuance of November 13th Complaint Committee

Good evening, SOTF Administrator Frank Darby,

I agree to DTIS Chief Administrative Officer Ron Vinson's request for a continuance of the November 13th hearing of Complaint #07082.

Although it is late for such a request, assuming this move has been planned for some time, I think little would be served by compelling the hearing on November 13th. My apologies to the members of SOTF.

I assume the matter of #07082 will be continued to the next regularly scheduled session of SOTF

appropriate the subject of this Complaint. Please inform me of the hearing data as soon as convenient.

I may attend the hearing of November 13th in regard to other matters, but I would not expect to speak or report on Complaint #07082 in absence of DTIS members.

Thank you,

Wayne Lanier, PhD <w_lanier@pacbell.net>

At 11/9/2007 11:05 AM -0800, Ron Vinson wrote:

Dear Mr. Darby,

DTIS is in the midst of an office relocation and is requesting a continuance of Item #07082 at the November 13th Complaint Committee. The move will take place November 9 -13th. The Department has been in contact with the complainant about the department's request for the continuance and has indicated he is agreeable to continue this item at a later date.

Ron Vinson

Chief Administrative Officer

DTIS

(415) 554-0803 - office

(415) 554-4733 - fax

REQUEST THAT THE SUNSHINE ORDINANCE TASK FORCE [SOTF] MAKE A DETERMINATION IN THE MATTER OF COMPLAINT #07082, WAYNE LANIER, PHD, *versus* THE DEPARTMENT OF TELECOMMUNICATIONS AND INFORMATION SERVICES [DTIS].

01. To SOTF Administrator Frank Darby: Please print this e-mail to Adobe Acrobat searchable PDF file for distribution to SOTF Members, making it also available in searchable PDF file on the SOTF Web Site. I have attached such a file to this e-mail for your convenience. It is essential, to conserve SOTF time, that Members have this information before the hearing.

02. In advance, I apologize to the Members of SOTF for submitting a direct request for this Determination in the matter of #07082 before you. I make this request in the presumption that, upon reading and reflecting on my suggestions, you may see a larger advantage to the City in the course I propose.

03. Although this matter arose from my Sunshine Request #070411 for procedures guiding preservation and recovery of Public Records, the issue before us in #07082 concerns the extent and means of information redaction in the DTIS Disaster Recovery Plan.

DTIS has provided an essential part of their ~1,000-page Disaster Recovery Plan as per our agreement. DTIS argues, and I accept that some information in their Disaster Recovery Plan, if made public, might compromise computer system security. We disagree on the following: The extent of such redaction [49 redactions in 11 pages]; the failure to identify exactly what was redacted [only a black mark] and the specific security issue claimed to justify redaction [only "security" in a cover e-mail]; and, the means by which redaction was carried out [resulting in a PDF image file NOT searchable].

04. The opinion of the City Attorney Linda Ross [2006] establishes that a Disaster Recovery Plan is a Public Record. Both Chapter 67 and this opinion, either directly or by implication, require identification of the information redacted and identification of the reasons for redaction. Chapter 67 also mandates that, given the means, an agency must comply with a Sunshine Request for electronic Public Records in the requested specific format. Unfortunately, the language of this guidance is very general and has not helped resolution of the issues in Complaint #07082.

My contention is that this is a general problem, not limited to #07082, and a Determination is needed to serve as broader guidance.

05. Specific Arguments regarding security: As I understand DTIS, they argue for strong security, *i.e.*, if there is any imaginable chance that information made public might be used in any unintended way, the information should be suppressed [for the entire 1,000-page DTIS Disaster Plan, this would have meant ~5000-redactions]. A specific example is the telephone number or address of a secure public storage site. I argue for strong freedom of information, *i.e.*, information suppressed only if it is obvious to a reasonable person that, made public, it

would be used for harm. A specific example is the password to a secure computer server database.

06. Specific Arguments regarding redaction: As I understand DTIS, they argue that indicating the location of redaction and stating a general reason in a cover e-mail, *e.g.*, "security", is sufficient for the identification requirement. I argue that the identification requirement mandates presenting an argument to the "reasonable person" described in 05, above: That the kind of data redacted must be identified in each instance, *e.g.* "computer system password"; and, the specific reason served by redaction be identified, *e.g.*, "unauthorized use of this password might result in loss of records".

07. Specific Arguments regarding format: I requested electronic Public Records in Adobe Acrobat searchable Portable Document Format [PDF].

Searchable PDF is a widely-used means of providing and transmitting electronic records. A PDF reader is freely available on the Internet at no cost. The full version of Adobe Acrobat provides for many levels of record security. With reasonable security settings, it can be printed, copied, saved, and searched for words or phrases. Metadata from such a document indicates when it was created, who created it, how it was created, how it has been changed, and the conditions of its security. It is possible to configure a PDF file so that sensitive metadata are obscured - this is a form of redaction, however, and should be identified and justified. Published methods for directly redacting information in a PDF file exist, although they require special redaction software [*e.g.*, Redax from Appligent - see attached file "DS_RedaxLite.pdf"]. Comments are easily made in a PDF file, providing for identification and explanation of redactions. PDF files can be locked to prevent change of the document text and change or addition to comments.

As I understand DTIS, they argue safe redaction required the following steps:

Printing the native format of their Disaster Recovery Plan to paper, then using a black marker for redaction, then scanning the paper to an electronic image, then converting the image to PDF which was electronically transmitted to me.

The result was a PDF file not searchable, with all metadata redacted without identification. I argue that such method, laborious, time consuming, and expensive, was not necessary. I demonstrated one method, redaction in the native format [Microsoft WORD], followed by printing the redacted copy directly to searchable PDF and transmitting it to me.

Since this is not a universal method, as some native formats do not provide for redaction, I also attempted to provide a method that could be carried out entirely in Adobe Acrobat. Although such methods are described for later versions of Adobe Acrobat, especially by using special redaction software, I was unable to find a simple method for secure redactions in the Adobe Acrobat version I have, lacking special redaction software, and have had to withdraw the results of my efforts to date.

08. At the last SOTF meeting, determination of jurisdiction, DTIS Policy Analyst Barry Fraser and I agreed before the meeting to accept SOTF jurisdiction, eliminating lengthy arguments

wasting SOTF time. Our discussion continued after the meeting, and we found common ground in a joint concern for complicated efforts of redaction that waste the time of City agencies. I believe we can also find such common ground on identification of redaction and, possibly, on the limits of redaction. I expect some compromises need be made, since DTIS is likely to want stronger security and I am likely to want greater freedom of information. In addition, there are clear technical issues, some of which I find are beyond my expertise or resources.

09. Observation on the role of DTIS: As the City's experts on information technology, DTIS is uniquely qualified and positioned to take the lead in formulating general methods for preparing electronic Public Records for transmission to Sunshine requesters. Their resources are limited, however, and funding for an extensive project of research followed by educational efforts is problematic. Use of their expertise to test methods is a different matter.

10. My contribution: I am willing to devote some time to researching methods of redaction directly in Adobe Acrobat and preparing model redacted documents for DTIS to test. Further, if we are jointly able to agree on one or more methods for more efficient redaction of Public Records, either directly in Adobe Acrobat or in a general list of widely-used native formats [WORD, Excel, etc.], I am willing to write a brief guideline for SOTF that may be used by any City agency.

11. SOTF Determination: My sense is that this effort is unlikely without the umbrella and consideration of SOTF, presumably in the form of a Determination for resolving Complaint #07082. This is, therefore, a proposal that SOTF make a Determination *Re. #07082* to mandate and facilitate cooperative action between Complainant Dr. Wayne Lanier and DTIS Staff to agree upon a redacted searchable copy of the DTIS Disaster Recovery Plan. The objective here is to reach a wider resolution of issues arising in #07082 that may serve as a template for resolution of future Redaction disagreements; To create a precedent for future resolution of Complaints of a similar nature; and, To provide technical guidance by which City Departments can make reasonable redactions per Chapter 67 directly in Adobe Acrobat searchable PDF files. To this end, Lanier will carry out research and provide model redacted documents for DTIS to test. DTIS will, with reasonable speed, test these methods for suitability. DTIS will also provide information and guidance as their resources permit. DTIS will provide a copy of [introduction] Disaster Recovery Plan redacted according to the agreed method. Lanier will prepare a brief document for SOTF use explaining the method(s) used for redaction. Requirements shall be:

- Redaction entirely by electronic means, minimizing steps, and, if possible carried out entirely in Adobe Acrobat;
- Each redaction shall be marked, with type of information identified and reason for redaction specifically stated; and,
- Product shall be a redacted Public Record in searchable PDF format permitting printing, save, and copy.

There are two attachments to this e-mail:

Request_SOTF_Determination_07082_Lanier_v_DTIS_071231.pdf

[a searchable signed copy of this e-mail]

DS_RedaxLite.pdf

[a description of the PDF Redaction Tool]

Wayne Lanier, PhD



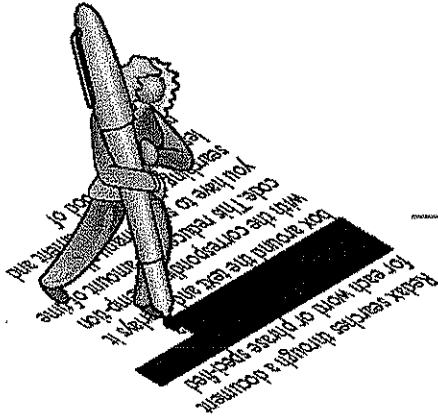
Wayne Lanier, PhD

[Handwritten signature]

*e-Signature verifiable
by certificate, or UserID+password.*

Digitally signed
by Wayne
Lanier, PhD
Date:
2007.12.31
13:43:25 -08'00'
Reason:
SUBMISSION
OF
DOCUMENTS
TO SOTF FOR
HEARING
Location: 250
Ashbury, San
Francisco, CA
94117

Redax Lite



What Is Redax Lite?

Redax Lite is a plug-in for Adobe Acrobat that lets you remove (redact) text from PDF files to assure confidentiality of sensitive information. It is a streamlined version of Appligent's Redax product, but at a much lower price, for businesses that need text redaction only—and do not require image redaction or the additional features that Redax provides.

Applications for Redax Lite include:

- Compliance with the Freedom of Information Act (FOIA), Privacy Act, and Health Information Portability and Accessibility Act (HIPPA)
- Protection of proprietary information in patent filings, New Drug Applications (NDAs), and Investigational New Drug Applications (INDAs)
- Deletion of private information from legal briefs before submission to U.S. courts and agencies

Redax Lite completely and securely removes information that you select for redaction. It parses the document, physically deletes the selected information, and generates a new redacted document. The deleted information cannot be recovered, because the redacted file is created without it.

Key Features

Standard Acrobat markup. Use Acrobat's highlight, underline, and crossout tools to select text for redaction.

Choice of redaction characters. Select any printable character or white space to replace redacted text.

Exemption codes. Use industry-standard exemption codes or redact without specifying a reason. U.S. FOIA code and Privacy Act code palettes are provided. You can also create your own custom exemption codes.

Bookmarks. Include bookmarks from the original document in the redacted file, if you wish.

Annotations. Delete annotations following redaction to ensure that they are not released with the document.

Viewing. View Redax boxes in Acrobat or Acrobat Reader—without Redax Lite installed.

Verification. Write the information in your redacted PDF file to a text file to verify that the content is appropriate for public viewing before releasing it.

Who Uses Redax Lite?

- U.S. federal government agencies
- U.S. state and local governments
- Government agencies and law enforcement outside the United States
- Government contractors and consulting firms
- Pharmaceutical companies
- Law firms and litigation support companies
- Human resource departments at corporations

Modes of Operation

Redax Lite can be run in a variety of ways:

Basic operations. The simplest way to use Redax Lite is to select text for redaction with Adobe Acrobat highlight, underline, and crossout tools. Even authors who do not have Redax Lite installed on their computers can mark text for redaction.

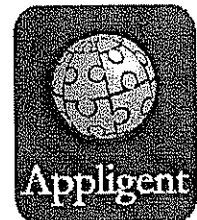
Automation options. To speed the redaction process, mark text to be removed by finding bracketed text in the document.

Supported Software & Platforms

Redax Lite is compatible with Adobe Acrobat 5.0 and above, and is available for Windows NT and higher.

Customer Support

Appligent offers both email and telephone support. As an Appligent customer, you are assured of receiving an email response within 24 hours. Phone support is available between 9 a.m. and 5 p.m. EST.





DENNIS J. HERRERA
City Attorney

ERNEST H. LLORENTE
Deputy City Attorney

DIRECT DIAL: (415) 554-4236
E-MAIL: ernest.llorente@sfgov.org

November 5, 2007

Sue Cauthen, Chair
Members of the Complaint Committee

Re: Wayne Lanier v. Department of Telecommunications and Information Services (07082)

Dear Chair Cauthen and Members of the Complaint Committee:

This letter addresses the issue of whether the Sunshine Ordinance Task Force ("Task Force") has jurisdiction over the complaint of Wayne Lanier against the San Francisco Department of Telecommunications and Information Services ("DTIS").

BACKGROUND

On April 11, 2007, Complainant Wayne Lanier made a public records request to Chris Vein of DTIS for any policy, procedure, guideline or other controlled instruction used by DTIS to maintain public records in electronic form; backup such records; and recover such records in event of loss of the original records. On April 16, 2007, Chris Vein responded and cited 67.25(b) and California Public Records Act section 6253(c) for an extension of time to respond to the request. The extension period elapsed and Wayne Lanier claims that DTIS did not comply with the requests.

COMPLAINT

On October 10, 2007, Wayne Lanier filed a complaint against the DTIS alleging violations of section 67.21, 67.25 and 67.34 of the Sunshine Ordinance.

SHORT ANSWER

Based on Complainant's allegation and the applicable sections of the Sunshine Ordinance and the California Public Records Act, which are cited below, the Sunshine Ordinance Task Force *does* have jurisdiction over the allegation. The allegations are covered under (67.21 and 67.25) of the Ordinance.

DISCUSSION AND ANALYSIS

Article I Section 3 of the California Constitution as amended by Proposition 59 in 2004, the State Public Records Act, the State Brown Act, and the Sunshine Ordinance as amended by Proposition G in 1999 generally covers the area of Public Records and Public Meeting laws that the Sunshine Ordinance Task Force uses in its work.

Letter to the Complaint Committee

Page 2

November 5, 2007

The Sunshine Ordinance is located in the San Francisco Administrative Code Chapter 67. All statutory references, unless stated otherwise, are to the Administrative Code. Section 67.21 generally covers requests for documents and Section 67.25 covers Immediate Disclosure Requests. CPRA Section 6253 generally covers Public Records Requests.

In this case, Wayne Lanier claims that DTIS's failure to respond violates sections 67.21 and 67.25 of the Ordinance. He also claims that the failure is official misconduct under 67.34 of the Ordinance.-The Task Force has jurisdiction to hear this matter will determine whether DTIS violated the Ordinance and/or the Public Records Act.



SUNSHINE ORDINANCE TASK FORCE

1 Dr. Carlton B. Goodlett Place, Room 244, San Francisco CA 94102

Tel. (415) 554-7724; Fax (415) 554-7854

<http://www.sfgov.org/sunshine>

SUNSHINE ORDINANCE COMPLAINT

Complaint against which Department or Commission Telecommunications & Information Services

Name of individual contacted at Department or Commission Ron Vinson

- ☒ Alleged violation public records access
☐ Alleged violation of public meeting. Date of meeting _____

Sunshine Ordinance Section 67.21 (b), (c); 67.25 (b); 67.29-7 (a)

(If known, please cite specific provision(s) being violated)

Please describe alleged violation. Use additional paper if needed. Please attach any relevant documentation supporting your complaint.

Failure to provide records, failure to justify withholding, untimely response, and failure to maintain and preserve records

Do you wish a public hearing before the Sunshine Ordinance Task Force? ☒ yes ☐ no

*(Optional)*¹

Name Wayne Lanier Address _____

Telephone No. _____ E-Mail Address W_lanier@pacbell.net

Date 10/10/2007 _____
Signature

¹ NOTICE: PERSONAL INFORMATION THAT YOU PROVIDE IS SUBJECT TO DISCLOSURE UNDER THE CALIFORNIA PUBLIC RECORDS ACT AND THE SUNSHINE ORDINANCE, EXCEPT WHEN CONFIDENTIALITY IS SPECIFICALLY REQUESTED. COMPLAINANTS CAN BE ANONYMOUS AS LONG AS THE COMPLAINANT PROVIDES A RELIABLE MEANS OF CONTACT WITH THE SOTF (PHONE NUMBER, FAX NUMBER, OR E-MAIL ADDRESS).



Wayne Lanier
<w_lanier@pacbell.net>
10/11/2007 09:58 PM

Frank Darby Admin & Sunshine Ordinance Task Force
To MEMBERS <SOTF@sfgov.org>, Chief Administrative Officer
DTIS Ron Vinson <Ron.Vinson@sfgov.org>, ProSF
Doug Comstock <Dougcoms@aol.com>, Richard Knee
cc <rak0408@earthlink.net>, Erica Craven <elc@lrolaw.com>,
Bruce Wolfe <sotf@brucewolfe.net>, Harrison Sheppard
bcc
Subject Sunshine COMPLAINT DTIS Violation Public Records
Access

SUNSHINE ORDINANCE COMPLAINT TO SOTF

TO: Frank Darby Admin & all members of the Sunshine Ordinance Task Force <SOTF@sfgov.org>

FROM: Wayne Lanier, PhD <w_lanier@pacbell.net>

DATE: 07.10.11

RE: Sunshine Ordinance Complaint against the Department of Telecommunications and Information Services [DTIS] for Alleged violation of Public Records Access Sunshine Ordinance Sections 67.21(b); 67.21(c); 67.25(b); 67.29-7(a); and, the Allegation that violations of 67.21(b); 67.21(c); and, 67.25(b) constitute "Willful Failure to Comply" per Section 67.34

Please find attached the following Portable Data Format [PDF] documents, **constituting my Complaint:**

First Attachment DTIS NON-COMPLIANCE_070511 COMPLAINT_OF_071011.pdf = *Sunshine Ordinance Complaint* ;

Attachment-A Sunshine Request #070411 City Offices Departments.pdf = *Sunshine Request #070411 made to City Offices on April 11th, 2007* ;

Attachment-B DTIS Response delay 070416.pdf = *Letter Ron Vinson* ;

Attachment-C Courtesy Reminder Sunshine Request 070511.pdf = *Sunshine Request #070411 - Courtesy Reminder* ;

and,

Attachment-D Sunshine Request #070411 - Request_Public_Records_Promised-070923.pdf = *Sunshine Request #070411 - Request for Public Records as per your promise to deliver by April 30th, 2007* .

I should like to submit this complaint for consideration by **SOTF**, and would appreciate your placing it on your earliest convenient docket. This copy, in PDF format, has been signed electronically. It will show a question mark next to the signature when installed in your computer. Entry of my UserID+Password is necessary and sufficient to verify the signature.

I am also sending a printed copy *via* U.S. Mail.

Wayne Lanier, PhD <w_lanier@pacbell.net>



DTIS NON-COMPLIANCE_070511 COMPLAINT_OF_071011.pdf



Attachment-A Sunshine Request #070411 City Offices Departments.pdf Attachment-B DTIS Response delay 070416.pdf



Attachment-C Courtesy Reminder Sunshine Request 070411.pdf



Attachment-D Sunshine Request #070411 - Request_Public_Records_Promised-070923.pdf

SUNSHINE ORDINANCE COMPLAINT

SUNSHINE ORDINANCE TASK FORCE

1 Dr. Carlton B. Goodlett Place, Room 244

San Francisco, CA 94102

<http://www.sfgov.org/sunshine>

Complaint against the Department of Telecommunications
and Information Services [DTIS]

For Alleged violation public records access

Sunshine Ordinance Sections 67.21(b); 67.21(c); 67.25(b);
67.29-7(a); and, the charge that violations of 67.21(b);
67.21(c); and, 67.25(b) constitute "Willful Failure to
Comply" per Section 67.34.

Description of alleged violations shown on following
pages, along with citation of relevant documentation
[attached] supporting this complaint.

I wish a public hearing before the Sunshine Ordinance
Task force [YES].

Wayne Lanier, PhD

250 Ashbury, San Francisco, CA 94117

Telephone 415-346-4840

w_lanier@pacbell.net

Signature Provided electronically:



Wayne Lanier, PhD

*e-Signature verifiable
by certificate, or UserID+password.*

Digitally signed by
Wayne Lanier, PhD
Date: 2007.10.11
12:14:16 -08'00'
Reason: I am the
author of this
document
Location: 250
Ashbury, San
Francisco, CA 94117

Description of Complaint as alleged:

On April 11th, 2007, I sent Sunshine Request #070411 [Attachment-A] to Chris Vein, CIO Dept. of Telecom. & Inform. Svcs. Chris.Vein@sfgov.org as part of a survey of compliance with San Francisco City Code 67.29-7(a). Sunshine Request #070411 asked for, "... a Portable Data Format [PDF] copy of any policy, procedure, guideline, or other Controlled Instruction... used by your Office or Department to: Maintain Public Records in electronic form; Back-up such electronic records; and, Recover such electronic Public Records in event of loss of the original records." DTIS has not provided these Public Records, in violation of Section 67.21(b) of San Francisco Code.

On April 16th, 2007, I received a reply [Attachment-B] to Sunshine Request #070411 from Ron Vinson, Chief Administrative Office, DTIS. Mr. Vinson cited San Francisco Code 67.25(b) [see below] and California Code 6253(c), and asked for an extension to respond on or before April 30th, 2007. Section 67.25(b) requires response within 10-days.

I have not received any reply, or other communication from Mr. Vinson, or from any representative of DTIS since that e-mail of April 16th. DTIS has not provided the Public Records requested after a 10-day delay, indeed, after a 5-month delay, in violation of 67.21(b) and 67.25(b).

On May 9th, 2007, I sent a Courtesy Reminder [Attachment-C] to Mr. Vinson at DTIS, noting that: "Because of the critical importance to the City of maintenance, back-up, and recovery of electronic Public Records, I did not ask for an immediate response; I requested the documents by Friday, May 11th, 2007, one month after the request." In that Courtesy Reminder I observed: "The Department of Telecommunication and Information Services replied with a statement that they would comply by April 30th, 2007. No further communication nor compliance has been forthcoming." I received no response from Mr. Vinson, DTIS continued to violate 67.21(b); and, 67.25(b).

On September 23rd, 2007, I send an e-mail [Attachment-D] to Chief Administrative Officer DTIS Ron Vinson Ron.Vinson@sfgov.org, reminding him of Sunshine Request #070411 and his promise to reply by April 30th, 2007. In that e-mail, I requested that, in compliance with 67.21(c), Records Identification Responsibility of the Sunshine Ordinance, he identify that he either had no intention of complying with Sunshine Request #070411, or that he had no records responsive to Sunshine Request #070411. I

further requested that, if he had such records as requested, he identify them and arrange to provide them to me.

More than 10-days have elapsed since that e-mail of September 23rd. I have received no reply from Mr. Vinson or any other member of DTIS. By failing to identify whether DTIS has records responsive to Sunshine Request #070411, DTIS violates 67.21(c); by failing to provide the requested documents, DTIS continues to violate 67.21(b), and 67.25(b).

We have another window on DTIS compliance with San Francisco Code 67.29-7(a), "... shall maintain and preserve in a professional and businesslike manner all documents and correspondence." Sunshine Request #070411 explicitly addressed the situation of record preservation carried out by another City Department, or a consultant. Evidence produced in SOTF Complaint #07052 indicates that although the Office of the District Attorney claimed DTIS played a role in backing-up and storing electronic records off site, they were unable to produce any controlled written instructions guiding DTIS employees in this task. Assistant District Attorney Paul Henderson was pressed repeatedly, both by members of SOTF and by complainants, to provide either the DA's written instructions to employees carrying out record preservation; or other written instructions created by and used by DTIS. No such records were produced. We may presume Assistant District Attorney Henderson, or one of his assistants, queried DTIS on this matter. Their failure to produce such instructions is evidence that DTIS has no records responsive to Sunshine Request #070411. Lacking such Public Records, DTIS is in violation of San Francisco City Code 67.29-7(a). This is a more serious violation than simply failing to comply with a Sunshine Request. DTIS manages electronic records of many City entities. Losing public records through unprofessional practices places such records forever beyond Sunshine Request, and may disguise illegal destruction of public records.

San Francisco City Code section 67.34 "Willful Failure to Comply" provides no clear "triggers" by which complainants may determine when to allege that a City Office or Department willfully fails to comply. Since this is a serious charge, we turn to common sense. To demonstrate willful intent to withhold Public Records or to Identify Public Records, an Office must meet several conditions. First, either the Office must directly refuse to comply; or, fail to reply to requests over a lengthy period of time, especially with reminders, exhausting all reasonable patience. Secondly, it must be determined that the requested documents are properly Public Records. Thirdly, there must be evidence that the Department either has the requested Public Records; or, has no records

responsive to the request and fails to identify this condition upon request. Fourthly, there must be evidence that the department has intentionally pursued a strategy of obstruction and delay. These four tests demonstrate necessary conditions for allegation of "Willful Failure".

[1] Mr. Ron Vinson, DTIS Chief Administrative Officer, has failed to reply to requests over a lengthy period of more than 6-months, with two reminders, exhausting all reasonable patience. [2] Determination in Complaint #07052 has established the requested records to be Public Records. [3] Mr. Vinson has failed to provide the requested records, or to identify whether DTIS has or lacks records responsive to the request. [4] Mr. Vinson failed to respond 5-months after a requested delay, evidence that he intentionally employed Section 67.25(b) as a strategy to delay and obstruct compliance with Sunshine Request #070411. *In this Complaint, violations alleged meet the "common sense" conditions necessary for a charge under Sec. 67.34 "Willful Failure". If SOTF determines that DTIS must either produce the requested records, or must identify whether it has no records responsive, then a sufficient condition is met for SOTF to charge Mr. Vinson with violation of 67.34 "Willful Failure to Comply".*

I therefore allege that DTIS and Mr. Ron Vinson are in violation of Sunshine Ordinance Sections 67.21(b); 67.21(c); 67.25(b); 67.29-7(a); and allege that the violations of 67.21(b); 67.21(c); and, 67.25(b) constitute "Willful Failure" under Section 67.34.

Attachments to this Complaint are listed below:

Attachment-A Sunshine Request #070411 City Offices Departments.pdf *TITLE = Sunshine Request #070411 made to City Offices on April 11th, 2007.*

Attachment-B DTIS Response delay 070416.pdf *No TITLE = letter Ron Vinson*

Attachment-C Courtesy Reminder Sunshine Request 070411.pdf *TITLE = Sunshine Request #070411 - Courtesy Reminder*

Attachment-D Sunshine Request 070411 - Request Public Records Promised-070923.pdf *TITLE = Sunshine Request #070411 - Request for Public Records as per your promise to deliver by April 30th, 2007.*

ATTACHMENT #A

Gavin.Newsom@sfgov.org, Trent.Rhorer@sfgov.org, Mitch.Katz@sfgov.org, General.Manager@sfwater.org, Di

To: Gavin.Newsom@sfgov.org, Trent.Rhorer@sfgov.org, Mitch.Katz@sfgov.org, General.Manager@sfwater.org, DistrictAttorney@sfgov.org, City.Administrator@sfgov.org, Yomi.Agunbiade@sfgov.org, Chris.Vein@sfgov.org, Aaron.Peskin@sfgov.org

From: Wayne Lanier <w_lanier@pacbell.net>

Subject: Sunshine Request #070411 made to City Offices and Departments on April 11th, 2007

Cc: ProSF <home@prosf.org>, Christian Holmer <mail@csrsf.com>

Bcc:

Attached: D:\POLITICS\SunshineFiles\Sunshine Request #070411 City Offices Departments.pdf;

TO: [1] Mayor Gavin Newsom <Gavin.Newsom@sfgov.org>
[2] Trent Rhorer, Director Department of Human Services <Trent.Rhorer@sfgov.org>
[3] Dr. Mitch Katz, Director Public Health Department <Mitch.Katz@sfgov.org>
[4] Susan Leal, Director Public Utilities Department <General.Manager@sfwater.org>
[5] Kamala D. Harris, District Attorney <DistrictAttorney@sfgov.org>
[6] Ed Lee, City Administrator <City.Administrator@sfgov.org>
[7] Yomi Agunbiade, Director Recreation & Parks Department <Yomi.Agunbiade@sfgov.org>
[8] Chris Vein, CIO Dept. of Telecom. & Inform. Svcs. <Chris.Vein@sfgov.org>
[9] Supervisor Aaron Peskin, President Board of Supervisors <Aaron.Peskin@sfgov.org>
FROM: Wayne Lanier, PhD <w_lanier@pacbell.net>
DATE: April 11th, 2007
RE: Sunshine Request #070411 made to City Offices and Departments

This is a Sunshine Request for Public Documents *per* Article I Section 3b: *California Constitution* and Chapter 67: *San Francisco Sunshine Ordinance*.

67.29-7(a) of the San Francisco Sunshine Ordinance states:

"The Mayor and all Department Heads shall maintain and preserve in a professional and businesslike manner all documents and correspondence, including but not limited to letters, e-mails, drafts, memorandum, invoices, reports and proposals and shall disclose all such records in accordance with this ordinance."

I am performing an audit for publication of selected City Offices and Departments to determine how this requirement for record maintenance has been implemented for *electronic* Public Records.

Please [Reply] to this e-mail by Friday, May 11th, 2007, attaching a Portable Document Format [PDF] copy of any procedure, policy, guideline, SOP, or other controlled instruction [herein called "procedure"] used by your Office or Department to:

- Maintain Public Records in electronic form;
- Back-up such electronic Public Records; and,
- Recover such back-up electronic Public Records in event of loss of the original records.

If you maintain a *controlled copy* of the requested document(s) in paper form with a *handwritten signature* and *date*, please so indicate in your [Reply] e-mail, noting the name of the person who approved the procedure and the date of approval, and attaching an electronic PDF copy of the native document as requested.

If your Office or Department employs electronic signatures, printing to PDF will watermark the PDF copy with a "controlled-document" statement that only the original version is valid. Sending me this watermarked version as an attachment to your [Reply] e-mail will comply with my request.

If your Office or Department meets the requirement using *approved* printed books, booklets, manuals, or similar lengthy documents, please indicate this in your [Reply] e-mail, provide the exact title and date of printing of each the documents, and attach a PDF copy of the policy letter or other instrument through which your Office or Department documented approval.

If you do not have a any procedure addressing one or more of the requested topics, please indicate this in your [Reply] e-mail.

If you do have such procedures, but for technical reasons cannot comply in the specific manner requested, please describe the problem in a [Reply] e-mail and we will work out a way around the technical impediment.

If I have not received by May 11th, 2007, a [Reply] e-mail in one of the forms described above, I will assume you do not intend to comply with this Sunshine Request.

If you have any questions regarding the meaning of any of the terms of this Sunshine Request, please see my e-mail to your Office or Department of April 9th, 2007, entitled Control, Maintain, Back-up, and Recover Electronic Records.

Thank you,
Wayne Lanier, PhD

ATTACHMENT-B

X-Apparently-To: w_lanier@pacbell.net via 69.147.64.48; Mon, 16 Apr 2007 09:57:43 -0700
X-Originating-IP: [209.77.149.27]
Authentication-Results: mta147.sbc.mail.mud.yahoo.com from=sfgov.org; domainkeys=neutral (no sig)
X-Originating-IP: [209.77.149.27]
To: w_lanier@pacbell.net
Cc: Barry Fraser <Barry.Fraser@sfgov.org>, Thomas Long <Thomas.Long@sfgov.org>
Subject: Re: Fw: [Suspected Spam]Sunshine Request #070411 made to City Offices and Departments on April 11th, 2007
X-Mailer: Lotus Notes Release 6.5.4 March 27, 2005
From: Ron Vinson <Ron.Vinson@sfgov.org>
Date: Mon, 16 Apr 2007 09:56:43 -0700
X-MIMETrack: S/MIME Sign by Notes Client on Ron Vinson/DTIS/SFGOV(Release 6.5.4|March 27, 2005) at
04/16/2007 09:58:20 AM,
Serialize by Notes Client on Ron Vinson/DTIS/SFGOV(Release 6.5.4|March 27, 2005) at
04/16/2007 09:58:20 AM,
Serialize complete at 04/16/2007 09:58:20 AM,
S/MIME Sign failed at 04/16/2007 09:58:20 AM: The cryptographic key was not found,
Serialize by Router on InH01a01/SFGOV(Release 6.5.4|March 27, 2005) at 04/16/2007 09:57:45

Dear Mr. Lanier:

In order to properly respond to your Request, DTIS requires additional time in order to consult with another interested department or departments. In accordance with San Francisco Administrative Code Section 67.25(b) and California Government Code Section 6253(c), DTIS will respond on or before April 30, 2007.

Ron Vinson
Chief Administrative Officer
DTIS
(415) 554-0803 - office
(415) 554-4733 - fax

Sabina Crivello/DTIS/SFGOV

04/11/2007 02:30 PM

To: Ron Vinson/DTIS/SFGOV@SFGOV

cc

Subject: Fw: [Suspected Spam]Sunshine Request #070411 made to City Offices and Departments on April 11th, 2007

Ron,

As promised, this is the soft copy of the hard copy in your inbox.

Sabina

----- Forwarded by Sabina Crivello/DTIS/SFGOV on 04/11/2007 02:28 PM -----

Chris Vein/DTIS/SFGOV

To Sabina Crivello/DTIS/SFGOV@SFGOV

cc

04/11/2007 12:18 PM

Subject Fw: [Suspected Spam]Sunshine Request #070411 made to City Offices and Departments on April 11th, 2007

----- Forwarded by Chris Vein/DTIS/SFGOV on 04/11/2007 12:18 PM -----

Wayne Lanier <w_lanier@pacbell.net>

Gavin.Newsom@sfgov.org, Trent.Rhorer@sfgov.org, Mitch.Katz@sfgov.org,
General.Manager@sfgov.org, DistrictAttorney@sfgov.org,
To City.Administrator@sfgov.org, Yomi.Agunbiade@sfgov.org, Chris.Vein@sfgov.org,
Aaron.Peskin@sfgov.org

04/11/2007 12:15 AM

cc ProSF <home@prosf.org>, Christian Holmer <mail@csrsf.com>
Subject [Suspected Spam]Sunshine Request #070411 made to City Offices and Departments on April 11th, 2007

TO: [1] Mayor Gavin Newsom <Gavin.Newsom@sfgov.org>
[2] Trent Rhorer, Director Department of Human Services <Trent.Rhorer@sfgov.org>
[3] Dr. Mitch Katz, Director Public Health Department <Mitch.Katz@sfgov.org>
[4] Susan Leal, Director Public Utilities Department <General.Manager@sfgov.org>
[5] Kamala D. Harris, District Attorney <DistrictAttorney@sfgov.org>
[6] Ed Lee, City Administrator <City.Administrator@sfgov.org>
[7] Yomi Agunbiade, Director Recreation & Parks Department <Yomi.Agunbiade@sfgov.org>
[8] Chris Vein, CIO Dept. of Telecom. & Inform. Svcs. <Chris.Vein@sfgov.org>
[9] Supervisor Aaron Peskin, President Board of Supervisors <Aaron.Peskin@sfgov.org>
FROM: Wayne Lanier, PhD <w_lanier@pacbell.net>
DATE: April 11th, 2007
RE: Sunshine Request #070411 made to City Offices and Departments

This is a Sunshine Request for Public Documents *per* Article I Section 3b: *California Constitution* and Chapter 67: *San Francisco Sunshine Ordinance*.

67.29-7(a) of the San Francisco Sunshine Ordinance states:

"The Mayor and all Department Heads shall maintain and preserve in a professional and businesslike manner all documents and correspondence, including but not limited to letters, e-mails, drafts, memorandum, invoices, reports and proposals and shall disclose all such records in accordance with this ordinance."

I am performing an audit for publication of selected City Offices and Departments to determine how this requirement for record maintenance has been implemented for *electronic* Public Records.

Please [Reply] to this e-mail by Friday, May 11th, 2007, attaching a Portable Document Format [PDF] copy of any procedure, policy, guideline, SOP, or other controlled instruction [herein called "procedure"] used by your Office or Department to:

Gavin.Newsom@sfgov.org, Trent.Rhorer@sfgov.org, Mitch.Katz@sfgov.org, General.Manager@sfgwater.org, Di

To: Gavin.Newsom@sfgov.org, Trent.Rhorer@sfgov.org, Mitch.Katz@sfgov.org, General.Manager@sfgwater.org, DistrictAttorney@sfgov.org, City.Administrator@sfgov.org, Yomi.Agunbiade@sfgov.org, Ron.Vinson@sfgov.org, Aaron.Peskin@sfgov.orgProSF
 From: Wayne Lanier <w_lanier@pacbell.net>
 Subject: Sunshine Request #070411 - Courtesy Reminder
 Cc: <home@prosf.org>, Christian Holmer <mail@csrsf.com>, Amanda Witherell <Amanda@sfbg.com>, Erica L. Craven <elc@lrolaw.com>, Erica L. Craven et al <SOTF@sfgov.org>
 Bcc:
 Attached: D:\POLITICS\SunshineFiles\Sunshine Request #070411 D:\POLITICS\SunshineFiles\Courtesy Reminder Sunshine Request 070411.pdf; City Offices Departments.pdf;

TO: [1] Mayor Gavin Newsom <Gavin.Newsom@sfgov.org>
 [2] Trent Rhorer, Director Department of Human Services <Trent.Rhorer@sfgov.org>
 [3] Dr. Mitch Katz, Director Public Health Department <Mitch.Katz@sfgov.org>
 [4] Susan Leal, Director Public Utilities Department <General.Manager@sfgwater.org>
 [5] Kamala D. Harris, District Attorney <DistrictAttorney@sfgov.org>
 [6] Ed Lee, City Administrator <City.Administrator@sfgov.org>
 [7] Yomi Agunbiade, Director Recreation & Parks Department <Yomi.Agunbiade@sfgov.org>
 [8] Ron Vinson, CAO Dept. of Telecom. & Inform. Svcs. <Ron.Vinson@sfgov.org>
 [9] Supervisor Aaron Peskin, President Board of Supervisors <Aaron.Peskin@sfgov.org>
 FROM: Wayne Lanier, PhD <w_lanier@pacbell.net>
 DATE: May 9th, 2007
 RE: Courtesy Reminder regarding
 Sunshine Request #070411 made to City Offices and Departments

This is a courtesy reminder. Sunshine Request #070411 [attached in PDF format] was sent to your office on April 11th, 2007. Because of the critical importance to the City of maintenance, back-up, and recovery of electronic Public Records, I did not ask for an immediate response; I requested the documents by Friday, May 11th, 2007, one month after the request. My purpose was to provide City Departments with reasonable time to resolve any questions arising from my request. I also provided for technical problems and for dealing with documents in forms not conveniently sent by e-mail attachment.

The San Francisco Public Utilities Commission has complied with my request. Thank you.

The Department of Human Services stated in an e-mail dated April 16th, 2007, that "The Human Services Agency has an extensive and sophisticated system in place for all data maintenance and recovery in the event of a major disaster, including an earthquake." No documents were enclosed, however. No further communication or compliance has been forthcoming.

✓ The Department of Telecommunication and Information Services replied with a statement that they would comply by April 1, 2007. No further communication nor compliance has been forthcoming.

The City Administrator's Office directed me to the General Services Index, apparently an index to paper documents [no distinction was made between electronic and paper documents in the index]. Few, if any, of the many documents listed and generically described were stored off site. None appeared to address

electronic document back-up and recovery. The Office then stated: "To the best of our knowledge, the Department has no other documents responsive to your request."

The Recreation and Parks Department responded with several e-mails addressing matters not part of Sunshine Request #070411, including sending a document that had no bearing on the back-up, storage, or recovery of electronic Public Records. Reiteration and explanation of Sunshine Request #070411 finally resulted in the statement: "The Department does not possess any other document that is as you describe beyond the document we already sent."

The Office of the Mayor and the remaining City Departments have neither replied to, nor complied with Sunshine Request #070411.

A PDF copy of this e-mail is attached.

Wayne Lanier, PhD
<w_lanier@pacbell.net>

Attachment - D

Chief Administrative Officer DTIS Ron Vinson, 9/23/2007 01:47 PM -0700, Sunshine Request #070411 - Re

To: Chief Administrative Officer DTIS Ron Vinson <Ron.Vinson@sfgov.org>
From: Wayne Lanier <w_lanier@pacbell.net>
Subject: Sunshine Request #070411 - Request for Public Records, as promised
Cc: Sunshine Ordinance Task Force <soff@sfgov.org>, ProSF <home@prosf.org>
Bcc:
Attached: D:\POLITICS\SunshineFiles\Sunshine Request #070411 City Offices Departments.pdf;
D:\POLITICS\SunshineFiles\Response Documents\DTIS Response delay 070416.pdf;
D:\POLITICS\SunshineFiles\DTIS\Sunshine Request #070411 - Request_Public_Records_Promised-070923.pdf;

TO: Chief Administrative Officer DTIS Ron Vinson <Ron.Vinson@sfgov.org>
FROM: Wayne Lanier, PhD
DATE: September 23rd, 2007
RE: Sunshine Request #070411 - Request for Public Records, as per your promise to deliver by April 30th, 2007.

Dear Chief Administrative Officer Vinson,

On April 11th, I requested of nine Departments or Offices of the City and County of San Francisco, including DTIS, any procedure, policy, guideline, SOP, or other controlled written instruction guiding how your Department carries out the tasks: Maintain Public Records in electronic form; Back-up such electronic Public Records; and, Recover such back-up electronic Public Records in event of loss of the original records. [See Attachment #1.]

In response, you replied by e-mail that you would respond by April 30th, 2007. I have received no further response since that e-mail. [See Attachment #2.]

Given the length of elapsed time, I must either assume you have no intention of responding to me, or you have no records responsive to my request.

I am writing today to verify that either one or the other assumption is a correct and true description of record keeping at DTIS, of which you are the Chief Administrative Officer.

Such verification is important for several reasons:

If you intend to refuse to comply with Sunshine Request #070411, I need to verify this as a specific refusal to comply.

If you have failed to comply because you have no records responsive to my request, I need to know this because section 67.29-7(a) of the San Francisco Code *Sunshine Ordinance* states: "The Mayor and all Department Heads shall maintain and preserve in a professional and businesslike manner all documents and correspondence, including but not limited to letters, e-mails, drafts, memorandum, invoices, reports and proposals and shall disclose all such records in accordance with this ordinance."

As the Chief Administrative Office of DTIS, you are the Department Head and, therefore, directly and personally responsible for ensuring that the task of preservation of Public Records, including electronic

Public Records, is carried out in a professional and businesslike manner. Failure to ensure this task of preservation is carried out is a violation of San Francisco Code, Section section 67.29-7(a).

Furthermore, DTIS, unlike other City Departments, has a unique responsibility for preservation of electronic records. Employees of DTIS may be responsible for carrying out for some other City Departments the tasks of server maintenance, server drive back-up, storage of server drive back-ups at an off-site location, and recovery and validated reinstallation of such server drive back-ups in the event of disaster or other loss. It is a serious issue if DTIS is operating without authorized procedures or other controlled written instructions.

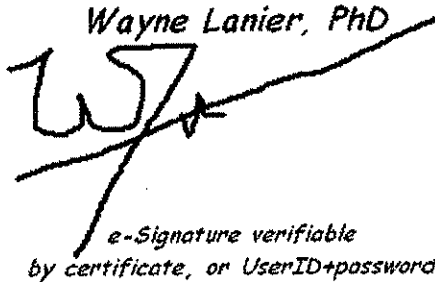
So, I again request that you identify and provide to me any controlled written instructions guiding the preservation of electronic Public Records received, created, or maintained by DTIS, by means of the commonly-accepted professional practice of backing-up such electronic Public Records, storing such electronic back-ups off site, and recovering such electronic Public Records in the event of disaster or other loss. If you do not have such controlled written instructions as described, I request that you verify that your Department has no record responsive to my request as part of the Public Record identification responsibility of the San Francisco Sunshine Ordinance.

Thank you,

[A PDF copy of this e-mail is attached as #3]

Wayne Lanier, PhD <w_lanier@pacbell.net>



Wayne Lanier, PhD

e-Signature verifiable
by certificate, or UserID+password.

Digitally signed by
Wayne Lanier, PhD
Date: 2007.09.23
12:49:02 -08'00'
Reason: I am the
author of this document
Location: 250 Ashbury,
San Francisco, CA
94117



SOTF/SOTF/SFGOV

10/24/2007 09:10 AM

To w_lanier@pacbell.net

cc

bcc

Subject Complaint Received re: DTIS

Mr. Lanier,

This is to confirm receipt of your complaint. Attached is the official Sunshine Ordinance Task Force complaint form that I have completed for your review. Please review the form for accuracy, make any necessary corrections then sign and return it to me via e-mail or fax. Once I receive the signed form your complaint will be, assigned a file number, and you will be notified that a hearing has been scheduled with the Complaint Committee and the full Task Force in November.



W/Lanier Complaint.pdf

If you prefer, you can also complete and submit your complaint on line by going to the following link.

http://www.sfgov.org/site/sunshine_form.asp?id=18564

Frank Darby, Administrator
Sunshine Ordinance Task Force
1 Dr. Carlton B. Goodlett Place
City Hall, Room 244
San Francisco, CA 94102-4689
SOTF@SFGov.org
OFC: (415) 554-7724
FAX: (415) 554-7854



Wayne Lanier
<w_lanier@pacbell.net>
10/25/2007 12:56 AM

To SOTF <sotf@sfgov.org>
Doug Comstock <Dougcoms@aol.com>, Richard Knee
cc <rak0408@earthlink.net>, Erica Craven <elc@lrolaw.com>,
Bruce Wolfe <sotf@brucewolfe.net>, Harrison Sheppard
bcc
Subject Re: Complaint Received re: DTIS

History:  This message has been replied to.

Mr. Frank Darby, Administrator SOTF,

I am somewhat puzzled by your e-mail to me, appended below.

I sent you a courteously-written **Sunshine Complaint**, both by e-mail and by US Mail [printed on paper]. Both versions were signed. I followed exactly your form, as shown in your "electronic" submission [which does not permit a copy and was designed for the convenience of the programmer, not the user]; and, as shown in the photocopied paper form which I used as template. I captured exactly the information requested, in the sequence and language requested. I did not fill out the photocopied paper form because that would have either required a typewriter, which I do not have, or a hand-written document, which would have been more difficult for you to read and considerably more effort for me write.

You have returned to me a PDF version you filled out, showing my name differently, changing the detail of my complaint, and stripping it of its continuation sheet and the information recorded thereon. You, in effect, are now requesting me to repeat my entire complaint, in your style, for purposes not at all clear to me.

My understanding of the Sunshine Ordinance and of the role of SOTF is that the author of the Ordinance intended any reasonable complaint to be accepted, to be heard, and its validity to be determined, even were it written on a school child's lined Indian Tablet paper in pencil. The validity of a Sunshine Complaint does not rigidly reside in a photocopied form bearing the City seal.

My complaint was not a casual afterthought. It was not the result of a thoughtless motive, incompletely realized. It was not the raving of a semiliterate buffoon, bent on harassing the City, or the SOTF. It was a carefully written document, addressing a serious issue in this City, following your form, putting forth the facts of my complaint, and signed electronically.

It is difficult for me to believe SOTF is so rigid that identical information, absent an image of the City seal, fails to constitute a valid complaint.

There is, however, another issue in this matter that may make your e-mail, whatever its intent, moot.

When I originally filed the Sunshine Complaint you received, in its offending format, I also provided a copy to Mr. Ron Vinson, Executive Officer of DTIS. That was simply a courtesy, I did not expect a response.

Some days later, as a result of my complaint, I was contacted by DTIS Analyst Mr. Barry Fraser and CEO Mr. Ron Vinson. In the course of a long telephone call, Mr. Vinson agreed to send me the two Public Records requested in Sunshine Request #070411.

A few days after the telephone call, I received from Mr. Barry Fraser, the second of the Public Records I had requested in Sunshine Request #070411 [Recovery upon Disaster]. I read it, finding that Mr. Fraser had redacted every employee name or title and every telephone number in the record [without indicating the redactions].

I wrote back, noting such wide-scale redaction went well beyond the letter or spirit of Chapter 67, or, indeed, the Sunshine Amendment to the California Constitution. It also made the document very difficult to read, or to interpret. As might be imagined, Disaster Recovery depends upon rapid and accurate networking under very difficult circumstances. I also point out that Mr. Fraser had failed to send the first Public Record requested.

Coincidentally with your e-mail, I received another e-mail from Mr. Fraser. Attached to that e-mail was the first of the Public Records I requested in Sunshine Request #070411 [Back-up procedure]. I have not had time to examine it yet.

This is where things stand at the moment.

I am not certain whether DTIS has actually attempted to comply with Sunshine Request #070411, or is simply spinning things out by sending me documents fractured by massive redactions. I have not read the second document sent. I am disturbed by the massive redaction of what I understand to be City employee names, the titles of City employees, City office telephone numbers, and even, in one instance, what may have been the emergency telephone number 911.

Your e-mail does not help this decision process. I had thought to carefully study the Public Records sent to me, satisfy myself whether these redacted Public Records represented proper compliance, and either continue with my Complaint or withdraw the Complaint. The purpose in continuing the Complaint would be to resolve the issue of massive redaction, since DTIS has clearly sent me records, whether I can make sense of them, or not. I took Mr. Harrison Sheppard's memorandum to SOTF at its face value - that instruction about and interpretation of Chapter 67 constitutes a pivotal role of SOTF.

I have copied this e-mail response to various members of SOTF and I request you put the issue before them. I have no interest in wasting their time or my own time on *pro forma* matters.

Wayne Lanier, PhD



SOTF/SOTF/SFGOV

10/25/2007 09:17 AM

To Wayne Lanier <w_lanier@pacbell.net>

Doug Comstock <Dougcoms@aol.com>, Erica Craven
cc <elc@lrolaw.com>, Harrison Sheppard <hjslaw@jps.net>,
Kristin Chu <kristin@chu.com>, Richard Knee
bcc Ernest.Ilorente@sfgov.org

Subject Re: Complaint Received re: DTIS

Mr. Lanier,

The complaint form that I provided to you in no way negates or diminishes the complaint letter or support documents that you submitted. The form provides a consistent format and a summary of your complaint to assist Members of the Task Force and the Deputy City Attorney, and will not replace the documents that you submitted. Also, please note that the form was sent to you in compliance with the Task Force's complaint procedures (attached).



1_Complaint Procedures_rev 5-22-07_Final.pdf

Subsection B.1 of the procedures, in part, says "A letter or complaint form may be submitted to the SOTF via mail, fax or electronic mail (email) or in person. If a complaint letter is received, the Administrator shall complete a complaint form and send a copy to the complainant.

The complaint form was sent in keeping with these procedures. If the description of the violation that I identified is incorrect I will gladly make the corrections.

Frank Darby, Administrator
Sunshine Ordinance Task Force
1 Dr. Carlton B. Goodlett Place
City Hall, Room 244
San Francisco, CA 94102-4689
SOTF@SFGov.org
OFC: (415) 554-7724
FAX: (415) 554-7854



SOTF/SOTF/SFGOV

10/30/2007 08:38 AM

To w_lanier@pacbell.net, Ron Vinson/DTIS/SFGOV@SFGOV

cc

scau1321@aol.com; sotf@brucewolfe.net;
bcc Ernest.Illoriente@sfgov.org; nicksf94114@yahoo.com;
Kristin@Chu.com

Subject Sunshine Complaint Received: #07082_Wayne Lanier vs
DTIS

This e-mail is to confirm that the following/attached complaint and support documents has been received. The Department is required to submit a response to the charges to the Task Force within five business days of receipt of this notice. Please refer to complaint number #07082 when submitting any new information and/or supporting documents pertaining to this complaint.



W/Lanier Complaint.pdf

A hearing is scheduled with the Complaint Committee of the Sunshine Ordinance Task Force who will determine whether the Task Force has jurisdiction over this matter, and to clarify the complaint.

Date: Tuesday, November 13, 2007

Location: City Hall, Room 406

Time: 4:00 P.M.

Any support documents to be considered by committee members, prior to the meeting, must be submitted by 4:00 P.M. Monday, November 5, 2007

Also, attached is the Sunshine Ordinance Task Forces complaint process.



Complaint Process.pdf

Frank Darby, Administrator
Sunshine Ordinance Task Force
1 Dr. Carlton B. Goodlett Place
City Hall, Room 244
San Francisco, CA 94102-4689
SOTF@SFGov.org
OFC: (415) 554-7724



Wayne Lanier
<w_lanier@pacbell.net>
10/30/2007 12:49 PM

To SOTF <sotf@sfgov.org>
cc
bcc
Subject Re: Sunshine Complaint Received: #07082_Wayne Lanier
vs DTIS

Good morning, SOTF Administrator Frank Darby,

I received the e-mail attached below this morning. I cannot open the last file [showing some sort of Microsoft flag] with file name: "Attachment-D Sunshine Request #070411 - Request_Public_Records_Promised1". Apparently my computer does not have the required executable software. I tend to avoid Microsoft whenever possible. Such a problem is why I normally request PDF files. Please clarify this issue for me.

Unexpectedly, DTIS telephoned me. I suspect their call, breaking five months of silence, was motivated by the possibility of "Willful failure to comply" as one of the complaint issues.

For whatever reason, they apologized for the long silence. We reached what I thought was an agreement for them to supply the files requested in #070411.

During the weeks prior to today, they have, *via* two different e-mail attachments, supplied three files, nominally addressing Request #070411.

One of these files [having to do with their Disaster Recovery Plan] has been so heavily redacted that I have difficulty determining whether it addresses the issue for which I requested records. The redaction are not identified [as required by Chapter 67], but apparently include every name and title of any person or DTIS employee mentioned in the record [in apparent violation of Chapter 67], as well as every telephone number mentioned in the record [also in apparent violation of Chapter 67].

I have informed DTIS about the problem of excessive redaction and unidentified redactions, but they have not sent an un-redacted copy of the record or invoked any reasons for redaction compliant with Chapter 67. What is not clear to me is whether DTIS is simply misinformed about redactions permitted under Chapter 67, or whether this is further obstruction. I explicitly told DTIS that, if the records sent appeared to be responsible to Request #070411, I would withdraw the Complaint. ***The part of their Disaster Plan that they sent is questionable, and I am presently uncertain whether it is made meaningless by excessive redactions .***

Once you informed me of the requirement for use of your special paper form, I concluded a delay might enable me to resolve the issues of compliance and redaction. I gather you have circumvented the requirement for the special paper form, and a Complaint #07082 now stands.

Today is Tuesday, 10/30/2007 by your notation. I will explicitly address the problematic record within five business days.

Regards,
Wayne Lanier, PhD



Wayne Lanier
<w_lanier@pacbell.net>
11/01/2007 10:38 AM

To Sunshine Ordinance Task Force MEMBERS
<SOTF@sfgov.org>
Richard Knee <rak0408@earthlink.net>, Erica Craven
cc <elc@lrolaw.com>, Doug Comstock <Dougcoms@aol.com>,
Ron Vinson <Ron.Vinson@sfgov.org>, Bruce Wolfe
bcc
Subject Document Supporting Complaint #07082

SOTF Administrator Frank Darby,

Please find attached to this e-mail a PDF Document Supporting Complaint #07082, before the Sunshine Ordinance Task Force. Please place this PDF document in the SOTF record and provide a copy to each member of SOTF.

Thank you,



Wayne Lanier, PhD <w_lanier@pacbell.net> Response SOTF 07082 on 071101.pdf

November 1, 2007

Wayne Lanier, PhD, to SOTF

RE: SUNSHINE COMPLAINT #07082 WAYNE LANIER VS DTIS

Sunshine Complaint #07082 was originally brought before the Sunshine Ordinance Task Force [SOTF] because the San Francisco Department of Telecommunications and Information Services [DTIS] failed to comply with Sunshine Request #070411. For almost 6-months, DTIS failed to respond to courteous reminders.

Shortly after filing #07082, I was contacted by DTIS and held a lengthy telephone conversation with CEO Ron Vinson and Policy Analyst Barry Fraser. They explained that DTIS Disaster Recovery Plan ran to more than 1,000-pages in length. Based on further discussion, I agreed to accept and they subsequently provided the following documents: DTIS Disaster Recovery Plan TOC; Part 1 of DTIS Disaster Recovery Plan; and, Service Level Agreement [for record backup]. I agreed to withdraw the complaint if the records provided were responsive my original request #070411.

Nominally by title, the records provided should have been responsive to Sunshine Request #070411. In fact, I found one had been made "not responsive".

In the copy of Part 1 DTIS Disaster Plan supplied, every title, name, telephone number, system designation, and identifier had been redacted. No redaction was identified or marked on the copy, no reason was given for redaction, and no citation to Chapter 67 was provided.

The best analogy I can draw is to a payment/receivables record in which the persons paid, the amounts paid, the persons paying, and the amounts received had all been redacted. In short, audit of the copy of Part 1 DTIS Disaster Plan supplied was not feasible, post redaction.

The object of Sunshine Request #070411 was to verify and audit the written instructions for back-up, storage, and recovery of electronic Public Records in the event of a disaster. The most comprehensive and important of the Public Records supplied was massively redacted in ways not in compliance with Chapter 67. This converted a Public Record that, whole, would have been responsive, into a skeleton of the Public Record and not responsive. DTIS has not complied with Sunshine Request #070411 and Complaint #07082 is not withdrawn.



Wayne Lanier
<w_lanier@pacbell.net>
11/01/2007 10:21 PM

To Sunshine Ordinance Task Force MEMBERS
<SOTF@sfgov.org>
cc Ron Vinson <Ron.Vinson@sfgov.org>
bcc
Subject City Attorney Ruling Supporting Complaint #07082

SOTF Administrator Frank Darby,

Please find attached to this e-mail a PDF Document from the Office of the City Attorney supporting and clarifying Complaint #07082, now before the Sunshine Ordinance Task Force. Please place this PDF document in the SOTF record and provide a copy to each member of SOTF.

Thank you,



Wayne Lanier, PhD <w_lanier@pacbell.net> City_Attorney_Rule_Disaster_Plan_Redaction_060915.pdf



DENNIS J. HERRERA
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.



Wayne Lanier
<w_lanier@pacbell.net>
11/02/2007 09:49 AM

To Sunshine Ordinance Task Force MEMBERS
<SOTF@sfgov.org>, ProSF <home@prosf.org>
cc Ron Vinson CEO DTIS <Ron.Vinson@sfgov.org>
bcc
Subject In the matter of Complaint #07082 Lanier v DTIS

SOTF Administrator Frank Darby,

Please provide a copy of this e-mail to each SOTF member...

On November 1, 2007, I placed before the Sunshine Ordinance Task Force a PDF copy of a Memorandum by Linda M. Ross, General Counsel Mayor's Office, entitled *Guidelines for Redacting Information from Plans Created by the City To Anticipate and Respond to Emergencies Created by Terrorists or Other Criminal Activity* .

This Guideline applies directly to the matter of Complaint #07082 Wayne Lanier, PhD, versus Department of Telecommunications and Information Services [DTIS].

In April of 2007, I sent Sunshine Request #070411 to DTIS. I requested DTIS written instructions guiding the back-up, storage, and recovery of electronic public records in the event of disaster or other loss.

DTIS CEO Ron Vinson sent me a brief note asking for more time. He did not reply further, even in the face of a courteous reminder and, subsequently, a much stronger reminder many months later.

Recently I filed the Complaint now designated #07082. In that Complaint I listed violations of Sunshine Ordinance Sections 67.21(b); 67.21(c); 67.25(b); 67.29-7(a); and, the charge that violations of 67.21(b); 67.21(c); and, 67.25(b); triggered "Willful Failure to Comply" per Section 67.34. I copied the complaint documents to DTIS.

Very quickly after I filed the complaint, DTIS CEO Vinson contacted me and we had a lengthy conversation. He courteously apologized for the long delay in contacting me and stated willingness to comply with my request. We discussed ways that DTIS might comply. One problem was that the DTIS Disaster Plan, which presumably responded to the matter of recovering electronic public records post disaster, was over 1,000-pages long!

To resolve this issue, I agreed to receive and examine the DTIS Disaster Plan table of contents and Part 1, much shorter components of the larger document. After some misunderstanding, I also requested and was sent a document addressing the "back-up" of public records. **I told DTIS CEO Vinson that I would drop the complaint if the records sent to me were responsive to my original request.**

I found the copy sent to me of Part 1 of the DTIS Disaster Plan was not responsive. This was because that copy had been so massively redacted that I could not realistically audit its content. For explanation, I have compared the matter to a *payment/receivables document in which all names and amounts of money have been deleted* .

With such redaction of a supplied Public Record, Complaint #07082 stands.

We have precedent, however, to resolve the matter. The Memorandum from the General Counsel of the Mayor's Office does, indeed, provide clear guidelines. The first is that **a Disaster Plan is a public record**, subject to public scrutiny. The second is that **all redactions must be clearly indicated and explained fully**, the burden resting on the Department to defend redaction. The third is that redaction is permitted only to preserve clearly-defined security.

I have underlined parts of the third "guideline" for a reason. We have seen in the present presidential administration a trend of enlarging "security", with a vague nod and wave of the hand, to encompass virtually every "bit" of information. The Memorandum is clear on this matter: Security reasons for redactions must be realistic, they must be compelling, they must be clearly defined and explained. San Francisco City and County is not the Bush administration!

I urge SOTF Members to require DTIS CEO Ron Vinson to reexamine Part 1 of the DTIS Disaster Plan in the light of the Memorandum, carefully indicating each redaction and explaining for each redaction, including appropriate citation, why such redaction is necessary to preserve City security and compliant with both Chapter 67 and the Memorandum.

I have not attempted to argue against any redactions in the document sent to me. As the Memorandum makes clear, **defense of redaction is a DTIS responsibility**. City Offices have repeatedly embarked on such time-consuming and improper redaction, while claiming that requesters put them to great trouble and waste of time. This is a specious charge.

I also urge members of SOTF to examine a wider issue. Member Sheppard has written compassionately of City Officers facing charges under Sec. 67.34 of the Code. Because this is a serious charge, in Complaint #07082, as originally written, I listed four tests necessary for a charge under Sec. 67.34.

San Francisco City Code section 67.34 "Willful Failure to Comply" provides no clear "triggers" by which complainants may determine when to allege that a City Office or Department willfully fails to comply. Since this is a serious charge, we turn to common sense. To demonstrate willful intent to withhold Public Records or to Identify Public Records, an Office must meet several conditions. First, either the Office must directly refuse to comply; or, fail to reply to requests over a lengthy period of time, especially with reminders, exhausting all reasonable patience. Secondly, it must be determined that the requested documents are properly Public Records. Thirdly, there must be evidence that the Department either has the requested Public Records; or, has no records responsive to the request and fails to identify this condition upon request. Fourthly, there must be evidence that the department has intentionally pursued a strategy of obstruction and delay. These four tests demonstrate necessary conditions for allegation of "Willful Failure".

At the time I wrote the inset paragraph above, I had not encountered a second way Offices may fail to comply with a Sunshine Request and pursue a strategy of obstruction: **By supplying a document so massively redacted as to be meaningless**. In the course of preparation for the upcoming hearing, I have run across numerous other instances where long delays were first used to avoid compliance with requests; then, as a last resort, records supplied were redacted to the point of uselessness.

Let me be very clear. **DTIS Officers have been courteous when dealing with me when they did respond and have stated a willingness to comply**. At issue is whether this courteousness and stated willingness to comply has masked *accidental* , or *intentional* failure to comply with a simple Sunshine Request made under Chapter 67.

Wayne Lanier, PhD <w_lanier@pacbell.net>