

PILOT
 LCI/CONT LCs
 OSA INT/CONTS
 SNR HCO INT/CONTS
 LCs
 HCOs
 DSAs

SECURITY SITUATION HANDLING CHECKLISTS

Refs:	
HCO PL 16 Dec 68	SECURITY DIV 1
HCO PL 23 Jan 59	ETHICS
HCO PL 21 Apr 70	FIELD ETHICS
HCO PL 1 Sept 69R	COUNTER ESPIONAGE
FO 1664	DIVISIONAL PRIMARY FUNCTIONS
SPD 2 Oct 88	ORGANIZATIONAL SECURITY
HCO PL 30 Oct 62	SECURITY RISKS INFILTRATION
HCO PL 23 Nov 59	EMPLOYMENT OF CRIMINALS
	FORBIDDEN
SO ED 4234"Int	HCO & OSA COORDINATION ON
	SECURITY & INVESTIGATION MATTERS
HCO PL 23 Dec 65	SUPPRESSIVE ACTS,
	SUPPRESSION OF SCIENTOLOGY
	AND SCIENTOLOGISTS
HCO PL 27 Oct 64R	POLICIES ON PHYSICAL HEALING,
	INSANITY AND SOURCES OF TROUBLE

Attached are several checklists for use by PICO and OSA/ DSA personnel in the handling of security risks and security related situations. They are intended as a guideline of actions which can be taken which are in alignment with the above policy letters. The checklists themselves do not supplant policy which should be used as the guiding factor in handling such matters.

The point of using them is that proper coordination exists between HCO/Snr HCO and OSA and most importantly that the situations are actually handled.

The checklists are to be kept by I&R Chfs, HASes, DSAs, Snr I&R Int, Snr PCO Int, Staff Security Officer OSA INT/CONT, Security Chf Snr HCO INT, OSA Invest terminals, and Security personnel where posted, for use by them. This checklist should be implemented by any one of these terminals who discover that such a situation exists in an org or in the field that requires immediate coordination and handling.

The types of security situations which may come up on HCO/OSA lines are described in the policy references listed above and are generally listed in SO ED 4234 INT as items a-o, which are listed here as follows:

- a. PTS Type C situations with public where an external source is threatening legal or pushing someone to threaten legal.
- b. Illegal PCs category number three, where a person has connections to an outside intelligence agency of some sort.
- c. Any threat of legal action or any other attack from a public against the organization.
- d. Squirrels or declared individuals who are pushing onto org lines or lines of staff or public in good standing, either covertly or overtly.
- e. Newspaper reporters, psychiatrists, psychologists, police, intelligence agency connected personnel trying to get on org lines.

- f. Persons PDHed to do destructive actions against Scientology* and those who PDHed them.
- g. Attempted suicide cases or PTS Type IIIs and any external or antagonistic connections to them.
- h. Criminals or persons with a criminal record who are trying to get on org lines.
- i. Institutional, and shock cases trying to get on lines.
- j. Persons who have come to investigate Scientology for news stories or any other reason.
- k. Members of squirrel groups or suppressive groups, or past members of such groups.
- l. Incidents of theft, break-in or physical attacks on Scientology persons or property.
- m. Persons who are encouraging Scientology public or staff to take illegal and destructive actions.
- n. Persons engaged in mutiny or outright sabotage or any of the actions described in HCO PL 1 Sept 69, Rev. 24.9.83, COUNTER ESPIONAGE.
- o. Persons who are members or connected to members of Anti-Religious groups organized to attack or persecute religions.

In addition to the above, the checklists give a guideline for dealing with any instance of an illegal PC per HCO PL 6 Dec 76RB, ILLEGAL PCs, ACCEPTANCE OF or troublesome source as per HCO PL 27 Oct 64R, POLICIES ON PHYSICAL HEALING, INSANITY AND SOURCES OF TROUBLE found on org lines, serious enough to present a security risk to the organization; or any attempted enemy infiltration detected on Scientology lines.

There are 4 separate checklists provided:

1. One which lays out the internal actions to be taken by HCO.
2. One which lays out external actions to be taken by OSA/DSA personnel.
3. A specialized checklist for dealing with PTS Type III cases found on org lines.
4. A specialized checklist for handling of a theft of org property or material.

When a checklist is logged out to a situation, each step, upon completion, should be initialed with date and post title of the person executing the actions. Once the matter is handled the checklist can be filed with any folders related to the matter.

Sin: I&R INT

Approved by
LRU" COMM INT

Authorized by
AVC FLAG®

for
CHURCH OF SCIENTOLOGY
INTERNATIONAL

CSI:AVCF:BPO:PJ:jb

28 29



SENIOR HCO INT

DIRECTIVE

FDD 367 DIV 1 INT

24 August 1998

TO: SNR HCO CONTS }(
OSA
SECURITY I/Cs ALL ORGS (OR AS HFA)

INFO: CO CMO INT, WDC SCN, WDC OSA, IMEC
LCI, SNR HCO INT, OSA INT, FNCC, FB
CLO, CONT NCC, FOLO PGMS CHFS
ORG FRs, DSAS, ECs, HASes,
DIR I&Rs, SECURITY i/Cs

* **CONFIDENTIAL** *

ORG SECURITY BASICS PROGRAM FOR CLASS V AND CC ORGS

INFORMATION:

It is time to get really professional about security in our orgs and create an extremely safe space for Golden Age of Tech auditing and training to occur. This program is going to help you accomplish just that.

Investigation has found that those orgs with beefed-up security measures were not getting hit by criminals. The successful actions done by these orgs were researched and have now been put into an extensive Org Security Checklist. Once done in every org, the criminals, plants and psychos will undoubtedly have to look elsewhere to wreak havoc. And we'll continue on with the business of setting people free.

PROGRAM PURPOSE:

TO SECURE AND SAFEGUARD OUR CHURCHES.

MAJOR TARGETS:

1. THE STAFF HATTED ON SECURITY AND WEARING THEIR SECURITY HATS TO SAFEGUARD THEIR CHURCH.
2. SECURITY BASICS REALLY GOTTEN IN CREATING A FORTRESS AGAINST SPs AND A SAFE HAVEN MADE WHERE PEOPLE CAN GO FREE.

PRIMARY TARGETS:

1. Where no Security I/C exists, the HAS (or as HFA) is to assign the hat of Security I/C to the actual terminal who HFA's this hat in Dept 3 of the org. An actual named person on staff is to hold this HFA.

HAS (or as HFA)

2. Take full responsibility for the rapid execution of this program.

SECURITY I/C

3. The Security I/C (HFA where necessary) is to immediately telex the Cont Security Chief and give your name, your other post if you are HFAing the Security I/C function, and an attest that you have taken full responsibility for rapidly executing this program.

SECURITY I/C

4. Study and understand the following references:

HCO PL 30 Oct 62	SECURITY RISKS INFILTRATION
HCO PL 16 Dec 68	SECURITY DIV 1
SPD 1 Aug 95	SECURITY CORDLESS PHONES
HCO PL 29 May 61 II	SECURITY OF HOUSE
HCO PL 9 Sept 66	SECURITY
HCO PL 15 Nov 65	REPORTING OF THEFT AND ACTION TO BE TAKEN
HCO PL 1 Sept 69R	COUNTERESPIONAGE
HCO PL 9 Jan 80	DEPARTMENTAL MINI PROGRAMS: THE KEY TO ACHIEVEMENT
FDD 341 DIV 1 INT	RE: ORG SECURITY WEEKLY REPORT FORM
FDD 348 DIV 1 INT	RE: CHECKLIST FOR PREVENTION AND HANDLING OF SECURITY THREATS
HCO PL 5 Apr 65 III	SCIENTOLOGY MAKES A SAFE ENVIRONMENT

 SECURITY I/C

5. Study and word clear this program.

 SECURITY I/C

6. Set up your program folder so it is within easy reach and ready for use.

 SECURITY I/C

7. Work out and assign TMs to each target of this program against the overall production target.

 SECURITY I/C
VITAL TARGETS:

1. While executing this program, apply LRH policy and LRH tech in your actions.

 SECURITY I/C

2. At all times, set an example of high standards in production, appearance and conduct.

 SECURITY I/C

3. Report any departure from standard tech or policy per HCO PL 1 May 65 I, STAFF MEMBER REPORTS.

 SECURITY I/C

4. Ensure you and Reception have a list of emergency phone numbers for: Police, Fire, Church attorneys, DSA, all executives, Snr HCO Cont, OSA Cont, Security Chief Int and External Security Chief OSA Int (both via 213-960-3500).

 SECURITY I/C

5. In case of any serious security incident occurring in the org such as a break-in, theft, someone going Type III, a bomb threat, a bomb, a fire, a natural disaster, someone shot, etc., immediately contact your Senior HCO Cont, OSA Cont, Security Chief Int and External Security Chief OSA Int. Let them know what you are doing and what you propose and standby for further instructions, while you handle as best you can.

 SECURITY I/C

6. Any expenditures to upgrade security of the org are to be gotten through standard purchase orders from Financial Planning. (Ref: HCO PL 26 Nov 65R, FINANCIAL PLANNING)

 SECURITY I/C

7. Any time you run into any counter-intention, disagreement or joking and degrading while executing this program, handle it with standard ethics policy and then report the matter to Ethics of your org, with an info to your Senior HCO Cont, OSA Cont, Security Chief Int and External Security Chief OSA Int. (Ref: HCO PL 22 July 82, KNOWLEDGE REPORTS)

 SECURITY I/C
OPERATING TARGETS:

1. On receipt of this program, meet with the Exec Council and do the following:

- a. Give them a copy of this program. Let them know this is confidential and is to be kept secure.

29 30

- b. Brief them on the information section of this program and the attachments (i.e., FDD 369 DIV 1 INT and its attachments). Let them know you will be working with them and ensure the org is safeguarded.
- c. Get their agreement and full support to get the org 100% safe and secure.
- d. Send a report on the results of your meeting to your Cont Security Chief (or as HFA) with an info to Security Chief Int.

SECURITY I/C

2. Call together the Dir I&R and DSA staff and brief them in the same fashion. Get them to read the attachments. Get their agreement to back up this program and get the org secure. Write up the results of your briefings as per target 1 above.

SECURITY I/C

3. Look over FDD 369 DIV 1 INT, ORG SECURITY CHECKLIST (attached). Get a good idea of the things to be looked for in regards to out-security and safety.

SECURITY I/C

4. At the next staff muster, off production time where the staff are all present, tell the staff you are now holding the post of Security I/C (HFA where necessary). Let them know you will be taking actions to improve security in the org. Then take them on a tour of the org as a group and look for any areas of out-security which exist and go over how these could be fixed. Things to look for would include but not be limited to: a) every piece of fire-fighting equipment and check if it is operational; b) all the entrances and exits and check if they are secure; c) any insecure doors to offices; d) any insecure pc folders; e) any insecure files such as Treasury, CF, Ethics; f) any insecure computers/disks, and g) any other security points they can find. Keep it uptone and interesting with no make-wrong. Keep notes of what was out; you can use this data in your later inspection you do as part of this program. Afterwards get the staff's agreement to handle each point found as out.

SECURITY I/C

5. At a subsequent staff muster, off production time where all the staff are present, tour the staff through the org again and find what outness were handled in the last tour and note which are still out. Keep a copy of the outnesses found for the compliance report.

SECURITY I/C

6. Correct each point found out on the second tour and chit those staff responsible. Keep notes of what was done to handle each point and copies of the chits for the compliance report on this target.

SECURITY I/C

7. At a subsequent staff muster, off production time where all the staff are present, drill the staff on going up and getting in comm with any new public or suspicious persons in or around the org and pulling strings to find out what they are about. Drill them to approach the person in a friendly fashion and get in comm with them, find out what they are there for in a very friendly way, and then pull any strings if the answers are incorrect or suspicious. Have them then route the person to the correct location such as out the door for a drunk, to HCO for an ethics particle, to Reception (while HCO and DSA are alerted to any possible plants), to the Registrar for a public who wants to buy, etc. Ensure they keep it real. Drill them until they really get it and are willing to confront anyone.

SECURITY I/C

8. At the same muster, drill the staff on having someone come up and attempt to get private information from them about the Church and its operation and then without giving out any information that they should not have, finding out what they are about and reporting the matter to HCO immediately. Drill them also on public asking valid questions about Scientology and correctly answering and routing them as well, so they can clearly see the difference between a security particle and valid public and handle appropriately.

SECURITY I/C

9. Some days later at a muster with all the staff, find out from the staff who has had any wins putting in security measures since the walk through of the building and the drilling. Acknowledge and validate anyone who has. This is counted as done once all the staff have been asked and any wins acknowledged. Ensure you send a short write-up of the wins given with the CR.

SECURITY I/C

10. Get together the DSA, Estates I/C (or as HFA) and any other executive or DSA staff member interested and do an inspection, using a copy of the ORG SECURITY CHECKLIST and its attachments, of all org properties, inside and out. Check each point. Note down any points found out. Note anything else found out which might not have been noted on the checklist.

SECURITY I/C

11. Once completed, sit down with all the terminals who did the inspection and create a mini program to handle each point found out, as per HCO PL 9 Jan 80, DEPARTMENTAL MINI PROGRAMS: THE KEY TO ACHIEVEMENT. Include targets for pushing through the needed finances.

SECURITY I/C

12. Once the mini program is complete, realistically TM out each of the targets.

SECURITY I/C

13. Make up two extra copies of the inspection notes and the mini program. Send one set to the Cont Security Chief and the other to Security Chief Int.

SECURITY I/C

14. Complete the mini program by daily working on the targets and being unreasonable in your demand for dones.

SECURITY I/C

15. Ensure there is a qualified, in-ethics, org staff Receptionist on post every second the org is open.

DIR PERS (OR AS HFA)

16. CONDITIONAL: If no Receptionist is on post every moment the org is open, alert the org EC with a copy to Security Chief Cont and Security Chief Int. Use LRH policy to get the post covered full time by a qualified staff member, including the use of HCO PL 22 July 82, KNOWLEDGE REPORTS.

SECURITY I/C

17. Verify each staff member holding Reception has been hatted by the the DSA on:

- a. How to handle search or seizure warrants.
- b. How to handle process servers (someone delivering a legal document against the Church or members of it).
- c. How to handle violent intruders or disruptive persons that come into the org.
- d. How to comply to any legal requirements on keeping files, if there are any for your org. (The DSA will know if there are any).
- e. How to tape record threatening phone calls as applicable in your area.

SECURITY I/C

18. Verify the Receptionist has the phone numbers (plus any pager numbers) and a way to call out to:

- a. The police
- b. The fire department
- c. Medical emergency personnel
- d. DSA
- e. Church executives
- f. Church attorneys.

SECURITY I/C

19. Ensure the Receptionist has a working:

- a. Tape recorder, with plenty of tape and hookup for taping calls as applicable
- b. 35mm camera
- c. Small chemical fire extinguisher for small fires and self-defense
- d. Panic button which sounds a screaming loud alarm
- e. Assist button which buzzes HCO, DSA and exec offices for help.

SECURITY I/C

20. Verify each Receptionist is hatted on using each of the above 5 items and they have drilled their use successfully. Have each show you how they would use it, so you know for a fact they have it. Correct them as needed.

SECURITY I/C

21. Get competent, ethical male staff members holding the night watch each night. Do this by creating and issuing a schedule, which is approved by EC, which covers each night.

SECURITY I/C

22. CONDITIONAL: If no night watch is on post every moment the org is closed, alert the org EC with a copy to Security Chief Cont and Security Chief Int. Use LRH policy to get the post covered full time by a qualified adult male staff member, including the use of HCO PL 22 July 82, KNOWLEDGE REPORTS.

SECURITY I/C

23. With the night watch guards, walk around the org and make up a full checklist, using the Night Watch Checklist attachment to the ORG SECURITY CHECKLIST. Add any points needed to ensure the org is really secure.

SECURITY I/C

24. Get the made up Night Watch Checklist done standardly each night for one week to count as being in.

SECURITY I/C

25. Write a commend on all night watch guards, Receptionists and any staff who have done a noteworthy job handling/improving security for the org. Get this distributed to all staff.

SECURITY I/C

PRODUCTION TARGET:

4 weeks to complete all the targets of this program.

PROGRAM COMMUNICATION:

Written compliance reports to your Cont Security Chief (or as HFA), with cc's to Security Chief Int and External Security Chief OSA Int.

Jeff Porter
SECURITY CHIEF INT

Authorized by
AVC FLAG LIAISON OFFICE

for
CHURCH OF SCIENTOLOGY
INTERNATIONAL

CSI:BK:JP:jp.dc

LRH, HCO, FLAG and SCIENTOLOGY are trademarks and service marks owned by Religious Technology Center and are used with its permission. Services relating to Scientology religious philosophy are delivered throughout the world exclusively by licensees of the Church of Scientology with the permission of Religious Technology Center, holder of the SCIENTOLOGY and DIANETICS trademarks. Printed in U.S.A.



SENIOR HCO INT

DIRECTIVE

FDD 369 DIV 1 INT

25 August 1998

TO: ALL DIR I&Rs AND MAAs

INFO: DSAs
ESTATES I/Cs

FROM: SECURITY CHIEF INTERNATIONAL

ORG SECURITY CHECKLIST

References:

HCO PL 24 Feb 71	OPERATING AT RISK
HCO PL 1 Sept 69R	COUNTERESPIONAGE
HCO PL 22 July 82	KNOWLEDGE REPORTS
HCO PL 24 Aug 65 II	CLEANLINESS OF QUARTERS AND STAFF, IMPROVE OUR IMAGE
HCO PL 20 Apr 69 II	HATS, NOT WEARING
HCO PL 4 Jan 66 III	SCIENTOLOGY ORGANIZATIONS
	COMMUNICATIONS SYSTEM: DESPATCHES
SPD 1 Aug 95	SECURITY CORDLESS PHONES

"Don't operate at risk. The way to save time and lives is do it right in the first place.

"'Hope' is the byword of the down-and-outer, the bums of skid row.

"Control your environment by doing things well and thoroughly.

"Then you are secure."--LRH (HCO PL 24 Feb 71, OPERATING AT RISK)

It is vital that our orgs are proofed up against criminals and the damage they can cause, so that we can get on with the business of freeing beings.

Although there has been an increase in crime internationally in the past two years, those execs and staff who have taken adequate actions to secure their organization have not had any problems.

Commonly stolen items include computers, followed by audiovisual equipment and then money, bookstocks and other mest. Thieves walk through unlocked doors or windows, or these are forced open. Once inside, unlocked offices are easily accessed. And records and files must be kept secure against any possible espionage as per HCO PL 1 Sept. 69R, COUNTERESPIONAGE.

So to assist you in getting in security in your org, a security checklist has been created for your use to help you put in tight security and get on, undisturbed, with flourishing and prospering and handling the underlying causes of the crime.

The checklist should be done by the Security I/C. If no Security I/C, it is done by the person who holds it from above. The DSA and Estates I/C should also go on the inspection, so as to assist in spotting any points that might need to be handled.

Once done, the results are then turned in to the Security Chief of your cont with a project of how you are going to handle each point. (Ref: HCO PL 31 July 83R I, BASIC MANAGEMENT TOOLS)

When you have completed the project, send a compliance report to the Security Chief Cont, who will forward the data to Security Chief Int.

The following is the checklist to be done:

SECURITY OF ENTRANCES

1. The front door is locked with a high security deadbolt lock. Purchase high security deadbolt locks which cost at least \$60 US dollars or more each, and which clearly state that they are high security deadbolt locks. Do not purchase inexpensive brands which professional criminals can easily open. _____
2. All other entrance doors also have high security deadbolt locks. _____
3. All entrance doors not watched by a Receptionist are actually locked with the high security deadbolt locks. _____
4. All accessible windows are locked with professional burglar-proof locks. This means locks specifically designed to stop burglars--not just latches. Check with your local police on what to purchase if you are not certain. _____
5. If there are any other possible entrances, they are locked with high security deadbolts. _____

RECEPTION AREA

6. There is a Receptionist on every minute the org is open. _____
7. There is a Night Guard on all night, every night. These staff must be in-ethics and not PTS. _____
8. The Receptionist and Night Guard have a club to protect themselves (but no guns, as they are too much of a liability even where they are legal to have them). _____
9. The Receptionist and Night Guard have a phone with which they can contact the police/fire departments, Cont HCO and OSA and OSA Int in case of an emergency. _____
10. The Receptionist is drilled on knowing every single person who comes in the org and politely finding out about anyone not known. _____
11. The Receptionist has a small chemical fire extinguisher for fires and for self defense. _____
12. Every person who holds the Receptionist hat and Night Guard hat, even briefly, has been hatted and drilled to a pass on all the following points:
 - a) Able to contact the DSA, HAS and ED, 24 hours a day. (Ensure each has a pager which is always on). _____
 - b) Able to quickly contact the police, fire department and bomb squad. _____
 - c) Can smoothly handle any suspicious stranger and find out exactly what they are about in an in-ARC manner, and then alert HCO and the DSA with the alert buzzer (see Attachment 1, section on RECEPTIONIST ALERT BUZZER). _____
 - d) Can use the 35mm camera. _____
 - e) Can use the video equipment and adjust the screens on the monitors. _____
 - f) Is checked out on the manual and can operate the VCR. _____
 - g) Is drilled on "taking a bomb threat", _____
 - h) Is drilled on handling trouble makers. _____
 - i) Is drilled on using the alert buzzer system. _____
 - j) Is drilled on using the RECEPTIONIST SERIOUS SECURITY EMERGENCY ALERT BUTTON (see Attachment 1, section concerning this system). _____

- k) Is drilled on pulling out and using the Security Situations Checklists. This means drilling on each checklist to a pass. _____
- l) Is drilled on using a small chemical fire extinguisher kept at Reception, for putting out small fires and for self defense if ever needed. (Do not actually discharge the extinguisher while drilling). _____
- m) Is drilled on how to tape a threatening phone call in those cities where it is legal to do so. (Check with the DSA to see if it is legal in your area). _____

SECURITY CAMERAS AND RECORDERS

(See Attachment 1, section on CAMERA SECURITY SYSTEM for details on video cameras and VCR).

- 13. There is a 35mm camera--a self-focus, automatic type, with film, batteries and a working flash--located at Reception. _____
- 14. There is a similar 35mm camera located in the DSA office for backup and use for DSA-related cycles. _____
- 15. Extra film is stored (in the org refrigerator), which gives it longer life, in case a lot of film is needed. (When possible, take the film out and let it warm up for an hour or so before taking it from its plastic container. Cold rolls of film attract moisture when put into a warm environment. _____
- 16. There is a video camera in Reception, so as to be able to see who is there. _____
- 17. There is a video camera outside the main street entrance, so that anyone approaching the building can be seen. _____
- 18. There is a video camera watching the DSA office entrance. The monitor for this camera is to be at Reception and a duplicate monitor in HCO. _____
- 19. There is a camera watching the ethics and personnel files. _____
- 20. There is a camera watching the pc folders. _____
- 21. There is a camera watching the CF files. _____
- 22. There are cameras for any other key entrance locations, as needed, to protect the building. _____
- 23. There is a VCR recorder which records all the cameras for 24 hours, and it is working. _____
- 24. There are enough VCR cassettes to keep one full week's recordings before having to re-record over them. _____
- 25. There are monitors for all cameras located in HCO. The VCR should be located there as well. _____

SECURE OFFICES

- 26. There are no money/checks/checkbooks lying around. _____
- 27. The Treasury door is kept locked when no one is there. _____
- 28. The HCO door is kept locked when no one is there. _____
- 29. The DSA office door is kept locked when no one is there. _____
- 30. The Treasury money/records are locked up in a working safe. _____
- 31. Money is taken to and from the bank securely by two or more people. _____
- 32. Money is banked daily so no large amounts are kept in org. _____
- 33. There are no cordless phones or cellular phones being used by the staff as per SPD 1 Aug 95, SECURITY CORDLESS PHONES. _____

34. The location of the phone connections in the org is secured with a good lock and is only accessible by the HAS. This is done so no one can easily get in and place a bug on the line, or listen in. _____
35. The KTL/LOC area is securely locked when the Supervisor is not there. _____
36. The Clear folders are locked up and only authorized Clears have access. _____
37. The other pc folders are kept locked up, so no one can walk off with them. _____
38. The ethics/pers files are kept locked up securely in HCO. _____

SECURITY OF COMPUTERS AND DATA

All the computers in the org must be secure. This is an important item as the most commonly stolen items are computers, and they often hold very valuable data on them.

39. Any small laptop type computers are locked away in a locked drawer/filing cabinet when not in use. _____
40. Larger computers are secured with burglar-proof steel cable systems, which can be purchased from large computer stores. _____
41. Every computer has passwords so they can only be accessed by authorized personnel. _____
42. All computer disks are securely locked up when not in use. _____
43. All backup tapes of the system and release installation disks are to be kept in a safe when not in actual use. _____
44. Computers with org data are not connected to modems. This is a must to prevent professional hackers from breaking into the systems and stealing or altering data or planting viruses. _____
45. No computers are linked to the Internet, even if for only part of the day, unless this is an authorized Scientology On-Lines computer. _____
46. The main computer is secured in a well-locked room. This is usually the DSA or FBO office in most orgs. _____
47. Only authorized HCO staff use the telex machine and are using it securely. _____
48. All faxes are only sent by HCO and the terminal sending them is fully briefed by the DSA on what can be sent and what is not okay to be sent via fax. _____
49. The CF data is securely locked up so only those authorized staff can access this data. _____
50. The Addo data is securely locked up with access only to authorized staff. _____
51. There is an operational shredding machine for all the staff to use, which turns the paper into small, unreadable bits, not long strips. _____
52. There are clearly labeled shred bins for staff to put their shredding in. It's important that these shred bins are identical and do not look like any other bins. This is so the staff in a different area than their office don't make the mistake of putting shredding in the wrong bin. _____

FIRE SECURITY POINTS

53. There is adequate fire equipment for each floor which works. (e.g., fire extinguishers are actually filled and work). _____
54. The staff are hatted on using the fire equipment. You need to actually check this at the next muster and ensure they all do know how to use the equipment. _____

- 55. There are no fire hazards, such as blocked exits. _____
- 56. There are no insecure chemicals, paint, etc., which could burn easily. _____
- 57. There are no fire hazards, such as poor wiring in the building. _____
- 58. There are no fire hazards, such as unsafe electric heaters. _____
- 59. There are adequate smoke detectors throughout the building. _____

SECURITY OF KEYS

- 60. No unauthorized staff have keys to areas they shouldn't have access to. You'll need to survey each staff member and find out what keys they have. _____
- 61. Any locks with missing keys have been replaced with new locks. _____
- 62. No public have keys. _____
- 63. Keys are not left in unlocked desk drawers or other similar locations where staff/public/criminals can get them. _____
- 64. An up-to-date key log is kept by the Dir RAM or Treasury terminal HFAing this post. _____
- 65. A key log exists to temporarily log in and out any keys which are temporarily issued to authorized staff for their use. _____
- 66. Keys to org spaces are securely locked up, not available to unauthorized staff or any public. _____
- 67. Exec offices, HCO, DSA office, Treasury, C/S Office, pc folder storage, CF, Addo and all exterior doors have been re-keyed under presently contracted trustworthy staff and keys have been given only to those who are cleared to have them. _____

SECURITY OF PUBLIC

- 68. HCO has a list of all public who are, or could possibly be, a security risk and a program to handle each one. A copy of this list is to be forwarded to the DSA, Cont HCO and Snr I&R Int each week. _____
- 69. All pes are being checked to ensure they are not illegal as per HCO PL 23 Oct 61 II, HGC PREPROCESSING SECURITY CHECK. Actually look to ensure this is being done. _____
- 70. All students are being checked to ensure they are not illegal as per HCO PL 1 Nov 61, HCO WW SECURITY FORM 5A (page 33 6, Tech Volume VI). _____
- 71. All pes sign an enrollment form. Look, don't listen. _____
- 72. The C/S attests there are no security threat public on lines. Again, have the C/S look and sign an attest. _____

STAFF QUALS

- 73. All staff are qualified for staff by actual review of their files per:
 - HCO PL 11 Nov 76RB I STATISTIC CHANGE, HCOS AND QUAL DEFINITIONS
 - HCO PL 23 Nov 59 EMPLOYMENT OF CRIMINALS FORBIDDEN
 - HCO PL 29 July 71 III PENALTIES FOR THE HIRING OR RECRUITING OF INSTITUTIONAL OR INSANE PERSONS
 - HCO PL 29 June 68 ENROLLMENT IN SUPPRESSIVE GROUPS
- 74. All existing staff have received a 7B check as per HCO PL 18 Sept 61R, HCO WW SECURITY FORM 7B. _____
- 75. All new staff receive a 7A check as per HCO PL 13 Sept 71, HCO WW SECURITY FORM 7A. _____

76. HCO has a list of all staff who are, or could possibly be, a security risk and a program to handle each one. A copy of this list is to be forwarded to the DSA, Cont HCO and Snr I&R Int each week.
77. The C/S attests there are no staff security threats in the org or, if any exist, that there is an active program being done by the C/S and/or HCO, and/or Qual to handle the matter. Get the C/S to actually look and sign an attest that this is true.

NIGHT WATCH CHECKLIST

78. The Night Watch/Security I/C has a checklist which is being done every night and MINIMALLY contains the items in the Night Watch Checklist. (See Attachment 2).
79. The Night Watch/Security I/C is taking effective action to handle any and every point that is out in the Night Watch Checklist, including writing reports on all outnesses found.

By doing the above checklist, making a project to handle the outnesses and then getting it done, you will have increased security in your org tremendously. I am counting *on* you to get a fast and professional product, so the org, staff and public are really secure from harm and able to get on with the job of freeing beings.

Jeff Porter
SECURITY CHIEF INTERNATIONAL
SENIOR HCO INTERNATIONAL

Approved by
SENIOR I&R INTERNATIONAL

Authorized by
AVC FLAG LIAISON OFFICE

for
CHURCH OF SCIENTOLOGY
INTERNATIONAL

CSI: BK: AS: JP: jp. jh

RE; ORG SECURITY SYSTEMS

In order to keep your org secure, there are some security systems which need to be installed immediately.

LIGHTING

One of the simplest, least expensive and most effective security systems are bright lights at night.

Go outside at night and look at the current lighting all the way around your org. If you also have parking, check the lighting for that as well.

What you want is lots of very bright light at night. The type, which by investigation is the best for deterring criminals, is the bright white/blue type of lights, not the soft yellowish lights. The large ones are "metal halide" (halogen) or "mercury". A number of 300 or 500 watt halogen lights work well if placed all around the org. You can also get much larger ones for big parking lot areas/large buildings.

Get one, put it up and see how much coverage you get. Then purchase the rest so that you have full coverage. To save on electricity, you can purchase lights which have a photo-electric sensor which turns the lights on at night and off when the sun comes up.

It cannot be emphasized enough just how effective bright lights are at night for keeping the criminals away.

CAMERA SECURITY SYSTEM

The camera system must have cameras and monitors watching all the key positions in the org. It requires a VCR, recording all these cameras 24 hours a day. This system can be installed by one of your staff who has a basic understanding of these types of systems. They are not very complicated.

The cameras themselves should be the newer model micro-chip type cameras. Purchase them from a major manufacturer such as Panasonic, Toshiba, Sanyo, etc., so you get a decent quality camera which will last for many years. They come in black and white or color. Color are more expensive, but are recommended, especially for the Reception and front entrance cameras, as they show the color of the person's clothes.

The cameras can be very small and hidden. Or they can be large enough to be easily seen. It's recommended that the Reception and outside cameras are easily seen, as they will help act as a deterrent to criminals.

The pictures from the cameras should be split, with one set going to monitors in Reception and one set to monitors in HCO. HCO and Reception will be able to see the same pictures. This can be done by splitting the actual cable, using a "T-splitter" or by running cable from one monitor's "out" jack to the second monitor.

The monitors (TV screens) should ideally be large monitors which contain 4 pictures on each screen. This is done using a "quad splitter" (splits the screen into 4 different parts, with a different camera view in each). This system also allows the viewer to bring up any one of the pictures onto the full screen when needed, to get a better view. Using the large monitors saves on cost and space and it's easier to record them using the VCR.

The VCR is important as it can be used to check back for who went into an area at any time. It can also be used legally as evidence of crimes committed. Just prior to writing this issue, a criminal was able to be arrested by the police using video evidence from the org's VCR, showing the criminal clearly committing the crime.

The type of VCR to be used is one which will record for 24 hours on one tape. SONY makes one of these called a Time Lapse Recorder. Other manufacturers make them. Most large electronic security equipment distributors will carry them.

There needs to be enough VCR cassettes to record for a full week before recording over any of the cassettes again.

The following are the MINIMAL locations to be recorded by camera, monitor and VCR:

- a. Main entrance: looking at who is walking up to and into the building.
- b. Reception: looking at who is in the Reception area, as well as the Receptionist.
- c. DSA office entrance.
- d. Ethics/pers files: Looking at the entrance area, either inside or outside the files space. If they are stored in more than one location, then more cameras will be needed.
- e. Pc folder storage.
- f. CF files.
- g. Any other key locations: This could be another entrance area which the Receptionist would watch. It might include parking lots, other floors, other adjacent buildings used, etc.

Camera motion detectors are a recommended option which can be added to this system. These set off an alarm whenever the camera "sees" any motion in the screen of any camera set with this system.

MOTION DETECTION SYSTEM

In order to help protect the Church when there are few or no staff working in the org, motion detectors hooked up to screamingly loud sirens are used.

These systems can be purchased at any large security company supply store and are not very expensive at all. They can easily be installed by anyone with just basic electronics hatting.

The motion detectors are put in key locations and hooked into a panel which allows them to be turned off and on individually. This is important, as you may want to set the alarm in some locations, but leave others free due to a situation, such as a C/S working late and needing to move around in certain locations. This would also allow the Night Guard the ability to turn the alarms off in any areas he was going to inspect and then turning them back on again.

These panels are then hooked up to sirens which are so screamingly loud, that the noise alone would scare off any criminals. The sirens need to be heard in every part of the org.

The minimal areas which need to have motion detectors are:

- a. HCO
- b. Treasury
- c. DSA Office
- d. Pc folder storage
- e. Pers/Ethics folder storage
- f. CF
- g. Any entrance area, including back doors, roofs, basements, etc.
- h. Any area which a criminal might break in through, such as an office with windows on the ground floor,
- i. Any area which contains computers or other valuable electronics gear, the first item criminals usually steal,
- j. Any other area you want to alarm, such as a private parking lot, adjoining buildings, etc.

RECEPTIONIST SERIOUS SECURITY EMERGENCY ALERT BUTTON

This is an alarm which allows the Receptionist to alert EVERYONE in the building that there is a serious security emergency in Reception. It also is used to help scare away any serious criminals. This would only be used when the Receptionist was faced with an armed criminal, or an explosive or fire bomb being thrown into the org, etc.

This system is extremely inexpensive and is easy to install. The system has a button or switch at Reception. The button/switch is out of sight. It also must be protected, so it cannot possibly be accidentally set off. There are buttons/switches with protective covers which can be gotten for this purpose.

Once pushed, this button/switch sets off a siren in Reception that is so loud that any criminal would be scared and probably run off the second he heard it. You want to get the loudest possible siren for this.

This system would only be used for the most severe security situations, as it would disrupt sessions and students.

RECEPTIONIST ALERT BUZZER

The Receptionist needs to have another hidden button installed at her desk. This leads to buzzers located in HCO, DSA and any key exec offices. If the Receptionist needs help to handle a drunk or psychotic person or something similar, she can push the button and the execs/staff who hear it can come and assist.

This system should be fairly quiet so it won't disrupt the entire organization or any public, but it will get assistance for the Receptionist when needed.

Codes should be worked out and drilled by the staff. Example: Rapid repeated buzzes means a serious situation and need help fast; two slow buzzes repeated every few seconds could be a request for just the DSA. Work out and drill these codes.

This buzzer and the other alert button/switch should be in a hidden position that the Receptionist can use, without being obvious about it.

POLICE/SECURITY ALERT SYSTEM

There is an optional system which is recommended. This is a panic/alert button which goes directly to the police or a security company which then sends an armed officer to investigate. Many cities around the world now have these. You can call your police department and ask them about such systems.

If your city has both systems, find out which one responds the fastest and get that system. They usually charge an initial fee or monthly fee, plus a fee for any response.

Again, any one of your staff or trusted in-ethics public who is hatted on basic electronics can research and install the above systems. They are not complex. If you do have any questions, you can always contact your nearest Base Security Chief or Security Chief Int.

NIGHT WATCH CHECKLIST

The following checklist is the minimal checklist to be used by the Night Guard each night to ensure the org is secure. You should add any points to this which are peculiar to your organization, such as added buildings, parking lots, special locked areas, etc.

1. The front door is secured with a high security deadbolt. _____
2. All other entrances are secured with a secure deadbolt. _____
3. All accessible windows are locked. _____
4. There is a club available for protection, if needed. _____
5. There is a phone available with emergency numbers. _____
6. The Receptionist has a small chemical fire extinguisher. _____
7. There is a working 35mm camera at Reception. _____
8. Extra film is stored in the org refrigerator. _____
9. There are working video cameras in Reception and outside. _____
10. The 24 hour VCR recorder is working and is turned on. _____
11. The emergency alarm system is operational. _____
12. There are no money/checks/checkbooks lying around. _____
13. The Treasury door is secure. _____
14. The Treasury money/records are secured. _____
15. The HCO door is secure. _____
16. The DSA office door is secure. _____
17. The KTL/LOC area is securely locked. _____
18. The Clear folders and other pc folders are locked up. _____
19. The ethics/pers files are locked up. _____
20. All the computers in the org are logged off and secured. _____
21. The CF data is securely locked up. _____
22. The Addo data is securely locked up. _____
23. There is adequate working fire equipment for each floor. _____
24. There are no fire hazards, such as blocked exits. _____
25. There are no fire hazards, such as unsafe electric heaters. _____
26. There is an operational org shredding machine. _____
27. Random checks are done of trash baskets for shredding. _____
28. KR's were written on any serious out-security found. _____