

Drill _____:

USING BUTTONS. In each of the following write out 3 ways that you could connect up the target person as anti-love or pro-hate of his/her bosses (or person with power to influence his/her job) buttons.

- a. Target: Bob Jones 18 yr old stock clerk in local grocery store.

Boss: fires kids who are druggies, loves employees who are on time to work.

- b. Target: Mrs. Grover a 45 year old volunteer worker at the local Charities Assn.

Boss: Director of the assn. hates people who drink alcohol, and hates employees who wear any type of religious symbol (ie, cross, jewish star, etc.)

- c. Target: Bill Bonehead 25 yr old reporter at the local newspaper.

Boss: Hates enthusiastic reporters or ones who develop their own story ideas. Loves robotic "yes men" to work under him.

- d. Target: Byron P. Stonehedge 60 yr old director of the United General Corp., a multi-diversified \$300 million dollar a year corp.

Bosses: Chairman of the Board likes company men who tow the line; once got a director fired because the directors got bad national press when ~~the~~ his wife committed suicide off of a Las Vegas hotel after running up gambling debts - hates company scandal like this. Stockholders like dividends and earnings from their stocks, hate anything that could prevent such.

- e. Target: Dr. Ughlie, internationally known psychiatrist, 57 yrs old, professor at a local private college and in private practice.

Bosses: The local college alumni and president love good PR for their school, which hold up their image as a college with famous professors; hate bad PR.

VALUABLE/PROTECT: in each of the following write out 3 different ways that you could threaten or attack what each target person considers valuable or is protecting.
Smmmm

- aa. Target: Robert Dayman editor of local newspaper, 56 yrs old.

Val/pro: His status in media circles, belongs to national media clubs and assns. His cow breeding farm 10 miles out of town.

- bb. Target: Free-lance writer Sandra Haney, 32 yrs old, single, promiscuous 2d, drinks alcohol or smokes pot daily.

Val/pro: Doesn't want her parents to know about her promiscuity. Values her "freedom" as a free lancer. Protects herself from being at effect with others, likes to control and attack others.

- cc. Target: Investigator in local district attorney's office Todd Briggs, 45 yrs old, married, one child.

Val/pro: Being able to play golf every saturday and sunday, gets very ARC broken if he can't. His free time after work at night, hates to stay after 6 pm to work a minute after quitting time.

- dd. Target: Congressman Harris, 51 yrs old, 1st term in office, widower, 2 married children.

Val/pro: His PR as "an important person" in his community - likes for people to admire him, which is built on his this rickety PR as congressman and as former county commissioner.

- ee. Target: Dr. Goldnose, local child psychiatrist, 48 yrs old, unmarried.

Val/pro: Doesn't want anyone to know that he gets sexually aroused by children, that he performs various perversions with his child patients and keeps a collection of nude pictures of children.

1. Third party a group to another group ensuring that you get as your product an observed conflict between the two.
- j. Write up results.

Drill _____:

Planning operations: Take each of the following situations and data and plan a three channel operation for each one, using full target series tech, with the purpose of removing or fully restraining the enemy concerned. The viewpoint on each of these is to get something going fast on each enemy and not to get involved in lengthy researching or data collecting. Fast research targets may be added if necessary.

- a. Mock up an operation on: a local psychiatrist who doesn't formally practice psychiatry anymore, but has a column in a local newspaper in which he discusses just about anything he wants to, colored by his psych viewpoint. He has been traced back as the Who behind local press attacks on the Church. We know that he attends orgies rather frequently with male prostitutes; that he's married with two children; that he's a social heroin user - uses it 1-2 times a month at parties; that the owner of the newspaper's wife is a rabid Christian and despises anyone who is against that; that the newspaper owner dearly loves his wife and would do anything for her; that the psych likes to go sailing weekly on his yacht; and that he smokes camel cigarettes.
- b. Mock up an operation on: a female publisher who is behind printing great quantities of entheta on Scn. We know that she is a registered alien (not a US citizen); that if aliens are convicted of a crime they will be deported; that she is wanted for contempt of court in her native country, Germany; that she occasionally smokes marijuana; that she owes lots of money to writers whose books she published and has many outstanding bills to pay (printing, office supplies, lawyers, etc) and is actually very very insolvent; that she has been doing business in Chicago for 5 yrs without a license; that her father was a Nazi who killed over 1,500 Jews in Poland; that she is engaged to be married to a man whose father is the conductor of the Chicago symphony orchestra.
- c. Mock up an operation on: a local squirrel group leader who blew the Sea Org four years ago and now has a rapidly expanding squirrel group. We know that he is money motivated; is married but has affairs with female students; we have 2 BSMS in his group 1 is a student, the other handles the finances of the group; that he gets Scn HCOBs and re-writes them verbatim except that he changes mentions of Scn/Dn to the name of his own group and LRH's name to his own; that he's auditing a local policeman; that he has a grant for \$5,000 with the local

government to pay his "research" expenses for the next 2 years which he spends on utility bills and other operating expenses; that he's got two pet dogs and one pet turtle; and that he spends lots of time and money maintaining his obsession, a restored 1928 Rolls Royce.

- d. Mock up an operation on: An SP writer who works for a popular national magazine and who on his own has developed international comm lines with anti-Scientologists and disaffected staff members. He acts as a "switchboard" for entheta on Scn and LRH and sources many false reports on his own. We know that he drinks liquor daily; has a hobby of building model airplanes; has been an award winning writer but hasn't won an award for 5 years; that the publisher/owner of the magazine's pet love in life is to get his own name onto as many board of directors or committees lists of social do-gooder or charity give-away associations, etc. as he can; that the writer's senior editor will get very upset with or fire any writer who doesn't put in some working time at the office in the evenings or weekends and that the writer puts in just enough ~~time~~ extra time to keep his boss happy; that the writer likes to go fishing and hunting.
- e. Mock up an operation on: a disaffected Scientologist who blew Scn from his local hometown mission last year and is now writing entheta in the local college newspaper where he attends school and writes in the newspaper as part of his journalism studies. One of his entheta articles got bought by a nationwide college wire service and was printed in many college papers throughout the US. We know his parents and a few of his friends names from his former records at the mission and that he likes sports, but that's about all.

*100-100-100
or 100-100-100*

Drill _____:

Following are drills to practice locating buttons for use in Ops. These are ~~not~~ means all the ways to find buttons. Any difficulties encountered should be reported to your supervisor so that proper referral to materials or cramming can be done.

HATE/LOVE.

- a. Write down 5 separate hate or love buttons that you have observed others to have had. (examples: When I was a kid I remember our local butcher used to hate kids running through his store, in fact he'd lose business by throwing the mother's of such children out of the store before handling their meat orders. Mrs. Kolby, my 5th grade teacher, loved students who wore newly cleaned and pressed clothes so much that she'd give them higher grades than they deserved.) _____
- b. Go through some magazines and find long stories or interviews of various people until you can get 3 different people from which you can extract hate and love buttons. Write down what you found on each person. _____
- c. Go observe as many people as necessary so that in the end you can have observed 3 different people about which you know at least one of their hate/love buttons each. You may not speak with any of these people except to maintain your cover in the area. Write up your results. _____
- d. Go through the literature (magazines, newsletters, bulletins, etc.) of a professional, trade or specialty group and note down the ~~manharmmrring~~ hates and loves of that group gleaned from the literature. _____
- e. Interview the head of personnel in some company under suitable guise and find out "reasons why" (Hate/love buttons) their personnel get hired, fired, demoted and promoted. _____
- f. Go to a store, factory, agency or somesuch and interview or survey or converse with several employees to discover the hate and love buttons of the management. (minimum of 5 people) _____
- g. Locate a local executive or manager of some local business or activity who handles junior s or owns the business. Now by observing him, interviewing him or those who know him, and reading anything published about him and/or his line of work, find his hate and love buttons.

VALUABLE/PROTECT

aa.

aa. Write down 5 separate valuable or protect buttons that you have observed others to have had. (example: my neighbor used to spend most of her spare time and most of her money collecting and mounting butterflies, which she kept in a bank vault when not working on them or viewing them. My uncle used to be very concerned about keeping the family together, he arranged all the family parties, even made up reasons to get family members together and bought family gifts which he really couldn't afford). _____

bb. Go through as many CIC files on individuals as necessary until you can by file data alone find on 3 people what each person considers valuable or is protecting. _____

cc. Get into good comm with 3 different individuals and find out something each considers valuable or what they are protecting. _____

6: 7/8/7

Drill _____:

8592

Spreading rumors. Flunk for anyone spotting you as a source of falsity or troublemaking, etc.

- a. Spread a rumor to another. _____
- b. Write up results. _____
- c. Spread a rumor to another and get him/her to spread it to someone else. _____
- d. Write up results. _____
- e. Get a rumor spread around a small group to a point where at least 2 others repeat it to others. _____
- f. Write up results. _____
- g. Get a rumor spread around a large group (more than 50 people) to a point where at least 5 others repeat it to others. _____
- h. Write up results. _____

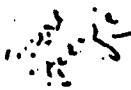
Drill _____:

Third partying. Flunk for being challenged as source of third party or conflict.

- a. Third party someone to another. _____
- b. Write up results. _____
- c. Third party someone to another ensuring that you get as your product certainty that that person 3rd partied to really is in doubt about the other person or has a lessening of ARC for that person.
- d. Write up results.
- e. Third party someone to another ensuring you get as your product an observed conflict between the two.
- f. Write up results.
- g. Third party a group to another group ensuring you get as your product certainty that the group third partied to really is in doubt about the other group or has a lessening of ARC for that group.
- h. Write up results.

Drill _____:

Creating effects. Do nothing illegal or anything which done without thought could reflect poorly back on the Church or yourself - ie, press, police record, etc. naming the Church or yourself. Flunk for disbelief of your guise or effect not fully created.

- a. Select a guise and do something to get another to go into sympathy with you and help you.
- b. Write up results.
- c. Select a guise and do something to get another to intentionally avoid you or get angry with you.
- d. Write up results.
- e. Get into the guise of a salesman/lady and go into a store under the guise that you work there, until you get someone ~~nm~~ (customer) to ask you a question and you handle them as applicable.
- f. Write up results.
- g. Get into the guise of a nurse or doctor in a hospital or medical facility to the point where you give an order or direction to someone inside the facility (public or staff person) and they comply fully believing your identity.
- h. Write up results.
- i. Get into the guise of being a wealthy individual in a Cadillac, Mercedes, Jaguar or Rolls Royce dealership and get a salesman to give you his services for over a half hour and test drives of at least 3 different autos. (If you don't drive, may substitute an exclusive chain of jewelry stores, ie, Tiffanys, to try on 10 different diamond rings over 1/2 hr period of time.)
- j. Write up results.
-  k. Mock up a guise and get at least 3 different people to believe it and handle you for at least 5 minutes all at the same time.
- l. Write up results.
- m. Mock up a guise and get at least 20 people all at the same time to stop what they're doing and pay attention to you for at least 3 minutes.
- n. Write up results.

Drill _____:

Creating incidents which reflect on others. Flunk for being spotted as creator. Take care here to use real targets or elements of society which are downstat, criminal or suppressive.

- a. Locate some type of mental health clinic or psychiatric hospital and find some area where a bunch of employees work together in one space. (Like a business or records office, or some psych consultants that work in one area, etc. Pick out a target employee to run an op on. Now from direct observation in the area ~~xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx~~ and anything you may know about such areas from your own experience, pick a beingness to assume which would be disliked in that environment. Now connect that beingness up with the target person (either while the target person is present or absent) in such a way that impinges with one or more of the target persons fellow employees (ie, you're certain that the fellow employee/s won't immediately dub-in your connection to the target person as being okay or not unusual). This must be done by some type of personal visit (not phone, mail, etc.). _____
- b. Write up results.
- c. Do the same as the previous channel, same employee or a different one in a different area if you wish, but this time run the channel with the target person's senior as your public instead of his fellow employees. Must be done by some type of personal visit by yourself or by getting an FSM to do it. (r-factor and drill FSM as needed). _____
- d. Write up results.
- e. Do the same or similar thing on a target person, his/her boss as the target for your channel, and an FSM must be used to execute the ~~target~~ the channel. You may do all the research, etc. yourself, but you must run an FSM to actually ~~pa~~ physically carry out the op. (no letters, phone calls, etc.)
- f. Write up results.

Doc #
8592

Drill _____:

Recognizing basic effectiveness of plans. Take into account effectiveness, security, legality, workability, etc. when making your decisions. Choose which basic plan is best.

- a. General scene: person to restrain/remove, Mr. Jones, employee in local govt. agency attacking the Org.
 1. Order hundreds of dollars worth of liquor in Jones's name and have it delivered to his home to cause him trouble and make the liquor store owner dislike him.
 2. Call up Jones's boss and accuse Jones of being a homosexual.
 3. Send Jones's boss evidence of Jones accepting bribes on his job, with copies to police and local FBI.
- b. General scene: a psychiatrist who has instigated attacks on the org via police and press.
 1. Expose his Nazi background to the press with evidence that he still attends local Nazi meetings.
 2. Wake him up every night by calling him on the phone and threatening him.
 3. Send an FSM in to be a patient of his for a year to disperse the psych during sessions.
- c. General scene: a newspaper executive Clyde McDonald who's behind local attacks.
 1. Poison him while he's asleep so he'll never start another attack.
 2. Make known to the paper's owner that McDonald is responsible for the paper's decreasing advertising revenues.
 3. Spread a rumor around to the paper's employees that McDonald is a communist.
 4. Put itching powder in McDonald's clothes so he'll scratch himself all day, thus preventing him from writing a story.

- d. General scene: a grammar school teacher who got an applied scholastics grant cancelled and is continuing to cause trouble for ASI in other schools.
 - 1. Cleverly kidnap her and run reverse processes on her while implanting the phrase, "I will never attack ASI again, I love ASI."
 - 2. Get copies of the court records where she was found guilty of child molesting and send a copy to the school principal, board of education, and a few school childrens parents.
 - 3. Send a male FSM in on her who, after she falls in love with him, will get her to move out of the country with him.
 - 4. Pay ten of her students to write dirty phrases about her on the schoolroom blackboard.
- e. General scene: a local Catholic bishop is causing many local attacks on the org.
 - 1. Send several FSMs over to the Catholic church to swear at him in confessionals.
 - 2. Connect him up to abortion and/or pornographic activities.
 - 3. Write the Pope an anonymous letter stating that the bishop is really a rabbi under cover.
 - 4. Spread a rumor around town that he's against air pollution.
- f. Mock up 5 similar examples as above on your own, noting the correct answer.

- i. Third party a group to another group ensuring that you get as your product an observed conflict between the two.
- j. Write up results.

524-J

SECURITY OF PENETRATION PEOPLE



Aside from normal action of briefing person on security also do the following:

1. Have all folders pulled on person and stored in safe location or in go including personnel folders, ethics folders, pc folders. Have person removed from any mailing lists. Notify US to have this done in other areas, include ASHO, AO etc.
2. If needed do up a dummy ethics order and have a copy printed for you and person backdated declaring them, etc.
3. Do not use office phones for comm as they may be tapped.
4. Brief them so they fully understand what is needed and wanted.
5. Give them over to a competent CO.

(17)

1000-CV

4 November 76

COLL OFF FLAG GO

Re: Security Measures Taken w/FSM's

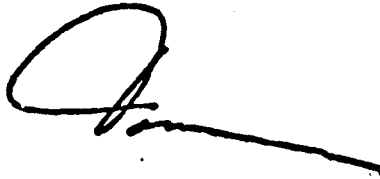
Dear Randy,

1. Ensure that the FSM's don't have any familial or other PTS sits on their lines.
2. Ensure that the FSM has a believable background and that they know it.
3. Ensure that phone calls are made in code and that if something hot needs to be communicated that a meeting is set up - the meeting set up is also in code.
4. Ensure that any auditing of the FSMs is done at the safe house and not in their homes.
5. Drill them on being alert to tails.
6. Any offensive action that they take is drilled before the action is taken.
7. Ensure that they give a real background on personnel application: which doesn't include SCN.
8. Any meetings not in homes are in places where they will not attract undue attention or look like some sort of weird, criminal activity. (ie. drug connection, etc.)
9. Where possible, the FSMs do not let people they work with know where they live.
10. They don't give out their phone numbers to others.
11. They maintain no financial, or other tracable ties to former addresses.
12. If they have some sort of PTS, etc, sit to handle they are not put on any sensitive cycle until that is handled.
13. Auditors and others not in the GO who come into contact with these FSMs don't get any info that they don't need to know about the FSMs, or their jobs.
14. They have no SCN materials in their houses.
15. They have any sensitive material locked up.
16. They xerox things that are needed in the office, instead of taking out a file, prolonging the cycle and endangering the connection to the church.
17. Where attention is drawn to them or a possible connection between them and the C of S and an adequate cover is mocked up to divert attention away from their area.

18. Whenever an FSM is directed into an area in which they have to get info which may present a hit of an outpoint, a suitable cover is designed for them to be in an area BEFORE they go there, and also worked out as to what their response would be if they were discovered.

That's about it.

Love,

A handwritten signature in black ink, appearing to be 'Tom', with a large loop at the start and a long horizontal stroke extending to the right.

Tom.

After you have the documents, you have to put them in a presentat, form and send them uplines.

There is currently a large backlog in CDC material - probably about two feet of material - and the backlog grows weekly.

Therefore, you have to have an order of priority in sending material uplines.

Following is the order of priority I use with some exceptions:

1. data on Scientology that deals with a PT situation - Snow White material first.
2. data on Scientology that deals with a past situation - Snow White material first.
3. Incident material on Interpol.
4. non-Scientology information re Interpol (comm lines, finances, minutes of meetings, etc.)
5. incident material on other enemy groups.
6. non-Scientology information re other enemy groups (comm lines, etc.)

Before a pack of material is sent uplines I put it all in date order and retype any documents that will not xerox well. This retyping takes the most time of any part of the admin cycle.

Also, if there are a number of different files I'll divide them up into separate packs, usually along the lines of the individual file folders they were found in. Sometimes, where there are no logical divisions between the different file folders, and there is a lot of material (such as the Interpol material), I'll just combine all the different files and put them all in late order and send it uplines with headings like "Interpol Correspondence, Jan - May, 1965". The packs should be no larger than can easily be handled and stapled.

The pack is then ready to be excerpted. While excerpting, the C's and I's are counted and any data of interest is noted on a separate sheet of paper for later follow-up.

The excerption sheet is then typed up with two cc's.

Routing is as follows:

- one copy goes to SEUS Sec(AE) (or via SEUS Sec to Br I Dir at'l if it is Snow White material),
- one copy goes to CSG Comm-Csg(AE) - this is the original excerpted copy,
- If it is Snow White material a cc just of the excerption sheet goes to CSG Asst SW,
- an extra copy(AE) is made up for W and sent to SEUS Sec. This routing, however, is not shown on the cover sheet.
- The copy is retained, routed through the AG to the Branch I files.

After the excerpting, you need to make one copy of the excerption sheet (before you made two cc's when typing it). If it is Snow White material, you need two copies - one for CSG Asst SW.

copy is not required to be re-excerpted in red. CSC gets the original excerpted copy.

When all the reports are compiled they should be put into envelopes one addressed to SEUS Sec which contains his and KW's copy, and one addressed to Con Comm US which contains CSC's and CSG's Asst SW copies. These envelopes are sealed with tape, marked "personal", and hand routed to the AG's office for the mailpack. The file copy is also hand routed to the AG's in-basket on her desk.

If an analysis of the documents was done, that would also go into the envelope to the SEUS Sec.

It is smart to try and stay on top of the CDC admin and ensure that at least one report a day goes out.

Also, if you have a spare 15 minutes here or there, use it on retyping documents.

OPS OFF

Ops Officer is responsible for the planning, researching and carrying out of ops (planned and put together locally and approved by US Ops or or sent down from US)

This includes coordination with Coll Off as to ongoing hot areas and close comm with Br I dir as to areas needing Ops planned for them.

Responsibility extends to the following areas:

1. ENSURING THAT WITHOUT QUESTION OR ANY RESERVATION THAT NOTHING DONE IN THE OPS AREA BOUNCE BACK AT THE CHURCH OR PUT THE CHURCH IN ANY JEOPARDY.
2. Ensure that needed security precautions are kept in regarding clean (no fingerprint materials) so that source cannot be traced on ops.
3. Hat sufficient FSM's to carry out the bulk of routine ops work (typing and stuffing of envelopes)
4. Hat personnel or carry out needed surveys and research for ops or have research done by Coll Off as coordinated by Br I Dir.
5. Have a safe place to store ops materials and maintain an adequate supply of clean material and instruments (ops typewriter).
6. Take the time to do ops right. It's worth it to do it right and not cut corners..

TYPE OF HEARING	<i>Final</i>
CASE NO.	<i>C420153</i>
EXH. NO.	<i>iii</i>
FOR IDENTIFICATION ONLY	
DATE	<i>5-22-84</i>

Operations Definitions

See 7/8/7

8591

BUTTON SURVEY: A comprehensive examination, inspection, researching or investigation of persons which have control or influence over an attacker's position of power to discover what they hate and love. Also the same activity in relation to the attacker to discover what he considers valuable or what he is protecting. The results of surveys are what Operations plans and channels are based on.

CHANNEL: (dictionary) The medium or route by which information, trade, influence, etc. are transmitted. Any means of passage through which something moves or passes.

(Ops) The way in which Operations buttons and data are utilized to bring about an enemy restraint or removal. There are usually 3 channels to an Operations project or plan.

INCIDENT: (dictionary) A definite distinct occurrence; an event. A relatively minor occurrence or event that precipitates a public crisis.

(Pl, G01150) "...any created incident and the result of such."

(Ops) A set of circumstances or event created covertly (stage manage behind the scenes), exceeds the standard enemy defenses, and which is of detriment to the enemy when exposed. It can be exploited by Bl or FR.

REMOVED: past tense of remove. Remove (dictionary): To take away. To do away with; eliminate. To dismiss from office.

(Ops) An attacker of Scn or Scns dismissed from the position of power from which he attacks as a result of Operation's actions.

RESTRAINT: Any influence that holds back from action, checks, represses; that limits or restricts, inhibits; that restricts freedom of action by either moral or physical force frequently for one's own good.

(Ops) An enemy restricted on a gradient scale, from covertly to permanently, from attacking Scn or Scns as a result of Operations actions. For statistical purposes restraints are classified as either "serious" or "mild".



DATA NEEDED BY OPS ON EACH LOCATED WHO

- ★ 1. Standard ODO with time track and a brief, summarized, well-rounded picture of terminal. (Following # 2,3,4,5&6 are the key areas data is needed)
- ★ 2. Criminal background of terminal.
- ★ 3. Financial involvements (inflow & outflow of money)
- ★ 4. Legal involvements (summary of actions)
- ★ 5. Terminal's main interests, personal habits, fears, vices and any other items of interest.
- ★ 6. Friends and enemies on the terminal's 1st Dynamic
Friends and enemies on the terminal's 2nd Dynamic
Groups that the terminal belongs to and any groups or terminals, who are enemies of that group.
7. What the terminal considers valuable & is protecting
- ★ 8. Simple org board the terminal is on, clearly noting his position and his seniors and noteworthy juniors.
9. What persons have the power to fire terminal from the position he holds.
10. Any rules or regulations that if broken would cause the terminal to lose his job/position.
11. Any regulations concerning licenses that the terminal holds that would cause him to lose his license if violated(ie. law, medical, contractor, etc.)
- ★ 12. Scandals, conflicts, disputes directly or indirectly connected to terminal.
- ★ 13. Documents that show criminality of terminal (ie. cheating on income tax, discrediting data in personal letters, use of drugs, etc.)

14.

15.

Ops Planning

Ops planning goes over all the data on the WHO that Ops research has compiled and with all the data available on the WHO, plans out channels of attack on the WHO that will effectively remove/restrain the WHO from his position of power. Ops planning on a WHO is done using the data series, target series, all Scientology tech applicable, and intelligence tech. The following points should be followed in planning an operation:

1. Initially plan out at least 3 channels of attack with the data you have at hand. Do not wait forever to get all data collected, but also do not run Ops that would be dangerous without essential data. Basically a brighter idea is needed with less data available. 3 channels being done instead of less is because there is a higher percentage of getting results and also this will tend to confuse... and spin the WHO as there are 3 attacks instead of just one.
2. Continue to plan Ops utilizing feedback from completed Ops so that the WHO has persistent attack on him and continual pressure. Do this consistent attack until the WHO is obliterated.
3. Stay away from harassment actions that are only for the sake of doing channels or revenge. ie: Sending pizzas from every Pizza delivery restaurant. These basically have been unsuccessful as they do not achieve any real effective result, except for letting the WHO know that he is under attack. There may be times when 50 pizzas every day being sent to a WHO would be effective, but this would be in such a case where the WHO was restimulated heavily by seeing pizzas, smelling pepperoni or seeing pizza delivery boys, etc.
4. Always include a way of getting feedback in an operation, so you know what type of result you are getting and for further planning of channels in those areas that give good results.
5. Ensure proper security is planned in an operation, ie: use of an untraceable typewriter, paper without fingerprints, proper covers by FSM's, etc. (See security write-up and security section data in hat materials of Ops US hat checksheet)
6. Use the target series exactly to programme out an operation on a WHO. Ensure the major target is based on a real, current situation and is an achievable purpose.
7. Find out what the exact resources are for the area the Op will be implemented in and what the capabilities are of your terminals implementing the Op.
8. Keep the targets in an operation simple, yet complete.
9. Analyse properly the actual situation with the WHO and what the best line of attack should be done by the GO as a whole. It may be necessary to suggest that PR or Legal do some specific action as a finishing off of the WHO. Never wait for another bureau to handle a WHO, as Ops is responsible and has the capabilities to handle WHO's totally without the other Bureaus in the GO. Liaison though is very important with the various GO bureaus, specifically the Legal Branch 2(attack area of Legal) and PR Branch 1(attack area of PR).
10. A believable source must be provided in an operation, thereby

CO HATTING

Case officer is responsible for running the penetration personnel recruited..

CO is responsible for hating on security, hating as operative, defining objects as assigned by penetration I/C and ensuring that objectives are achieved.

CO is responsible for operatives ethics both as regards work and personnel and for this reason should be familiar with PTS tech type A and type I handling and phenomena. Should keep operatives morale up.

CO sets meeting time and place, responsible for overall security. Hat of personal security of the operative belongs to the operative. Hat of product officering and pushing for completions is that of CO--must be done with ARC and not to extent that operative is not maintaining proper security or is not false reporting to "protect self".

(ex. Order go to zoo, have crocodile open mouth and count teeth by yourself now--reply Sure--crocodile has 17 teeth (lie))

Ensure that if person unwilling that they can tell you about it and handle bug instead of false reporting or pr'ing.

The Key to being a good CO is to stay in good comm with the operative. Often the CO is the single link between the operative and scientology. As such the comm line must remain clean and open.

Therefore I never yell at an operative or hit them with heavy anything. I handle gently, using data series. Let them know when they are doing well, validate them for wins--let them know Br I area in upper condition when it is, at let them know in very vague terms of wins in other areas.

Usual procedure is to sit down, polish off business if first 5 or 10 minutes of meeting and then spend remainder of meeting (hour or so) just being in comm. Let operative talk, blow charge, get off considerations or whatever. Just be there as a friendly, interested terminal. Be businesslike for handling business and then let them know--so much for business, have coffee cigarette and just chat. If you feel good about being with them they pick this up and high arc level can be maintained.

~~xxxxxxx~~ Cardinal rule to be observed is no 2D involvement with any operatives. You will pay if you violate this rule and may pay very heavily.

Personal ethics of operative is under supervision of CO. Anything which affects the FOM's ability to work or function or produce or production is legitimately the domain of the CO regardless of what.

CO is able to locate such areas and get FOM to confront and handle whatever needs to be handled in area to keep on top of situation. If it does not affect work it is very wise to know about but unnecessary to do anything about it.

90 - C V

Ex. operative wants to "have an affair" with Wog. Give good R-factor on exact position FSM would be putting self in regarding must of maintaining security and never disseminating to wog and being on constant withhold, on never being able to tell and make it clear that this is the case..

Then put it to FSM--if you can handle it go ahead, watch for any bad indicators and check this area in casual conversation frequently. Ex. How is it going with Bill?

Make sure that FSM able to talk with you about most anything (high ARC level ensures this) Do not make FSM feel wrong or inadequate etc. Let them know that they are doing a hard thankless type work and are appreciated and valued, etc.

As a standing rule only handle to point that FSM capable of handling for self. Handle toward this. Ex. rollercoastering-- check for PTS and if SP located work with FSM on handling he or she can do. Ex--running around with several men and no time for work production down--find out why not producing. Let FSM know that running around with men detracting from work and that if she wants to do this it is her business so long as she produces and that it doesn't interfere.

I have had several instances of FSM/wog 2 d activity. They have resolved with R-factor on exactly what situation is and probable results. FSM dropped wog. Had one case of FSM caving in on relationship with married wog--found on inspection to be PTS 1 to person at evening job--xxx problem not with married wog at all--person could handle this.

If at all possible arrange autiding for your people.

Make sure that you stay in comm with people (minimum of one meeting together a week.)

Best way to arrange meetings is to set up next meeting at current one--this eliminates phone calls which can be tapped and enables good scheduling.

Simple phone codes can be used for signaling as needed

CO must communicate to operative that CO is out for operative and will do all possible to protect and take care of operative..

Best way to judge operatives is by their production.

Best way to run area is to get competent people and put them on job, brief them, let them get on with it, debug as needed and when they do well let them know. Extensive management not needed if competent well-briefed operatives there.

Let them propose solutions to problems, etc-

Best to plan ahead regarding FSM leaving job to ensure that FSM replaces self--work with to ensure this.

Let other FSM's be volunteers and doing it because they are dedicated and want to. I try to keep ordering at a minimum and simple requests at maximum. Then a simple request has effect of an order--they just do it because they want to.

If you can't tell FSM something--let him or her know that
If you can't do that--lie well.

One particular occupational hazard is that you are training these people to lie well, deceive, be tricky. There will often be a certain point where probably just out of cockiness or because it appears to be a workable operating basis they will try this with you.

You better be sharper and just let them know that it's good to be ~~km~~ clever and all but not with you.

Better to have them tell you that they decided to go fishing instead of working and ask this and say--well now I want you to get me the file than to chop them for this so that they will try and put by some sort of story the next time instead of telling you about fishing.

If you listen, repeat objective and let them know that you need and want fuel and so do they next time they won't go fishing, or if they do there is a sit. to be unraveled..

For some of finer points on dead drops etc. see Spy and Masters or Pridhkov lecture in the Pentkovsky papers.

STATS: (SEE ATTACHED WRITE-UP ON THE STATS)

1. ENEMY FILE ON SCIENTOLOGY, EXCERPTED CORRECTLY AND ON LINES - 50 pts
2. INCIDENT(S) PREDICTING AN ATTACK ON SCIENTOLOGY SHOWING WHO, WHERE, WHEN, WHAT. - 50 pts
- 2a. UNPREDICTED ATTACK - MINUS 50 PTS.
3. INCIDENT(S) DOCUMENTING CRIMINAL OR SCANDALOUS DATA ABOUT AN ENEMY - NOT PUBLICLY KNOWN - 20 points
4. INCIDENT(S) PREDICTING AN ENEMY ATTACK ON SOCIETY SHOWING WHO, WHERE, WHEN, WHAT. - .15 pts
5. INCIDENT(S) DOCUMENTING CRIMINAL OR SCANDALOUS DATA ABOUT AN ENEMY PUBLICLY KNOWN - 2 pts
6. ENEMY CONNECTIONS (PER G.O.1150, note these are usually gotten in high volume and so have a lower point value) - 1 pt
7. TIPS (PER DICTIONARY DEFINITION) - 1 pt
8. INCIDENT(S) SUPPLYING DATA TO PR, LEGAL, FINANCE OR ANOTHER G.O. GROUP - 1 pt.

0-0033

Confidential

OPS WRITE-UP

OPERATIONS OFFICER STATISTIC

Item:	Pts.:	#of:	Total
*1. A located enemy WHO or potential WHO removed from the position of power from which he is attacking or could attack.	(250)	_____	_____
*2. A located enemy WHO or potential WHO seriously restrained from attacking and whose position of power is seriously damaged.	(175)	_____	_____
*3. A located enemy WHO or potential WHO whose position of power has been impaired and/or his ability to attack is reduced and impeded.	(75)	_____	_____
4. A predicted attack prevented or depowered.	(50)	_____	_____
*5. A channel completed that results in an attack on a located enemy WHO or potential WHO in:			
(a) national or opinion leader type media.	(50)	_____	_____
(b) local media or non-opinion leader type media.	(20)	_____	_____
6. A full Ops channel off a programme/project completed. (US or other origin in standard Ops format)	(20)	_____	_____
7. A predicted attack not prevented or depowered.	(-50)	_____	_____
8. Any part of an operation blown where the enemy has evidence that it was of C of S origin.	(-250)	_____	_____
TOTAL _____			
* This applies to enemy groups as well, ie: (1) enemy group destroyed or taken over; (2) enemy group condition or position seriously damaged; (3) an enemy group condition or position impaired or impeded.			

Explanation of counting stats:

The overall result for each WHO or group is looked at on a weekly basis and the single applicable stat is assigned, rather than having a multitude of restraints or serious restraints. ex: Joe Blow has the IRS move hard on him, loses his wife, gets sued and gets a traffic ticket, would not be four restraints but would be considered one serious restraint as an overall result on Joe Blow.

Per #5 above, it was necessary to make a separate section for counting channels that resulted in media attack on WHO's or groups. #5(a) is a channel that gets extra points for a national/opinion leader type media attack, such as Time Magazine, national TV show, etc. #5(b) is the same points as a regular channel completed. Neither of these channels are counted in the #6 stat section, but are just specialized type of channels.

Burglary

Definition: Every person who enters any building with intent to commit grand or petit larceny or any felony is guilty of burglary. (p.1,a; p2.,a)

Defendant's entry into room to take personal property for temporary use, without intending to deprive owner thereof permanently, is not burglary. (p5.,a)

Burglary may be committed by a breaking on the inside and it is burglary to enter an inner door with an intent to commit a felony even though the inner door was unlocked. (p7,a)

Evidence that employee devised plan to steal his employer's property, that such plan involved entry into employer's store by other persons for purpose of taking delivery of property, and that one of such persons was induced by employee to enter store for expressed purpose of aiding and abetting him in consummating scheme to defraud employer was sufficient to sustain employee's conviction of burglary. (p1.,b)

One who enters a room or building with intent to commit a felony is guilty of burglary, even though permission to enter has been extended to him personally or as a member of the public. (p8.,a)

One who enters a room or building with intent to commit larceny is guilty of burglary even though express or implied permission has been given to him personally or as a member of the public. (p8,b)

Nighttime burglaries of a building currently used as sleeping and living quarters is burglary in the first degree, and all other burglaries by unarmed persons of other buildings, whether occupied or not, are in the second degree. (p11,a)

Punishment: Burglary in the second degree: by imprisonment in the county jail not exceeding one year or in the state prison for not less than one year or more than 15 years - in trial judges discretion. (p12,a, 13,a).

#

H

- * " " - Saint-Helena

Sept 2.

Plan for disguise

To create the image of an aging guy wanting to look hip as a means of regaining his youth a bit.

Mock-up would be as follows--

1. A somewhat mod wardrobe, bright colors, open necks, necklace, rings on fingers, cigarette holder, tan.
2. His head will be shaved and then HAIR'd to create "bays" and the impression that he is partly balding. This would involve shaving and plucking to create hairs and then using hair on bald area and using a sun lamp.
3. The contacts would be rechecked with the doctor who gave them out to see if they can be worn more often and for longer periods--debug. If not different frames would be gotten for his glasses.
4. His tooth would be capped.
5. He would lose some weight (or gain it) as he wished. Preferably lose some weight.
6. His eyebrows would be lightened and plucked. His hair done a light blonde. Side burns grown a different length.
7. Earth shoes would be gotten to change the posture.

These are the contemplated changes for Jeff.

11678

Jan 76

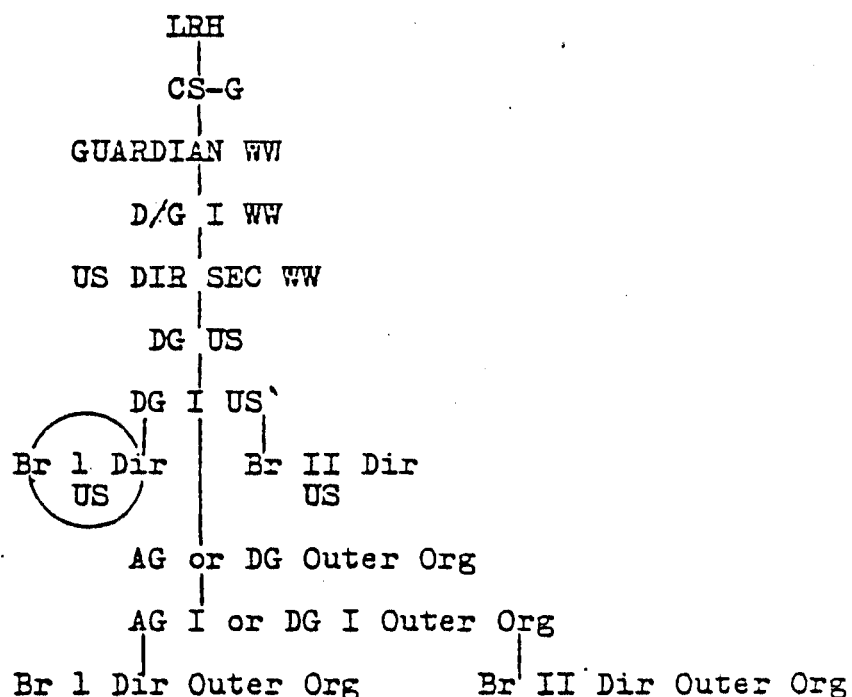
Branch One Director US Hat Write-up

3797

Gr

A. Purpose of Post: To see to it that external situations of opposition to LRH and Scientology or potential such external situations are estimated and communicated to those who need to know; and to see to it that external Whos behind oppositions to LRH and Scientology or potential such external Whos are located and restrained or removed either directly or in liaison with other Bureaus.

B. Position on the Org board:



C. Duties of HAT:

- C-1. To ensure that the proper priorities are kept aligned at all times as much as possible. If it should necessitate other less important cycles bogging or getting backlogged for awhile, fine. Get the important things done well first.
- C-2. Know what is important to the establishment both long range and in PT. Long Range importances are in policy, GO's and programs. Short range ones are in projects, orders, info and verbal liaison. How to find out about policy, GOs, programs, projects and orders is obvious. Info and verbal liaison is totally created from the post; and I have found that these do not just start and continue, they have to be

continually created. You have to let people know what kind of data you want and remind them from time to time. Also the more you exchange info with others the better the line stays in as the other terminal considers the line more valuable than when he receives no exchange - although this exchange of info isn't always possible as Br I data has security restrictions. Some lines I have found valuable are: (a) with Br II Br I regarding Br I publics that are connected to Br II sits; (b) with DG Legal and Br II Dir Legal regarding the course of litigation with enemies and data that Br I Br I can supply about those enemies or litigation plans, etc. to Legal; (c) to a lesser extent Br I Legal, usually regarding any indicators or hassles on Scn corporations from external agencies or entities; (d) Br I Dir PR regarding attacks on enemies and any data Br I Br I can supply for those attacks; (e) to a lesser extent Br 2 Dir PR regarding entheta already printed or data about what happened (good or bad) when trying to get a false report corrected; (f) to a limited extent from the Service Bureau regarding data of interest about my juniors locally or in the field that may come up in auditing, cramming, ethics or training cycles. (g) Soc Co-Ord regarding any external problems they encounter, and just their general plans in any area, what programs they are working on etc. in what areas (ie, if a Narconon or ASI is trying to get funding or a project started you can ~~expect~~ expect perhaps some opposition from local Br I enemies, etc); (h) From the DG I - this has been my most valuable info line and is mostly verbal. This line often contains data and info regarding the plans, etc. of other bureaus, and from DG US, Seniors at WW, CS-G and LRH. This line occurs randomly at the convenience of the DG I approximately 1-5 times daily. Lines A-F are mostly dispatch-info lines which get verbal only on clarification or when some co-ordination on an action is needed.

C-3. Know what is going on in collections, operations and CIC. This is done both by being on the written comm line and by verbal info and briefings. A weekly Br I target (battle plan) meeting is a good method to get info all at once when all are present. This is the only regular verbal, the other verbal lines occur randomly daily.

C-4. The greatest importance of C-2 and C-3 above is that the Br I Dir pulls them together as a major duty and activity of his post. This is the basis of estimation and being able to discern what is important (priorities). And this is the heart of what the Br I Dir post is all about.

- C-5. I don't have any hints on how to pull C-2 and C-3 together except to make sure you get both of them in as well as you can and know your basic Br 1 material (PLs and GOs) and I think you will find it just works. GO "Int Its Role" is probably the best source on how this is done.
- C-6. What you should find yourself doing as a result is: (a) noticing dangerous or potentially dangerous situations that need to be communicated to seniors, other bureaus, etc. and doing so with as full data as possible and with a recommended handling as applicable. (b) noticing indicators of potentially dangerous situations and making sure that your juniors follow them up as is appropriate to the priority of the matter. (c) recognizing when a Who behind opposition is really located and that person requires and gets attention for handling and gets handled. (d) recognizing when a who hasn't been found and making sure he gets found so that he can be handled and so that wrong targets aren't hit with resultant wasted time and resources.
- C-7. Anything can be done in Br 1 as long as the above points are done, and you as Br 1 Dir see that it gets done.
- C-8. See to it that security is in on Br 1 activities, specifically field activities, and to base the quality of security around the product to be obtained - not basing the product around security. In other words, product comes before security. This doesn't mean it's okay to be out-security as long as you get the product. It means you work out how to get the product and work out as well how to be secure in doing that.
- C-9. Ensure that CIC files are always kept in PT and x-filed properly.
- C-10. Ensure that when juniors are about to embark on an assignment (especially in covert data collections and ops) that they do not have Bad Indicators, disagreements, etc. and if they do to ensure that it gets handled or another person is assigned to the task before it is ever activated.
- C-11. To ensure that juniors are operating off of the proper priorities.
- C-12. To ensure that any technical data or techniques peculiar to Br 1 that aide or are needed to get production are obtained and put into usable form

or written up by those who have proven success at them.

- C-13. Ensure that CIC files are not viewed by unauthorized or insecure personnel from other bureaus; or used by authorized personnel in unauthorized manners - require a CSW for viewing or use.
- C-14. Ensure to the best of your ability that Br 1 problems or emergencies that cross your plate are handled or put into the proper area for handling and do not fly up to any senior to handle. While this is a standard duty of every staff member it is particularly important in Br 1 because so much of Br 1 data can initially appear to be "rush" or "vital data" that needs to be communicated to one and all ASAP. While such is often true, I have found that approx 80% of all such data when initially received at the Br 1 Dir level either contains a problem for a senior or leaves some questions to be answered which can be usually resolved rather quickly or overstates the danger of the situation or understates the danger of the situation. It is up to the Br 1 Dir to spot these and get such remedied before they get passed on.
- C-15. Ensure that seniors at the local level and up lines are kept well informed, especially about the major situations and handlings in Br 1. I have often found this difficult and know that my counterparts have as well because it "seems to take too long when I should keep producing or handling" or some other such consideration. Actually I have found that when I go compile such reports I end up knowing much more about what I'm doing and what is really going on than when I started writing the report.
- C-16. An extremely important concept to get and apply as a Br 1 Dir, so important in fact that it can mean the difference between success and failure on the post, is that the best defense is a good offense or outflow is holier than inflow. Whatever way you want to put it it is contained in many LRH policies, especially in relation to the GO. It would serve as a good motto for Br 1. It's actually quite magical. Things boom when Br 1 is attacking and morale gets very high. Don't underestimate what this can do, you have to do it and experience it for yourself to really get it. A good example of its use is when you are being attacked in some Br 1 scene and find yourself doing only defensive actions and feeling like everything bad is happening. Get on the attack in that scene! Pick a right target and attack heavily, you'll see what I'm talking about.

C-17. More specifics on the Br 1 Dir post and what to use as a guideline for success in Br 1 as I have operated it are expressed in the attached write-up "Concerning Br 1 US, Most Successful Year", which lists the successful and unsuccessful actions for all areas of Br 1 US.

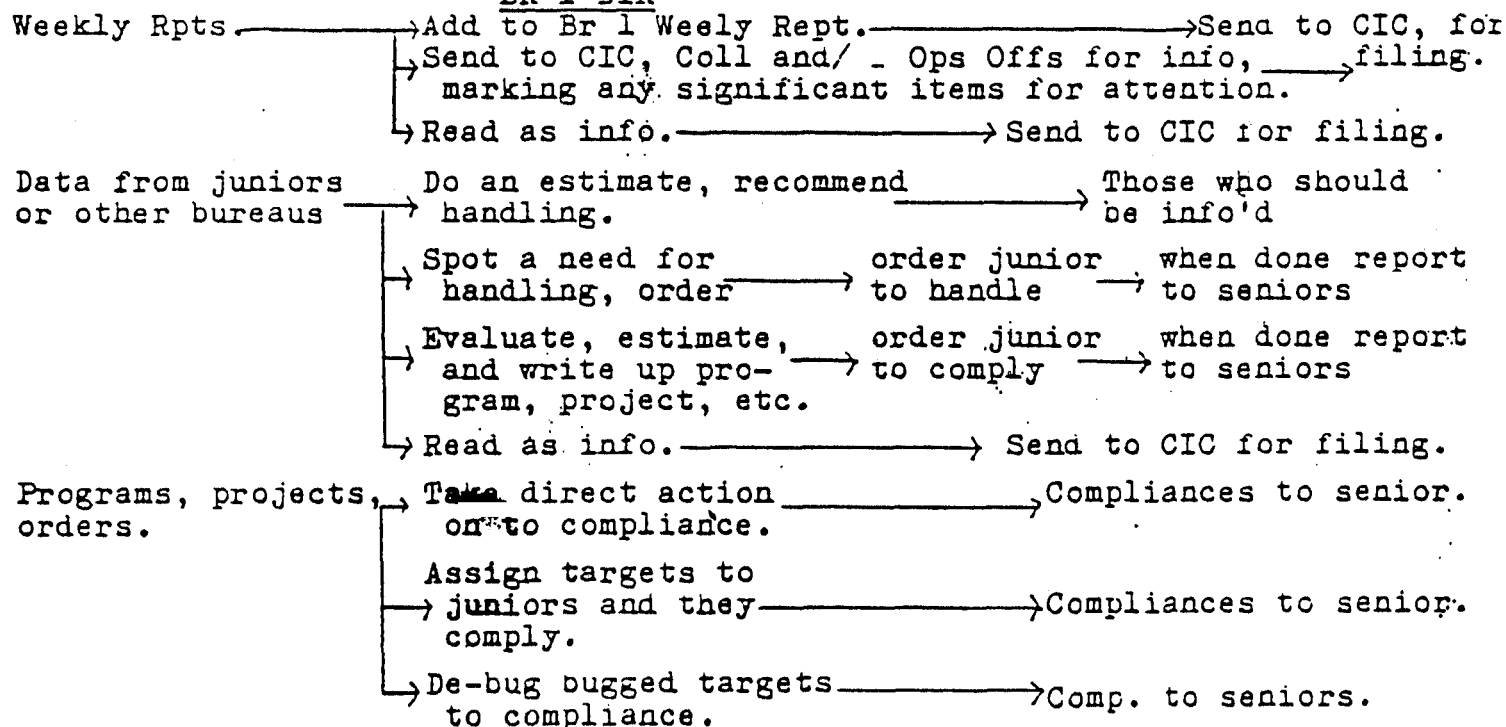
D. Checksheet: The checksheet for Br 1 Dir is the B1 checksheet minus the Br II items. And the Operations checksheet.

E. Materials: All materials for the checksheet are available in the Service Bureau or B1.

F. Org Board: see B.

G. Flow chart showing what particles are received by the post and what changes the post is expected to make in them.

BR I DIR



H. The product of the post:

1. Current or potential external situations estimated and communicated.
2. Current or potential Whos located and handled.

I. I have not come up with a stat that totally satisfies me. But two which have worked out satisfactorily are in order of use.

1. Combined total points of the Coll Off, CIC Off and Ops Off.

2. Combined total percentage of increase or decrease of each of the total points of the Coll Off, Ops Off and CIC Off. While more complicated to figure, this one is more accurate than the first.

The formula to figure the stat is:
(done separately for each section, Ops, Coll, CIC)

This weeks total points for that section. minus Last weeks total points for that section. equals

plus or minus "X". Then: "X" divided by the "Base Figure" equals

plus or minus "Y" %. Find the "Y" % for each section then add them all together to get the Br 1 Dir stat. total.

The "base figure" is the total points for that section the first week that section existed, or the first week you started to figure your stats this way.

As an example: the first week Collections started producing its stats its total was 100. This is your base figure. The next week it produced 125 points. So the % for that week is 25%. If the following week 150 points are produced, the % would again be 25 %.

Do this for each section each week and add up the percentages which is the Br 1 Dir total for that week and which will be added to your total from last week. Example:

<u>Last week Br 1 Dir Total</u>	<u>This weeks total +/- % of increase/decrease</u>	<u>This week's Br 1 Dir Total</u>
2652	Coll: +25%	
	Ops: +05%	
	CIC: -05%	
	<u>Br 1 Dir points: 25</u>	2677

The Coll, Ops, and CIC points scales are attached.

BR I DIR US.



FACT SHEET: Gabriel CAZARES
Mayor of Clearwater, Florida.

58

FACT: Mayor Gabriel Cazares is said to have been born in Alpine, Texas on Jan. 31, 1920. This was taken off of his handout minicoed vitae of his background.

FACT: That the County Clerk of Alpine, Texas has confirmed that Alpine, Texas has no record of him being born there. County Clerk phone number-1-913-837-2213.

FACT: Mayor Gabriel Cazares claims to have attended and to have received Mn MS (Master of Science) at the Jackson College, Honolulu, Feb.-May 1957 in Business Management.

FACT: A check with the Hawaiian Telephone company shows no listing for a Jackson College in Honolulu. Oahu, Maui and Kauai were checked. A further check with an office of the St. Andrews Priory School, a long time established school in Hawaii-about 100 years, determined that a Jackson College is in fact not listed with the Hawaii Department of Education presently. It was further checked with the headmaster's secretary of St. Andrews as to the existence of any such college. The secretary, a resident of Hawaii for over 50 years did say that there was such a college, but that it went broke and out of business in the 1960's. The school, when in operation

These records are on microfilm at the Pinellas County Courthouse in Clearwater.

59

it was operating out of a small house in Manoa Valley

FACT:

City of Clearwater Ordinance No. 1593 passed on second reading and adopted on Dec. 4, 1975 states that "...persons seeking nomination or elected to office in the City of Clearwater shall prepare and file with the City Clerk of the City of Clearwater in affidavit form a disclosure statement containing a listing without reference to amount of sources of income, including trusts, of the parties named herein, each person's spouse and minor children, if any; any interest held by any of the individuals named herein in any business whether it be a partnership, corporation, proprietorship or holding company; all real property whether owned in whole or in part in the State of Florida by the individual named herein...."

This ordinance further states... "Section 5. Any person, organization, society, association or corporation, or any agent or representative thereof, who shall violate the provisions of, this ordinance shall be subject, upon conviction, to a fine not exceeding the sum of Five Hundred Dollars (\$500.00), or imprisonment for not exceeding sixty (60) days, or by both such fine and imprisonment in the discretion of the Judge."

It further states... "Section 8. This ordinance shall become effective immediately upon its passage."

DATA:

The records show the Mayor of Clearwater has not filed his financial Disclosure Statement per the law, which he himself signed on Dec 4, 1975. To not immediately file is to be in violation of the City Ordinance No. 1593, which according to the ordinance, if convicted, one not filing could get up to \$500.00 in fines, or imprisonment not to exceed sixty days (60). City Clerk, Clearwater, Fla.

60

FACT:

Presently Mayor Cazares is on record at the County Court-house as owning, as an individual not a company or corporation, a total of 16,800 square feet of property in Clearwater. The records also show that he has had three other properties in Clearwater which were sold at 5 times the cost. One of these properties was financed by the Clearwater Neighbors. That one he bought for \$2,100 and it was sold for \$17,900. He bought the property on 21 August 1972 and sold it on 19 September 1973.

One of the properties he presently owns was also financed by Clearwater Neighbors.

According to State Corporation records in Tallahassee, the Mayor was a director of Clearwater Neighbors in 1969. The annual reports for Clearwater Neighbors show that the Mayor was Chairman of Clearwater Neighbors for years 1972, 1973, 1974. The annual report for year 1975 has not yet been filed.

The Mayor's wife, who has been in real estate since early 1970's is presently with the Clearwater Neighbors.

1166

The Clearwater Neighbors have purchased at least eight(8) pieces of property in Clearwater, costing more than \$60,000. 61

Seven of these properties were financed through an out-of-state corporation (Alabama), Molton, Allen & Williams Indorp., which has an office in Tampa.

Molton, Allen & Williams have financed over 5,000 properties in and around Clearwater and Pinellas County.

One other property that Clearwater Neighbors has was financed by Stockton, Whatley and Davin. This firm has financed over 5,000 properties in and around Clearwater and Pinellas County.

Molton, Allen & Williams Inc., 1501 S. Church, Tampa, an Alabama corporation, financed most of these property purchases for Clearwater Neighbors between early 1970 up June 1972. They are recorded as making their last transaction for Clearwater Neighbors in 1974. -

Since Mayor Cazares has been in office they have continue to make large purchases of property in and around Clearwater.

Property values and many businesses have continued to decline in Clearwater while the Mayor has been in office.

Molton, Allen and Williams and Stockton, Whatley and Davin have both financed 100's of pieces of property in and around Clearwater since the Mayor has taken office.

These records are on microfilm at the Pinellas County Courthouse in Clearwater.

Henry Benhamitarian Deeds Award - Given by the Clearwater Evening Lions Club

Oshe set a 2-mile Track Record while attending Los Angeles City College - He held

FACT:

62

Chester B. McMullen, Jr. filed suit against the Clearwater Sun, Mark Sahleman and others on July, 1975 for defamation. The same day he filed a suit against Mayor Cazares and others. The Plaintiff had been involved in developing "over 400,000 square feet of space for a commercial shopping center and offices and, originally, the building of a restaurant facility off or at the tip of Cooper's Point." McMullen's proposed development was to be a series of 20 multi-family multi-story residential structures.

What proceeded after this land was purchased was the Mayor (Cazares), the Clearwater City Commission and the Pinellas County Planning Council turned down the rights to develop Cooper's Point. Following this denial to develop the land the Clearwater Sun, Mark Sahleman came out with an article on April 19, 1974, and "continuing thereafterthe Defendants for the purpose of ruining Plaintiff's reputation as a citizen and attorney-at-law maliciously exposed Plaintiff to public hatred, contempt, ridicule, distrust and embarrassment...."

"The articles" according to the suit filed,..."in their entirety, and each of them, falsely convey the implication that CHESTER B. McMULLEN, JR.;....."was guilty of criminal conduct and that he as an attorney, landowner and developer was acting intentionally in disregard of the law to his own financial benefit."

FACT:

That following the proposal to develop the land Mr. McMullen and those associated with "Cooper's Point" were turned down by the Clearwater City Commission and the Pinellas County Planning Council, following that articles on "Cooper's Point"

63

and Mr. McMullon, Jr. came out in the Clearwater Sun written by Mark Sableman, which Mr. McMullan charged as defamation.

DATA: The file on this case, which this information came from, mysteriously disappeared early this morning before the file clerk at the County Building the records are in got to work. The sign out card, which one normally fills out with name, address etc, was filled out with only a ^{penned} ~~pencil~~ in name which was illegible. This is according to the file clerk responsible for having the files signed out for.

2. Service to Mankind - Given by Clearwater Noon, Breakfast and Evening Sertoma Clubs.
Also, awarded the District Service to Mankind Award which encompasses several states.

Rilgers Memorial Award - For the first time in history this award was presented to two people - Margaret and Gabriel Cazares. It is considered Clearwater's most coveted award given yearly for outstanding service in the community.

4. Betty Boman Earlen Deeds Award - Given by the Clearwater Evening Lions Club



A walk-in cycle goes generally as follows:

1) You must have a means of access to the building you are interested in. In a government building this almost always means either a government ID (or going in with someone that has a government ID), or an excellent suitable guise. A private building may be as simple as signing in.

When signing in to either a government or private building, the signature should be scrawled and the destination should not be your actual destination. Except in rare cases it is usually sufficient to say you are going to the library or some such place.

You should have a story already made up that will be plausible should you be asked what you are doing. This story also has to be very flexible or else you have to have different stories for different stages of the walk-in. A story that you would tell a guard on your way into the building may be entirely inappropriate if you're caught with your hand in the file cabinet. And it will make a difference if the person questioning you is a cleaner, guard, employee, and where you are, what you're doing, etc. So think it out well before you go in.

2) Locate a safe space in the building where you can sit down and relax and talk without feeling paranoid.

This can be a library table, an empty office - whatever looks good to you, and that you would feel comfortable with. Lots of times in a walk-in you'll have to sit around and wait a couple of hours for your target area to clear out. If you're not comfortable in the area you're waiting the rest of the cycle can go pretty rough.

While you're looking for this space you also have to really assume the beingness of the type of person you're alleging to be. For instance, if your story is that you are an employee of the organization you are in, you have to feel that you are an employee. If a cleaner walks in on you or a guard asks you a question you have to approach your response and manner of response from the viewpoint of your beingness. If a cleaner walked in on you in your office at the Org you'd probably say "Hi" and go about your business. You wouldn't get startled or upset or make some dumb excuse and run out of the room.

3) After you've located a safe space and are relaxed in it you should go out and get familiar with the building.

The first thing you have to locate is a xerox machine because if you can't copy the documents there's not much sense in being there. Also, you don't want to have already obtained the file and then have to waste time in finding someplace to copy it.

(Note: There is always the alternative of taking the file out of the building to copy. I very seldom do this unless I have to. I prefer to copy it in the building because you add too much time to the cycle by traveling to another building. You also have to

sign in and out again with the guard, which looks somewhat odd to an observant guard.)

Most government buildings have an excess of xerox machines. They are usually easy to find. Even most private buildings have a xerox machine in any large office.

You want to choose a machine that is located away from the area that you will be obtaining material from.

In a large government building you simply go to a different divisional area from the target area and find a xerox machine.

If you're in a private building, chances are there are many different organizations in the building. Go to another organization or suite of offices and locate a xerox machine there.

Oftentimes you will find the xerox machine locked. If you are familiar with xerox machines you'll know where the "Main On" button is. (Note: it's a very good idea to be thoroughly familiar with all manner of xerox, SCM, etc., copiers so that you can easily change paper and toner, clear jams, etc.) It will be protected by a locked cover but should be accessible by lifting up or pulling out a corner of the cover. For instance, on the xerox 7000 you simply lift up the corner of the cover nearest you as high as you can without bending the cover, and stick a finger (or a long instrument like a letter opener) in and push down the "Main On" button which is located to the front, just a few inches in front of the middle of the machine. Nearly all copiers are accessible with some variation of this, it just takes looking and experience.

Ensure* that you can turn on the machine, it works, and that you have sufficient paper. Then leave the machine on and leave the room.

"4) Locate the target area. You should already know the room number before going in.

Walk past the room, observing all rooms in the area for any lights or other indications that they are occupied.

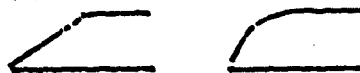
If it is apparent that the room, or rooms close to it are occupied, then go back and wait and check again in 30-45 minutes. But don't get into making a lot of trips past the area.

5) When the area is clear then go to the room door and try it to see if it is unlocked.

(Note: it isn't unusual for room lights to be left on and the doors closed with none in the room. If you have any feeling that someone may still be in a room, then go up and knock. If someone answers, open the door and ask them for a match or to use their phone, or some such. Also use the opportunity to look at the door latch so that you know its configuration.

If the door is unlocked, just open it and go in.

If it is locked then you have to figure out a way in. The most successful ways of opening a locked door have been variations on the credit card. This can be used if the latch is slanted or curved going into the door jamb:

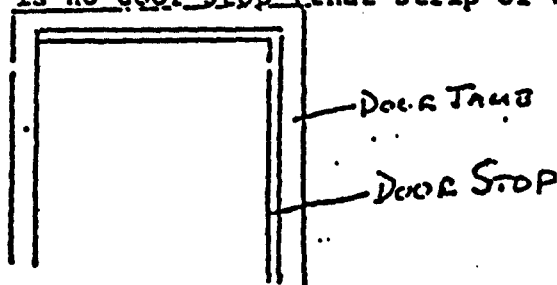


If the latch is straight



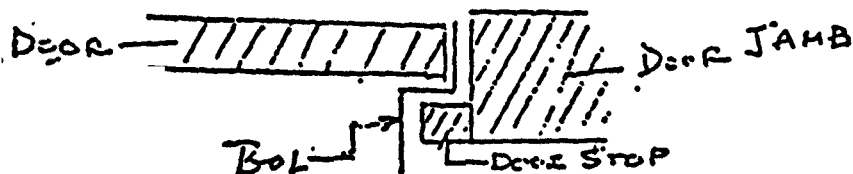
then the lock will have to be picked.

If you have a curved or slanted latch (this is the most common type of door latch) and there is no door stop (that strip of wood that

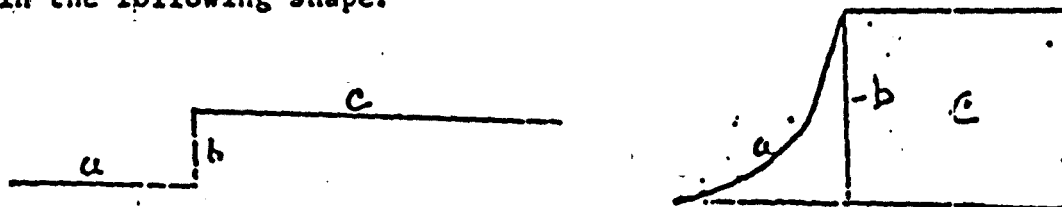


the door closes against) then it is a straight in shot with a credit card type tool (a piece of straight sheet metal is best). You just slide the tool in between the closed door and the jamb and slide it up under the latch - the door should open. In doing this it is usually best to pull the door towards you as it relieves pressure on the latch and makes the card easier to slide up. (SEE PAGE 3a)

If there is a door stop (as happens most frequently) then you can't just stick a credit card straight in - it has to bend around two corners:



The best thing is to manufacture a permanent tool rather than trying to bend up cards. You should obtain a thin sheet of metal and cut it out in the following shape:



The curved shape assists in raising the latch better than a straight-edge would do. The "b" section should be about as long as the average door stop (about 3/4", but measure it for yourself). The "c" section should be as long as will comfortably fit into your hand. The "a" section should be about 2-1/2" long, but only a portion of it will actually be working on the latch. Note that the slope of the "a" section drops off sharply at the beginning.

This tool is then inserted at the bottom of the doorway, slid up the doorway between the jamb and the door - thus opening the latch. If you have trouble inserting the tool, use your foot and push in the lower corner of the door as far as it will go. This should give you

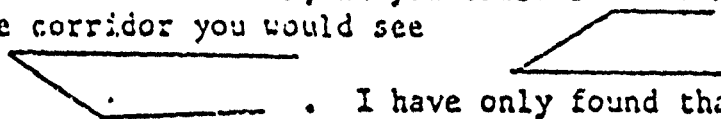
sufficient room to insert the tool. (See Page 4a, 4b)

It should be noted that you will need two tools - one for right hand doors and one for left hand doors.

As with the straight in shot it is usually best to pull the door towards you to relieve some of the pressure on the latch.

Often you will have to move the tool back and forth several times (or more correctly - up and down) to catch the latch correctly, while moving the door back and forth. Its a "feel" thing that you need experience on.

Now, very occasionally you find a latch that slants back into the room rather than out - that is, if you could look down on the latch from the corridor you would see

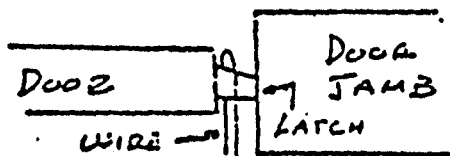


the normal I have only found that this occurs on doors without stops.

In this case, the tool, or credit card, won't work because the slant of the tool or the credit card is going in the wrong direction. You have to get something behind the latch to pull towards you.

Therefore, you should also carry about a 5 inch strand of flexible wire. The wire should be woven strands rather than one thick strand. The best I've found is the type of wire used to hang pictures that you can pick up at most hardware or drug stores.

Take this strand of wire (assuming there is no stop on the door jamb) and bend it in a semicircle. Slip the wire under the latch and maneuver the top of the wire out above the latch. Grasp both ends of the wire firmly and work it back and forth, pulling both ends towards you - and thereby working the latch out of the door jamb:



You have to be careful not to go too fast on this or you'll slip the latch out of the door jamb and have it slip right back in after the wire clears it.

These methods of opening locked doors have worked about 75% of the time. There are occasions where they won't work due to doors too tight, unoiled latches, etc.

There are also many odd configurations of latches and it helps to know exactly what the latch looks like. You can often find an unlocked door in the area, examine it (the latch), and try your tool out first on that door to get the feel for slipping that particular type of latch.

You'll also very occasionally run into doors with two locks on it. This can be slipped. In this case you need two tools. Insert one of the tools from the top of the door, slip the latch and hold it. Then insert the second tool from the bottom of the

WALL

Door



Push here with your foot to get extra room to insert the tool.

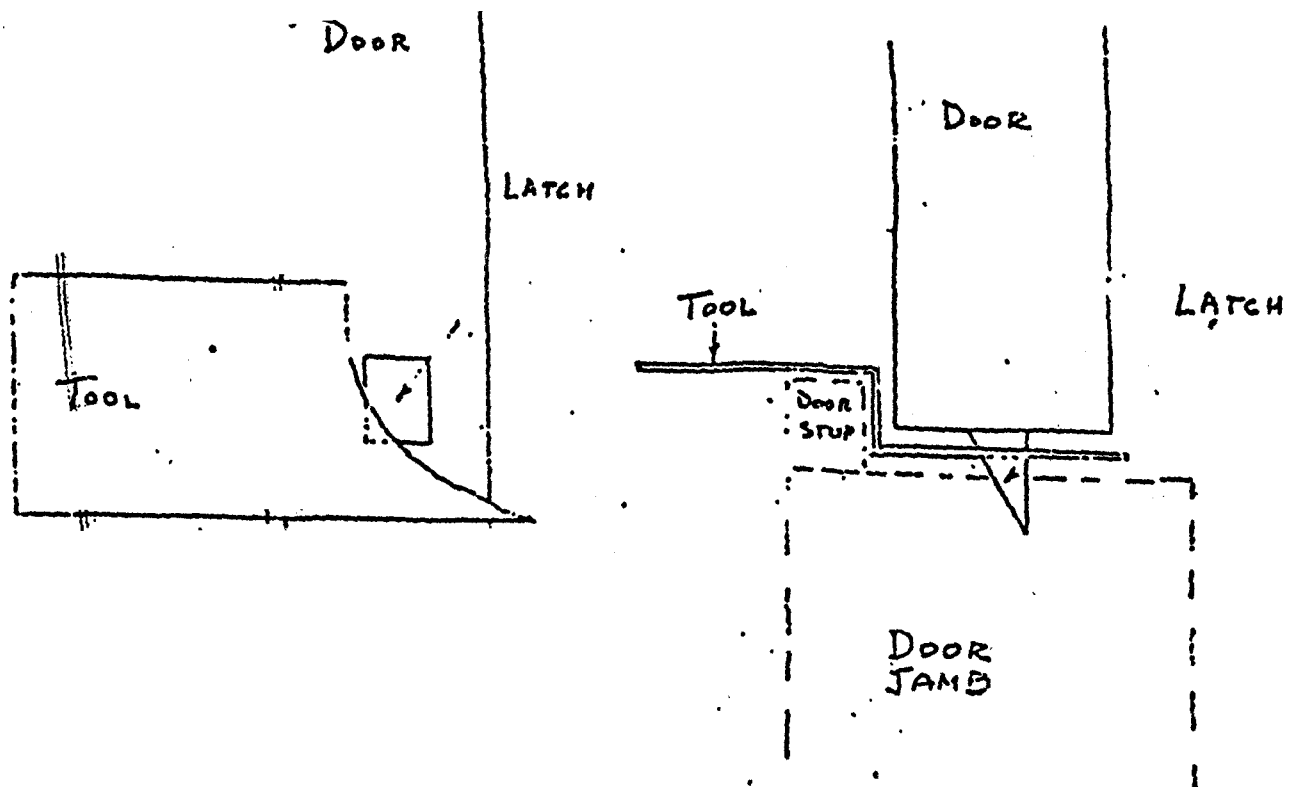
WALL

Once the tool is in position then slide it up the side of the door/door jamb to the latch.

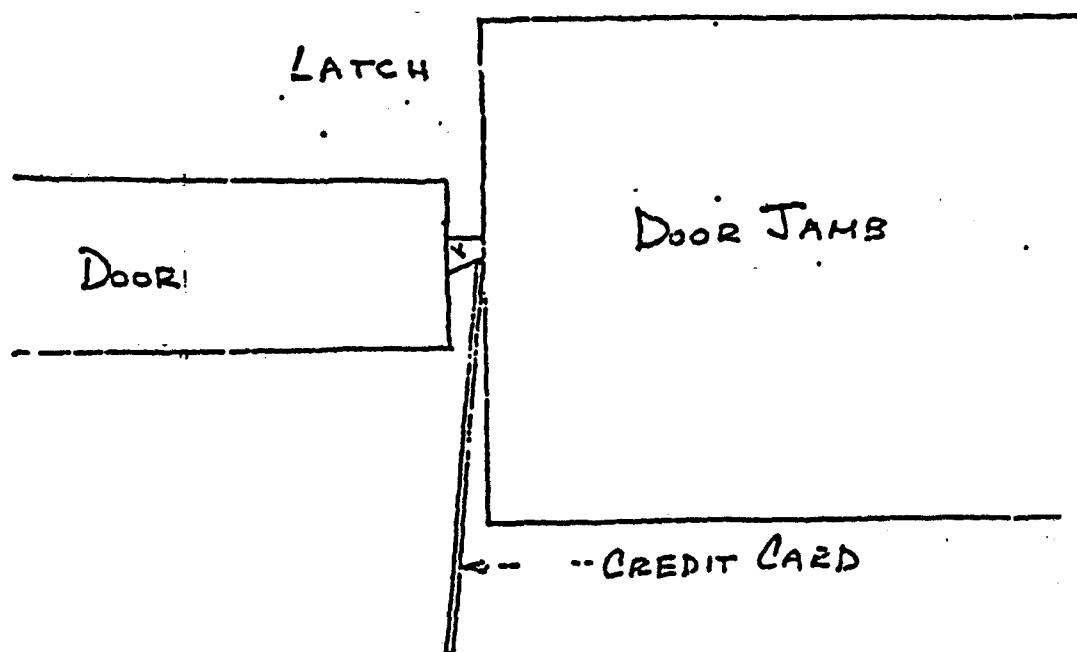
USE this extra space to maneuver the tool between the door, the stop and the door jamb.

480-1

PAGE 46



Front and top view of how the slanted tool works on the latch. As the tool is moved upwards, it forces the latch out of the door jamb.



The credit card is simply inserted in the space between the door and the door jamb and used to slide the latch out of the door jamb, working on the slanted part of the latch.

Well, slip the second latch and the door should open.

If a door won't open at all with this method, there is a very good chance (especially in government buildings) that there is a suite of interconnecting rooms adjacent to the room you are interested in. In this case, just try an adjacent door and go through the same routine again. If you have a number of different doors that could lead you to the same room, check the amount of "play" or looseness in each door and try the one that is loosest first.

Also, an old successful action if you know you are dealing with a suite of rooms, is to go into the rooms during the day and unlock one of the locked doors. It is likely that a door found locked during the day remains locked all the time and that other doors in the suite are used as the entrances/exits. The "locked" door is likely to not be checked each day on the assumption that it will stay locked. The best doors to choose for this are ones that tables, chairs, etc., have been pushed up against, as these doors are obviously not used as entrances/exits.

Of course, when you go into the suite of rooms during the day you should have a well worked out suitable guise that will logically explain your being there, or you won't get close enough to the door to unlock it unobtrusively.

One such suitable guise that was used involved going into the offices during the day with a clipboard and informing the secretaries that "Facilities Management" needed to check the locks on all doors. We had one door stay unlocked for three months using this technique.

By this time you should be in the office. If you're not, you either need more practice or you'll have to pick the lock.

The advantage, by the way, of slipping a latch as opposed to picking a lock is 1) to slip a latch takes 2-10 seconds compared with at least several minutes to pick it (unless you're very good), and 2) you don't need as much training and experience.

6) Once inside the office you have to locate the file you are interested in.

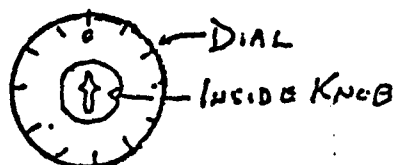
Most often the file will be located in a file cabinet and probably 50% of the time the cabinet will be locked.

As soon as you run into a locked file cabinet, immediately check the top middle drawer of every desk in the area of the cabinet and you'll almost surely find the key. If you can't find the key there, you'll have to search more thoroughly in different desk drawers. These keys have also shown up in file card boxes, taped to the cabinet, and locked in safes. But, I have never found a locked file cabinet and not been able to find the key in the room.

Combination safes occur infrequently. Like file cabinets, the combination is almost always laying around somewhere in the room.

again, check the top middle desk drawers of any desks in the vicinity of the safe, looking mainly for an index card sized piece of paper with the combination on it. (For some reason, all combinations I have found have been on this type of paper.) If you find nothing then check any alphabetical file card boxes. I have found the combination listed under "safe", "file", and "lock", but oddly, never under "combination". If you don't find it there you'll have to do a thorough search of other drawers and desk areas. There has been only one occasion where we weren't able to locate a safe combination - they are pretty easy to find.

Also, make sure that you know how to dial a safe combination. The most normal are 4 turns left (this is actually three times past the number and the 4th turn stops at the number), 3 turns right, 2 turns left, and one turn right to zero. You then turn the inside knob of the dial all the way to the right while holding the dial at zero:



When this is done then turn the dial as far right as it will go and the safe will open. On safes with no inside dial, just don't stop at zero. Go all the way to the right on the last turn and the safe will open.

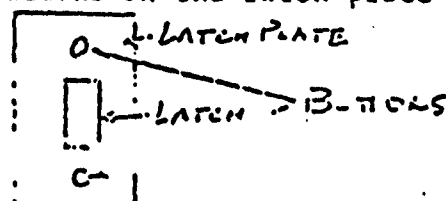
When you're finished with the safe make sure to set the dial back where it was before you opened it.

By going through the file cabinets, safes, desk drawers and desk tops you should now locate the file you are looking for.

One point to keep in mind while searching for the file is to keep the area (and the file when you find it) free of fingerprints. Optimally you should wear gloves. If this is not possible and you have to touch something, do so with the sides of your fingers or make sure that you smudge the prints. Prints can be easily smudged by giving your fingers a half turn as you withdraw them from the surface.

When you locate the file(s) put them in your briefcase.

On your way out of the room, if the door was locked when you went in, make sure that the door is now unlocked as you'll want to get quickly back in when you return. There are normally buttons on the latch plate of the door that push in and out:



... in whichever button is out and check the outside doorknob to see if it is unlocked, and then leave, closing the door behind you.

One other point when going into the room - often you will be working at night and you'll need a source of light. It is inadvisable to turn on lights unless you are thoroughly familiar with the area. You have no way of knowing who can see them especially if the office has an outside window. Instead, you should carry some type of small penlight flashlight. The batteries in these usually wear out after 30 minutes or so, so make sure you have sufficient batteries with you.

7) Return to the xerox room you originally picked out (or, if absolutely necessary, go to an outside xerox machine.).

It is best, if possible, to lock yourself into the xerox room so that noone can easily walk in on you unexpectedly.

One person should xerox while the other person puts the material back in the file, therefore, start xeroxing from the last sheet in the file folder.

You have to keep the files and papers clean of prints, so, if at all possible, wear gloves. If this can't be done then make sure you handle all pages with the sides of your fingers and your palms. This is easy to do after you get used to it.

Usually there is a title written or typed on the file folder. This should be xeroxed also so that you can keep the files separated.

If this is an "active" area - i.e. there is some type of current case going on and new material will be added to the file, it is wise to put a small pencil mark (inconspicuously) on the latest page in the file that you copy so you'll know where to start next time. Also, if there are a large number of separate files, you should mark them also inconspicuously so that you will know they have been done should you or someone else have to come back again.

Although I have never found it a problem, you should know that there is an internal counter in virtually all copying machines that will record the number of copies you make.

Also, once I ran across an agency which issued counting device to their employees as an economy measure to cut down on the use of the xerox machine. These devices are rectangular in shape - metal cases about 4"x2"x3/4" - that have a counting mechanism showing through the front "window" of the case. Without having one of these devices you can't operate the xerox machine. To operate the machine you place one of these devices into a rectangular hole on the control panel of the machine and when so placed, the machine will operate (after it is turned on of course).

If you run across this situation you'll have to search the desk tops and drawers in the vicinity of the machine to find one of these devices. This should be done before you search for the file(s).

When you finish xeroxing make sure there are no copies of yours in the machine, and turn it off.

W-1ns....,page 7.

Leave the room the way that you found it.

8) Return to the room you got the files from and replace them in exactly the place you got them from.

One thing that is good for the nerves is to be assured that no one has gone into the room (or may still be in there) while you were xeroxing. An easy way to handle this is to take a quite small piece of paper and stick it between the door jamb and the door when you are leaving to do your xeroxing. Leave a small end of the paper sticking out so you can barely see it from the corridor. Then, when you return and you see the paper in the same place you can enter the room with confidence.

If the paper should be disturbed when you return (this has not happened to me) you'll have to decide, based on the situation, whether to wait around and return the file, whether to return the file in some other fashion (e.g. "route" them back using the agency's comm lines, leave them in another office, etc.), or just take the files out with you.

After you have returned the files, look around the room and make sure that nothing else was disturbed.

Also, don't forget to relock a file cabinet if it was locked to begin with and make sure all keys are returned unfingerprinted to where you got them.

When you leave the room make sure the door is now locked (if it was locked to begin with) and smudge any prints that may be on the doorknob.

You should have your copies of the documents wither in an upper flap of your briefcase or in the main part of the briefcase turned face down with a book or legal pad on top. This is in case the guard checks your briefcase on the way out. All he will see are papers and won't be able to read any of them.

9) Miscellaneous:

a) I have nearly always found it better to approach guards and cleaners rather than shy away from them. This would be more in line with the beingness you have assumed.

I always try to establish some ARC with these people so they are comfortable with me in the area and assume that I belong there.

Cleaners usually come in after all the day time employees have left the area and therefore are not familiar with the day time employees.

Establishing ARC with these people has been so successful that they are often to open locked doors "because you forgot your key".

There is, of course, the liability that these persons can identify "me" as the person who was for such and such the liability.

There are exceptions to this. For instance you may do a walk-in looking for a specific piece of scandal material, but generally the above order of priority should be followed. You don't want to get on #3 before #1 is fully completed, no matter how interesting #3 may be, because your access can be cut at any time.

d) When you are dealing with an extremely large agency or group it is beneficial to mix an FSM with a walk-in.

The FSM will be limited pretty much to a specific area of the agency yet there may be many other areas of the agency that may have files on us. Having the FSM go out of her immediate area alone and walking around in other divisions or sections could be as bad as sending one person in to do a walk-in. There are exceptions to this, of course, where an FSM is extremely familiar with the whole building.

Just follow the normal routine of a walk-in when doing this, and steer clear of the FSM's actual area of employment.

e) Electronics can be a concern when doing a walk-in. There is a possibility that a door can be alarmed or that there are TV cameras that are monitored at a guard station, etc.

I have only run across this in "national Security" type areas which are usually not amenable to a walk-in anyway and require FSMs.

If you have any doubt about an area possibly being alarmed or monitored in some way you should check it out first.

You'll need to go into the area during work hours on some pretext, and get a good look at the inside of the room. You are looking for wires and switches around the inside door frame. Also look in the corridor for a panel that looks like a light switch cover that has a slot for a key, and two lights - usually a red and a green. This turns on and off an alarm system via a key. A green light usually means that the alarm is off and a red light means that it is on.

There are other devices such as pressure sensitive devices under a rug, or motion detectors, but I have little familiarity with them and have never run into them.

You also want to check the upper corners of the room (near the ceiling) for cameras, and also check the corridors for the same. Then, go to the guard station and see if there are any TV sets for monitoring the rooms and corridors.

If the above is done you can be reasonably certain that the area is "clean" or not.