

Researcher's Guide to Safety, Security and Media Relations at **UC Davis**



UC Davis Police Department
Calvin E. Handy, Chief of Police

SPRING 2002

This publication was designed for members of the University of California, Davis, research community. The information contained in this publication may not be applicable to any other community. Neither the Regents of the University of California, nor the UC Davis Police Department, assume responsibility for the use of this publication outside its intended audience. This publication may be disassembled and used as a master for printing more copies. Permission is granted for reproduction with no additions, deletions or alterations to original text or work.

UC Davis Police Department
One Shields Ave
Davis, CA 95616-8681

The logo of the UC Davis Police Department is a five-pointed star with a decorative border. The words "UC DAVIS" are written across the top points, and "POLICE" is written across the bottom points.

TABLE OF CONTENTS

INTRODUCTION	1
HISTORICAL PERSPECTIVE	2
RISK ASSESSMENTS	4
Procedural Security	5
Personal Safety	6
Facility and Agricultural Security	8
Residential and Hotel Security	10
Computer Security	11
Suspicious Packages and Letters	12
Bomb and Other Threats	14
Arson and Vandalism	15
Civil Disobedience and Protestors	16
MEDIA RELATIONS	18
RELEASE OF PUBLIC INFORMATION	20
CRISIS MANAGEMENT RESOURCES	21
POLICIES AND PROCEDURES	22
ACKNOWLEDGMENTS	23

INTRODUCTION

It is imperative that a safe and secure environment exist in which the University of California, Davis - a leader in research and education - can sustain its fundamental mission of teaching, research, and public service.

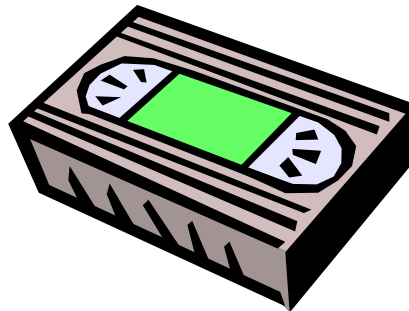
As a member of the university community, you can become the target of those who disagree with the nature of your research. They may believe that what you do is unethical, immoral and wrong, and they might use any number of methods to try and stop you from conducting your research.

Extremists have accelerated their efforts in opposition to the use of animals in biomedical research, as well as research into the genetic modification of crops and animals. Criminal activity against persons and property associated with this kind of research is expected to continue for some time to come.

The key to safeguarding yourself and your research is to **BE PREPARED.**

This publication is designed to assist you in preventing, managing, and minimizing the impact of incidents such as theft, vandalism, protests, and threats of personal harm. It also addresses your relationship with the news media and how you can best handle reporters' requests for information about your research.

This publication is intended to complement the video presentation that documents, but not in as much detail, ways you can safeguard yourself and your research from attack. The videotape is available from your academic department.



Remember - You can't always avoid becoming the victim of crime, but there are steps that you and your academic department can take to reduce the risk and discourage criminal and extremist activity.

HISTORICAL PERSPECTIVE

The history of animal/environmental extremist groups can be traced to England, with all groups now falling under the broad category of “eco-terrorism” - defined as any crime committed in the name of saving nature.

In 1973, in England, an animal rights extremist was arrested and convicted of arson. While in custody, he developed the technique of “hit and run” attacks with media publicity, and having small groups of individuals, to maintain secrecy and prevent law enforcement infiltration during the commission of their crimes. Shortly after his release from prison, he formed the *Animal Liberation Front* (ALF). The ALF, like its environmental counterpart *Earth Liberation Front* (ELF), has basic guidelines for “actions” (“actions” are criminal activity). If individuals or groups of individuals follow these guidelines, they are considered part of the ALF or the ELF. The guidelines are, basically, not to commit violent acts against any animal, human or non-human. Arson, vandalism, theft and burglary are not considered crimes or violent acts by people who identify with the movement. ALF and ELF actions have since spread to the United States.

The *Justice Department* is another animal extremist group that separates itself from the traditional eco-terrorist groups in that its members support violence - "We need to ask ourselves what works and go from there... let's not start from a position that violence is wrong, or law breaking is wrong." The *Justice Department* also has its roots in England, and has since migrated to North America. In 1996 it claimed credit for sending razorblade letters to hunting guides in Canada.

In 1998, individuals began to organize against genetic modification of crops when *Operation Cremate Monsanto* burned cotton fields in India. Anti-genetic engineering actions quickly spread to the United States and continue to be a concern.

UC Davis has long been a target for animal extremist groups and recently has also been a focal point for groups in opposition to genetically modified agriculture. According to an animal rights activist, "the first ever U.S. animal rights civil disobedience occurred there (UC Davis) in 1984, and, in 1987, the first ever fire set by activists destroyed an unfinished animal research laboratory (Thurman Lab)." That fire caused more than \$4 million in damage. Arson is described by the *Animal Liberation Front* as "by far the most potent weapon of direct action."

In April 1997, the 10th anniversary of the Thurman Lab arson fire was commemorated with a protest in front of the California Regional Primate Research Center. Thirty-two people were arrested, including leaders of various animal extremist groups from Oregon, Utah, Texas and California. A month before this protest, a small arson fire was discovered at the UC Davis Center for Comparative Medicine construction site on the grounds of the Primate Center.

In November 1997, a group calling itself the *Ape Army* demonstrated in front of the Primate Center as part of a nationwide protest tour of NIH-funded primate centers across the United States. This was followed in 1999 by the Primate Freedom Tour, which stopped at the UC Davis Primate Center for three days of demonstrations. There

were also demonstrations in front of the UC Davis Chancellor's Residence, as well as a UC Davis animal researcher's residence in the city of Davis.

In 1998, the ELF claimed responsibility for a \$12 million structure fire in Vail, Colorado. According to ELF, the fire was set to protect the lynx habitat. Meanwhile, a group calling itself the *Biotic Baking Brigade* claimed responsibility for throwing pies at the chancellor of UC Davis and the dean of UC Berkeley's College of Natural Resources for, respectively, a possible alliance with Monsanto and a confirmed agreement with the Swiss biotechnology company, Novartis.

In 1999, UC Davis and UC Berkeley began to experience vandalism to agricultural fields by groups opposed to the genetic modification of crops. A group calling itself *Reclaim the Seeds* damaged UC Davis crops of sugar beets, corn, watermelons and walnut trees. On New Years' Eve, 1999, there was an arson fire at Michigan State University due to the perceived collaboration between an MSU researcher and Monsanto Corporation.

Also in 1999, 10 UC Davis animal researchers were targeted in a nationwide terrorist action claimed by the *Justice Department*. Each was to receive a letter containing a razorblade and a threat to stop animal research by Autumn of 2000. Seven UC Davis researchers received the letters. All of the letters were recovered by the police unopened, and there were no injuries.

In the last action prior to the Spring 2002 publication of this booklet, *Reclaim the Seeds* claimed responsibility for August 2000 damage to a UC Davis cornfield.

RISK ASSESSMENTS



Procedural Security
Personal Safety
Facility and Agricultural Security
Residential and Hotel Security
Computer Security
Suspicious Packages and Letters
Bomb and Other Threats
Arson and Vandalism
Civil Disobedience and Protestors

Procedural Security

In addition to the security steps that you can personally take to safeguard University and your personal property, it is important that you encourage your academic department to take precautions, as well. Examples include ensuring that there is adequate interior and exterior lighting; installing lock-down devices for all theft-prone equipment such as computers; erecting perimeter fencing; and installing alarm systems in labs, greenhouses, offices, and other facilities, especially where sensitive research is taking place.

One of the first steps any academic department can take to reduce the chances of becoming a victim of crime is to hire wisely and encourage the highest standards of professionalism. Department heads should understand that they are taking unnecessary risks when there is no **BACKGROUND INVESTIGATION** and/or reference checks made of a job applicant. No academic or other department should feel compelled to employ an applicant in a sensitive job (especially in a plant/animal research facility) after that individual has demonstrated that he or she may not be worthy of trust or has indicated that they vehemently disagree with the nature of your research.

Other ways to encourage your department to maintain a safe and secure work environment include:

- Visitor monitoring – Screen and check in every visitor to your facility. This includes new vendors. Consider issuing dated visitor passes.
- Employee identification - Consider issuing photo ID badges for all employees. Adopt and enforce a policy requiring photo ID badges to be worn.
- Key control - Keep accurate files documenting who has been issued keys (including electronic access cards and codes). Conduct an annual audit to determine if someone has a key that he/she doesn't need. When individuals are no longer employed, make sure you have a procedure in place to retrieve any keys they have been issued. If there are a number of keys unaccounted for, consider re-keying.
- Computer Security - Require employees to use passwords, which should be kept confidential and changed often.
- File-cabinet security. Replace original manufacturer locks. Keep cabinets secure at all times.
- Trash control – Adopt and maintain a shredding policy for sensitive documents and computer disks. Remove all data from the hard drive before disposing of computers.

Last, but not least, you should encourage other department members to **DISCUSS SAFETY AND SECURITY ISSUES** unique to your facility, and consider additional safety precautions.

Partner with the Police Department – The police can survey your facility (or residence) and make safety and security recommendations.

Personal Safety

Ordinary criminals, extremist individuals and groups will generally attack facilities before resorting to committing crimes against people. But frustrated extremists will, on occasion, threaten and attempt to intimidate individuals within the research community by more direct means – e.g., following you home, placing nails under a tire, throwing a pie into your face, razor blades in a letter...

... Personal safety is all about taking a few simple precautions and not taking unnecessary risks.

Some ways that you can protect yourself are:

- Be alert to your surroundings and the people around you - especially if you are alone or it is dark. Be vigilant.
- Whenever possible, travel with a friend or co-worker.
- Park your car, walk, and stay in well-lit, high-traffic areas as much as possible.
- Walk confidently and at a steady pace, making eye contact with people when walking.
- Do not respond to conversation from strangers on the street - just continue walking. Avoid people who look out of place, even if it means traveling, temporarily, in a different direction.
- Have your car keys in your hand so you don't have to linger before entering your car.
- Prior to unlocking the car door, briefly inspect your vehicle, especially looking for items that may have been placed under the tires, or persons who may be hiding inside the passenger compartment.
- If your car breaks down, open the hood and turn on your flashers. If someone stops to help, stay in your locked car and ask him/her to call a law enforcement agency or a tow truck.
- Don't stop to aid motorists stopped on the road. Go to a phone and request help for them.
- If you work alone or before/after normal business hours, keep the office door locked.
- If someone comes to your home or office stating that he/she is a police officer, utility company worker, etc., ask to see identification. If you are unsure, call the agency that they represent and verify their identity.
- Never open your office or residential door without knowing who is on the other side.
- Be aware of escape routes for emergencies and post the Police and Fire Department numbers near telephones.
- Especially in rural or isolated settings, carry a cellular phone (or other portable communication device). In the event that you need to contact Police/Fire/Medical in an emergency situation, do not rely on a prompt response when you dial "911" - Instead, program the local emergency services non-emergency number(s) into your phones memory.

⇒ **Immediately report all suspicious persons, vehicles, and activity to your local Police Department.**



A suspicious person or vehicle loitering in an area for no apparent reason could be waiting for the right moment to commit crimes against you or your research. Obtain license numbers and a description of the vehicles or people, if you can.

You are in the best position to know what looks right or wrong where you work and around your home.

Facility and Agricultural Security

Thieves, vandals or extremist individuals or groups tend to avoid areas where they feel there is a good possibility that they will either be seen and reported to the Police, or that they will be unsuccessful in their criminal act.

If you strengthen the security of your research facility or agricultural station, extremists may tend to attack another, more easily defeated target, or they may simply forget the whole thing all together.

Here are a few tips on how you can deter criminal activity:

- Post signs at lab entrance(s), facilities, and field perimeters indicating “Restricted Area – Authorized Personnel Only” or “No Trespassing – Authorized Personnel Only.”
- Install an electronic intruder alarm system in labs, greenhouses, offices, and other facilities.
- Install lock-down devices for all electronic / computer equipment. Do not leave cash, sensitive materials/data, or other valuables unattended.
- Engrave theft-prone equipment with department ID. Record serial number, make, model and description of equipment.
- Provide photo ID badges to all staff and make it mandatory that they’re worn.
- Maintain strict key control. Consider re-keying if there are too many outstanding keys. Do not give/lend your University key(s) to anyone. Consider installing an electronic access control system for doors.
- Keep offices, labs, and vehicles locked when unoccupied or unattended for any amount of time. Make sure windows are secured, as well. Remove all valuable possessions from vehicles, or lock them in the trunk.
- Install metal latch guards to cover the latch and strike plate on all interior / exterior doors.
- Remove any exterior signage indicating the type of research being conducted. Do not place sensitive or personal information on a Web site.
- Eliminate exterior glass partitioned doors. Install solid metal/wood doors.
- Frequently inspect facility for potential or actual security hazards or breaches.
- Install / close the window shades/blinds whenever the facility/room is unoccupied, and at night, whether occupied or not.
- Keep trees and shrubs trimmed low and away from doors, windows and address numbers. This precaution will give you, other employees and patrolling police a view of potential problems and deny an intruder a place to hide.
- Around high-risk agricultural plots, erect quality perimeter fencing with posts set in concrete. Lock gates when unoccupied. Consider installation of an electronic perimeter / fence security system to detect intruders. Maintain strict key / code control.
- Around non-fenced areas, dig a perimeter ditch, erect high mounds, or bury posts to prevent vehicles from entering area except at gated entrances.



- Secure large equipment and vehicles in a locked/enclosed structure. Chain equipment together or to fixed objects. Utilize locking gas caps. Remove ignition keys.
 - Mark livestock/animals for identification via branding, tattooing, ear notches, and/or tagging.
 - Check and maintain adequate exterior lighting around out buildings and animal feed storage areas. Install perimeter fencing around grain or hay storage facilities.
 - Use confetti marked with an ID number to mark grain or hay.
 - Keep out-buildings/sheds locked when unoccupied or unattended for any amount of time. Make sure windows are secured, as well.
 - Consider making contact with people you don't know who appear to be loitering near your office, lab, or other facility. Ask them if you can assist them and try to ascertain what their business is.
 - In rural / isolated areas, have in your possession a cellular phone (or other portable communication device). In the event that you need to contact Police/Fire/Medical in an emergency situation, do not rely on a prompt response when you dial "911". Instead, program the local emergency services' non-emergency number(s) into your phone's memory.
- ⇒ **Immediately report suspicious people, vehicles, and activity to your local Police Department.**

Residential and Hotel Security

Here are few tips on how you can strengthen the security of your personal residence or hotel room when you travel:



- Maintain strict key control. Do not give/lend your house or hotel key to anyone. When you have your personal car serviced or valet parked, take your house key and garage door opener with you.
- Engrave theft-prone personal equipment with your California driver's license number. Record serial number, make, model and description of equipment.
- Install deadbolt locks and use solid core doors for all exterior entrances. Your front door should have a peephole.
- Pick a well-known and reputable hotel with interior corridors. Request a room between the second and seventh floors, near, but not next to, the elevator (1st floor rooms are more susceptible to burglary. Many Fire Department ladders won't reach the 8th floor.)
- Keep your residence/hotel (doors and windows) locked whether unoccupied or not. This is especially important if you are alone.
- Install an electronic intruder alarm system with contact switches at each window and entry door.
- Have address numbers large enough to be visible from the street and well lit.
- Check and maintain adequate exterior lighting. Consider motion-sensitive lighting.
- Place holds on your newspaper and mail when you're away from your residence for more than a day or two. Have someone take care of your yard while you're away.
- Utilize timers for interior lighting to give your home a "lived-in" look even while you are away.
- Keep trees and shrubs trimmed low and away from doors, windows and address numbers. This precaution will give you, your neighbors and police a view of potential problems and deny an intruder a place to hide.
- Secure valuables and sensitive research data in a home or hotel safe.
- Carry a cellular phone (or other portable communication device). In the event that the phone lines don't work, and you need to contact Police/Fire/Medical in an emergency situation, do not rely on a prompt response when you dial "911". Instead, program the local emergency services non-emergency number(s) into your phone's memory.



⇒ **Immediately report suspicious people, vehicles, and activity to your local Police Department.**

Computer Security



Cyber-terrorism may be defined as the unlawful use of computing resources to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives.

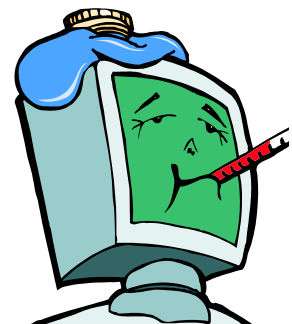
Cyber-terrorists may include those persons who remotely enter a computer network or individual computer without the permission, authorization, and sometimes, knowledge of the network or computer's owner (aka "hacking").

Cyber-terrorists may send, via electronic means (e.g., electronic mail), malicious "viruses" that are intentionally designed to damage or corrupt the data or files stored on your computer's hard drive or diskettes.

Therefore:

- Do not allow unauthorized persons to access your computer, especially files in which research or sensitive data is stored.
- Back up research or sensitive data every day. Minimally, secure all back-up tapes or disks in a locked, fireproof safe.
- Use virus protection software on all of the computers you access, whether at your residence or place of employment. Upgrade the virus protection software frequently.
- Be careful and cognizant of the source when you download files from the Internet. If you're unsure about the safety of the source site do not download any files.
- Do not open electronic mail (e-mail) attachments from (suspicious) persons or addresses that you do not know, or when you are not expecting the attachment(s). Delete the message(s) and attachment(s) immediately.
- Separate computers that contain research data from those computers you use to access the Internet or personal/professional e-mail.
- Frequently communicate with your employer's network administrator about computer security issues, including the isolation/protection of your personal or department Web site.

⇒ **Immediately notify your local Police Department** if you suspect your computer/network system has either been accessed without your permission ("hacked"), or you receive a targeted e-mail message containing a suspected virus from a person/source you believe to be a cyber-terrorist.



Suspicious Packages and Letters

Packages, envelopes and letters (hereafter referred to as “parcels”) delivered or intentionally left “abandoned” at your place of employment, or your residence, have the potential to contain such items as explosive devices, razor blades, poisons and other harmful material. These items may be enclosed in any number of ways, including hollow books, lunch boxes, briefcases and other containers. Their outward appearance is limited only by the imagination of the sender.

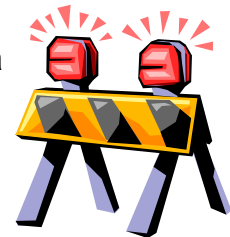
Though the likelihood of ever receiving this type of correspondence is remote, a small number of these devices have been discovered over the years, resulting in death, injury and the destruction of property.

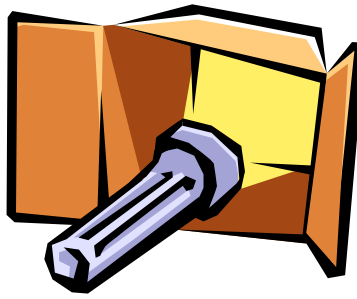
GENERAL PRECAUTIONS:

- Examine every parcel prior to opening it.
- Maintain secure mail procedures to control and restrict the possibility of someone tampering with incoming or outgoing parcels, or introducing a parcel that was not legitimately sent or received.
- Attempt to verify with the sender the contents of any suspicious parcel prior to opening it.
- Do not open any parcel by hand – always use a letter opener or similar device.

Here are some **WARNING SIGNS** that may assist you in identifying a suspicious parcel:

- Parcel that bears such wording as “Personal” or “Private”, or “Fragile – Handle With Care” or “Rush – Do Not Delay.”
- The sender’s and/or the addressee’s name, address, and/or job title is inaccurate, misspelled, fraudulent or missing.
- The sender is unknown to the addressee or the addressee is not expecting this particular parcel.
- The postal cancellation or postmark shows a different location than that of the return address.
- Parcel that reflects distorted handwriting or the name and address is prepared with homemade labels or cut-and-paste lettering.
- Parcel that has protruding wires, aluminum foil or oil stains visible.
- Parcel that emits a peculiar odor, or leaks an unknown liquid or substance.
- Parcel that has an excessive amount of postage affixed.
- Parcel, especially a letter, that feels rigid or appears uneven or lopsided.
- Package or article that is unprofessionally or sloppily wrapped.
- Package or article that has an irregular shape, soft spots or bulges.
- Package or article that makes a buzzing/ticking noise or sloshing sound.
- Pressure or resistance when removing contents from the package or article.





Now, you've examined the outside of the parcel, and you've seen some clues that suggest to you that the contents may be suspicious –

WHAT DO YOU DO?

- ⇒ Do not move, alter, open, examine, or disturb any found or abandoned parcel.
- ⇒ Do not place a suspicious parcel in water or a confined space like a trash can or file cabinet.
- ⇒ Place the suspicious parcel in an isolated area, like an empty office or conference room.
- ⇒ If possible, open windows in the immediate area to assist in venting potentially explosive or harmful gases.
- ⇒ **Consider evacuating the immediate area.**
- ⇒ **Immediately contact your local Police Department.**



ANTHRAX

If you receive a letter or package that allegedly contains “anthrax” or other poison, follow these steps:

Do not panic! Remain at your workstation. Do not move around.

Call the Police.

Evacuate the immediate area. Do not allow co-workers to touch the letter or mingle at your workstation.

If possible, place the letter or package, and its contents into a larger envelope. Do not seal the larger envelope.

Await the arrival of the Police. Follow their instructions.

Bomb and Other Threats

Every bomb or other immediate threat of a suspected explosive device should be considered as valid until all reasonable precautions for public safety have been taken, or until the danger to life and property has passed. Bomb and other threats may be received in any number of ways including, but not limited to, telephone, electronic mail or written correspondence. Any unusual or suspicious object should be reported immediately to your local Police Department. Suspected objects or materials should NOT be touched or disturbed.

WHAT TO DO:

- ⇒ When a bomb or other immediate threat is received via telephone at your place of employment or your residence, the person taking the message should keep the caller talking as long as possible and make written notes of the following:
 - ✓ The time and date of the call.
 - ✓ The assumed age and sex of the caller.
 - ✓ Any distinguishing speech characteristics.
 - ✓ What was said by the caller, as precisely and completely as possible.
 - ✓ Any background noise that may help identify the source of the call.
 - ✓ The phone number of the caller (if your phone is “Caller ID” equipped).

NOTE: A form, the “Bomb / Telephone Threat Checklist,” can be downloaded from the UC Davis Police Department Web site, and is available to assist you in obtaining information from, and about, the caller.

- ⇒ When a bomb or other threat is received via written correspondence (e.g., note or letter):
 - ✓ Do not continue to touch the letter or envelope.
 - ✓ Do not allow any other person to touch the letter or envelope.
 - ✓ Place the letter/envelope in a safe place where it cannot be touched or damaged.
- ⇒ When a bomb or other threat is received via electronic mail do not delete the message or modify it in any way.
- ⇒ **Immediately contact your local Police Department.**

* * * * *

After an evaluation/assessment of the content of the bomb or other threat, the decision to evacuate or close a facility shall be made jointly, whenever possible, by the Police Department and the department head and/or facility manager.

Arson and Vandalism



Many of the same precautions taken to discourage thieves and trespassers may also discourage arsonists and vandals.

Arson is most common in vacant/unsecured buildings and construction sites. Vandalism is most commonly committed in the evenings and on weekends.

In addition to those **Risk Assessments** identified under the **Facility / Residential Security** sections of this booklet, you should:

- Install smoke detectors/alarms, automatic and tamper-proof sprinklers, and other fire safety equipment.
- Clear your facility or residence of fuel sources such as yard trimmings, newspapers, leftover paint, old rags, and other trash.
- Secure flammable materials and substances in locked, fire-resistant cabinets or containers.
- Dispose of all flammable waste materials as quickly as possible (check with local authorities for approved methods of disposal).
- During the construction of new facilities, install perimeter fencing and employ security guards.

⇒ **Partner with the Fire and/or Environmental Health and Safety Departments** – they can survey your facility (or residence) and make fire safety and chemical storage recommendations.

⇒ **Immediately report suspicious people, vehicles, and activity to your local Police Department.** Obtain license numbers and description of the vehicles or people if you can.

Civil Disobedience and Protesters

Protestors and activists believe that government, and government entities (e.g., Universities), make, or have made, bad laws and/or policy decisions.

Protestors and activists believe that if legislation and political lobbying have failed, one other way to get a bad law or policy changed is for people to deliberately disobey the law in a public way - to engage in civil disobedience.

Not all acts of protest are unlawful. It is possible to peacefully demonstrate and exercise First Amendment rights through a lawful process. This usually means obtaining permission from the government.

Most groups do at least some planning prior to a lawful protest or the commission of an act of civil disobedience.

Any group that wishes to use civil disobedience or direct action / protest to achieve change must:

1. make absolutely clear what change is desired, usually by listing specific demands;
2. target a group or individual with the power to bring about the desired change;
3. design actions so that the cost of resisting change is perceived by the person/group in power to be greater than the cost of giving in.

This is done in one of two ways:

1. create problems for those in power that will not go away until they give in (for example, occupy their offices or zap their phone lines), and/or
2. educate the public in ways that both cause embarrassment to those in power and cause them to be fearful that the popular movement for change may grow strong enough to threaten their power (for example, interrupt news broadcasts or hang banners).



Because activists want to attract media attention, many, but not all, protests are planned and publicized well in advance. In either case, it is very important that you, others in your department, and your family have a response plan in place.

Partner with Facilities Services and your local Police.

At work, Facilities Services can respond to your location and assist in locking down stairwell and exterior facility doors, gates and elevators, so as to make it difficult for the protestors to invade your building or facility.

At work and home, your local Police Department can respond to your location to keep the peace and assist in protecting valuable research and personal assets.

Partner with your family and fellow employees to **conceive a plan** as to what you are going to do if protestors show up at your work or your personal residence. Suggestions include:

- Close and lock perimeter gates, and exterior and interior facility doors. Close window blinds.
- After locking down the facility or your residence, either evacuate or stay inside a locked (“safe”) room.
- If you arrive at your work or home and protestors are already present, go to an alternate location.
- **Do not** speak to, or argue with, the protestors. Avoid making eye or physical contact with the protestors.

⇒ Contact your local Police Department.

- Do not open any doors for anyone except the Police and employees of the University who have been sent to assist you.

MEDIA RELATIONS

Terrorist or other critical incidents, by their nature, draw news media interest. When the university has been the target of such activity, university spokespeople will be sought for news interviews. As a public university, UC Davis is obliged to provide information to help the general public understand the nature, value and purpose of the work conducted by its faculty, staff and students. In quiet times and in crisis, this informational effort will help to further understanding and to sustain public support.

While there are not conclusive data suggesting that those who are the targets of threats increase their risk by speaking publicly, it is understandable that those who have been so targeted would have concerns about increased exposure if they were to grant news media interviews. In such circumstances, the university's News Service will work to quickly identify appropriate administrators to serve as spokespersons to the public on behalf of the targeted individuals.

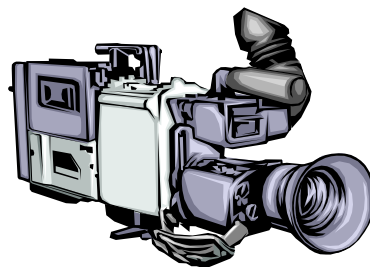
Efforts to inform and educate the general public about the campus's research and instructional programs should be sustained and year-round in nature, drawing upon the many faculty, staff and students engaged in those programs who wish the public to have a fuller understanding of their work.

WHAT TO DO:

- ⇒ Alert the News Service when you are anticipating media calls and do not want to be contacted.

You do have a right not to respond. The News Service will do its best to prevent such inquiries and to redirect interview requests. But be advised that the campus phone numbers of all university employees, including faculty and researchers, are public information available from campus directories, the campus operator and on the Web. When the News Service learns that media are planning to contact campus community members, it tries to provide advance notice. Unfortunately, it's not always known when media are planning to make such a direct contact.

- ⇒ If a reporter contacts you and you do not wish to grant an interview, you might respond, "I would prefer not to offer comment at this time. Please call the News Service at 530-752-1930 for assistance in reaching a campus spokesperson."



It is not necessary that you commit immediately to grant an interview. It is perfectly acceptable to obtain a reporter's name and publication or broadcast station, and to ask what type of information he or she is seeking and the deadline for response. Then, to allow yourself time to determine if you'll grant the interview (and, if so, how best to respond), tell the reporter you will call back in a short time (perhaps 20 minutes or an hour). In the interim, determine whether you are comfortable responding, and if you are the appropriate spokesperson. If you are uncertain or wish to redirect the inquiry, please contact the News Service for advice and consultation. The News Service can help identify an appropriate spokesperson from the administration, or from your school, division or department, to respond on your behalf.

- ➡ If you decide to grant the interview, give yourself time to gather your thoughts before responding.



The News Service can help you focus your comments and anticipate reporters' questions. The office routinely prepares background fact sheets that can aid your discussion.

If you are concerned about the publication of your photograph, the News Service will not publish or share your photo with news media without your permission. You may wish to review the images on your departmental Web pages to further protect your privacy.

It's not recommended that you grant an interview if a television reporter suggests blurring your image on the televised report to obscure your identity.

- ➡ **Advise the News Service when you have had media contact, and the outcome, so that its media relations professionals can best direct future inquiries.**

RELEASE OF PUBLIC INFORMATION

Just as in [media relations](#), efforts to inform and educate the general public about the campus' research and instructional programs should be sustained year-round. UC Davis supports the principle that access to information concerning the conduct of business in a public university is a right of every person. UC Davis further supports the principle of securing individuals', fundamental rights of privacy. It is the general policy of UC Davis to interpret the laws governing the access to various records liberally to the benefit of the individual (i.e., where discretion is allowed the protection of privacy should override the option to disclose).

Private parties and the media are allowed access to UC Davis records pursuant to the California Public Records Act (CPRA) (California Civil Code § 1798 et seq.). Some individuals will make requests for records under the Freedom of Information Act (FOIA); however, the University of California is not subject to FOIA, as it applies only to requests for records from federal agencies. FOIA requests are often made to such federal agencies as the National Institutes of Health (NIH) or the U.S. Department of Agriculture (USDA).

Any response to a request for records must be made within ten calendar days of the request's receipt.

WHAT TO DO:

⇒ All requests for University records should immediately be forwarded to the Information Practices Office for coordinated response.

Once the Information Practices Office has received the request, the coordinator will seek to gather the requested information and will consult with individuals about any concerns regarding the release of information. There are exemptions to providing some types of information under the California Public Records Act, and information regarding the privacy of individuals will be protected under the California Information Practices Act. The information practices coordinator, often with the assistance of campus counsel, will make certain that records are released in compliance with the law.

Questions regarding this section of the *Safety and Security* booklet may be referred to the Information Practices Coordinator, Office of Administration, 530-752-3949.

Whenever ANY doubt exists concerning the appropriateness of records disclosure, the Information Practices Coordinator should be consulted.

When NIH receives a request for copies of grant information involving a university researcher, its Freedom of Information and Privacy Act Office forwards a copy of the request to the principal investigator. The principal investigator can respond to the Freedom of Information Specialist at NIH by returning the letter with a signed approval for release of grant information. If, however, the principal investigator believes that portions of records should be withheld (e.g., exemptions include patentable information), then he or she should contact the campus Information Practices Office for assistance with the coordination of the response.

CRISIS MANAGEMENT RESOURCES

The following UC Davis public safety responders, departments and administrative units will partner with the research community to initiate practices designed to prevent, protect and respond appropriately to critical incidents, acts of crime, and requests for information:

POLICE DEPARTMENT

530-752-6859

Web site: police.ucdavis.edu

FIRE DEPARTMENT

530-752-1236

Web site: www-oes.ucdavis.edu/UCDFD/default.htm

ENVIRONMENTAL HEALTH AND SAFETY

530-752-1493

Web site: ehs.ucdavis.edu

NEWS SERVICE

530-752-1930

Web site: www.news.ucdavis.edu

OFFICE OF ADMINISTRATION

530-752-2081

Web site: vadmin.ucdavis.edu

FACILITIES SERVICES DEPARTMENT

530-752-1655

Web site: www-pplant.ucdavis.edu

EMERGENCY PREPAREDNESS PLANNER

530-752-5386

Web site: planit.ucdavis.edu

INFORMATION PRACTICES COORDINATOR

530-752-3949

Web site: vadmin.ucdavis.edu

RISK MANAGEMENT

530-752-6018

Web site: hr.ucdavis.edu/rmpl/

POLICIES AND PROCEDURES

The following UC Davis Policies and Procedures are available on the UC Davis web site (www.ucdavis.edu) to provide you comprehensive guidance reference many of the subjects briefly discussed in this [Safety and Security](#) booklet:

290-05	Campus Emergency Policy
290-08	Terrorist Acts Targeting Research
290-20	Fire Safety
310-40	Public Information and Media Relations
320-21	Privacy and Access to Information
320-23	Disclosure of Information from Public Records
350-85	Loss Of or Damage to University Property
360-35	Security Alarms
360-50	Key Control
370-30	Property Insurance
380-25	Disclosure of Information from Personnel Records

ACKNOWLEDGMENTS

The following individuals, and/or their staff, were major contributors to this *Safety and Security* booklet:

Bruce Naliboff

Lieutenant – Criminal Intelligence Unit (Retired)
UC Davis Police Department

Stan Nosek

Associate Vice Chancellor
UC Davis Office of Administration

Michael Oreschak

Sergeant – Crime Prevention Unit
UC Davis Police Department

Maril Stratton

Assistant Vice Chancellor
UC Davis Office of Public Communications

This booklet is an adaptation of the California Biomedical Research Association's "Crisis and Communications Manual." **Web site:** www.ca-biomed.org

Special Thanks

Kevin M. Smith

Former UC Davis Vice Chancellor for Research

Robin Parlow

Crime Prevention Specialist
UC Davis Police Department

PHONE NUMBERS

**POLICE – FIRE – MEDICAL
EMERGENCY
9-1-1**

**(FROM CELL PHONE CALL LOCAL LAW ENFORCEMENT AGENCY
NON-EMERGENCY NUMBER)**

**UC DAVIS
POLICE DEPARTMENT
530-752-1230**

LOCAL LAW ENFORCEMENT AGENCY

WRITE IN