Personal Security Guide

Emergency Numbers

In Pentagon/National Capitol Region Facilities	(703) 697-5555
Hearing-Impaired Persons in Those Facilities	(703) 693-7008
In Your Home, All Other Buildings, and Your Car	Call 911

June 2005

Pentagon Force Protection Agency
9000 Pentagon, Washington DC 20302-9000

This Guide can be downloaded from https://extranet.pfpa.mil
[PFPA Admin G-001]





Table of Contents

DISCLAIMER: THE PENTAGON FORCE PROTECTION AGENCY (PFPA) DOES NOT RECOMMEND, ENDORSE OR GUARANTEE ANY COMMERCIALLY AVAILABLE PRODUCT OR SERVICE REFERRED TO HEREIN -- THOSE DESCRIBED ARE ONLY EXAMPLES OF OPTIONS AVAILABLE. THIS ASTERISK (*) APPEARING IN THE TEXT REFERS TO THIS DISCLAIMER.

1. Context for This Guide

We live in a world that is usually safe but occasionally dangerous – and the National Capitol Region (NCR) has its share of such dangers. This Guide is intended to raise the security awareness of DoD employees to general risks, and offer options on how to improve personal security, not provide direction on how to deal with specific scenarios.

It complements the Level I Antiterrorism (AT) training all military, civilian, and contract employees in Pentagon/NCR facilities must receive on arrival. The Pentagon Force Protection Agency (PFPA) provides this weekly (details are at 703-614-8677). The refresher training required yearly thereafter is on-line at http://www.at-awareness.org.

What is the Threat and What is Your Role?

The main security concern in the NCR, as in all urban areas, is from crime. That from terrorism is much lower and in this area is more likely to focus on large symbolic targets than individuals. Nevertheless, this Guide considers both threats because neither can be ruled out, terrorism is a form of crime, and at the personal level defenses against both are virtually identical.

A caution: all suspected criminals and terrorists must be considered highly dangerous. Only police teams are equipped to deal with them. Pre-emptive action by other people often puts them at physical and legal risk, endangers bystanders, destroys key evidence, and obstructs police. Unless acting in self-defense or an official capacity, therefore, *your general role in personal security is only to execute passive measures, stay alert, summon help, avoid confrontations – and let police teams do their job.*

What is Personal Security and How Do We Achieve it?

Personal security is a general condition that results after adequate steps are taken to (a) deter, (b) delay, and (c) provide warning before possible crime, (d) if such warnings occur, to summon assistance, and (e) prepare for the possibility of crime in a constructive manner. Reasonable efforts to execute these five tasks can greatly reduce security risks, sometimes to negligible levels.

Security efforts will of course differ, based on the circumstances of each DoD employee. Pentagon/NCR duties, area of residence, family activities, and other factors influence security needs. Some people may need to upgrade the security of homes; others of their children; yet others of their travel, computing, and so forth.

How to Use This Guide

To satisfy such diversity, this Guide offers a menu not a cookbook. Section Two lists basic concepts. The eight following Sections address areas of typical threat, and "best practices" in each area to accomplish the five security tasks above. DoD employees should consider selectively implementing the options most pertinent to their own needs.

The most cost-effective way to do so is usually to improve existing layers of defense before investing in new ones, though new layers may also be required. For that reason, this Guide emphasizes security awareness, cooperation in local area watch systems, cell phones, rehearsals, and lower cost options. The common themes are integration and preparation.

Therefore, (1) assess the local environment, your activities, and the most credible threats, and (2) prioritize your needs, before (3) implementing options. Before buying, you might also want to consult reputable consumer references -- DoD does not recommend, endorse, or guarantee any commercial product or service noted. Those indicated herein are only examples of the kinds of options available. See the disclaimer on the Table of Contents.

Personal Security in Context

In sum, personal security measures by DoD employees are only the last of many tiered protections that include US programs abroad, homeland defense inside US borders, and myriad civil programs within the NCR itself. The employee and his or her family should see themselves as part of this much larger team, and support the teamwork with civil and DoD authorities that will continue to make criminality and terrorism very unpromising ventures.

2. TEN BASICS OF PERSONAL SECURITY

a. Assess Your Own Situation First

Unless you have a senior role in DoD or your work is of special interest to hostile intelligence, your most likely threat in the NCR is from crime. The best start point is thus to consider where, when, and how you could be most exposed to it in the context of home, family, travel, and other activity.

b. Develop and Implement Security Plans

Once you identify the most credible threats, go to Sections 3-10, select the most feasible options, and list them in brief. Those lists are the heart of your security plans. Implement them over several months in a reasonable manner, updating them later as needed.

c. Develop Security Awareness

Although you may need to upgrade old systems or buy new ones to achieve reasonable security, developing security awareness is the most cost-effective step because it enables people to avoid threats with alertness and foresight.

d. Train Your Family

Therefore, develop security awareness in family members. Develop it in a spirit of prudence; good security practice is common sense both for their welfare and as others might try to use them as conduits to you. Discuss security from time to time, and develop/rehearse plans with your family.

e. Maintain a Low Profile

Because a high public profile attracts criminal interest, keep your name out of the news. Don't discuss your affiliation with DoD, your work in it, or display your badges, when off DoD facilities. Your building access pass is unclassified, but a Common Access Card is For Official Use Only, requiring more control. Overseas, much more stringent measures are required.

f. Control Your Space

Don't open your door to strangers or give them means of easy access. If you are unsure of people, meet them in public rather than in private. Lock cars, offices, residences, and secure the keys to them. Avoid crowds, and volatile situations where you could be jostled or attacked – and if you see such situations developing, get up and leave.

g. Notice and Report the Unusual

Develop a sense of what looks normal. If you see suspicious people, evidence of being monitored, or other threatening signs, report them to local police -- and on the EAGLE EYES site at www.pfpa.mil (click AT/FP, then EAGLE EYES) or call 703-697-5555 -- and let authorities investigate.

h. Be Unpredictable

A regular pattern of activities facilitates hostile planning, while seemingly random behavior makes it so difficult that criminals will often look elsewhere. Unpredictability can also make you and your family unattractive for the more serious crimes that require planning.

i. Secure Sensitive Personal Information

Hostile action against people often requires detail on their jobs, addresses, cell phones, emails, vehicles, social security data, schedules, and security measures. Affiliation with DoD may also excite hostile interest. It is thus wise to burn/shred trash that reveals such information.

j. Protect Computing and Electronic Activities

Guard what you say in the electronic arena and consider upgrading security features on your devices, because commercial Internet, email, telephone, wireless, and related systems are highly insecure. All can be easily monitored, threats are rising, and heavy users are at particular risk.

3. Security of Your Person

Threats here can range from attacks driven by impersonal ends, such as armed robbery, to others motivated by anger or sex and focused on you as an individual. As all such attacks are very dangerous, if you have evidence of a specific threat to your person, report it to police.

Carrying personal weapons for security, however, is not recommended, despite their appeal. Police have long known that most people are not capable of using a weapon effectively on short notice, and that those who try usually lose it to their assailants, shoot themselves, or shoot innocent bystanders. Use of a personal weapon can also escalate violence to lethal levels when the typical assailant is ready for combat and the typical victim is not. That situation does not produce good odds.

And there are other constraints. Carrying concealed personal weapons is illegal in MD and DC, and legal in VA only with a special permit. Any use of a weapon against other persons is then legal only in clear self-defense – often difficult to prove in court. Finally, DoD employees face another issue: *no personal weapons whatever are allowed on or in Pentagon/NCR facilities*.

The best defense to threats on your person is thus to try to avoid where and when they are most likely – where you could be isolated and overwhelmed, and when emotions are high in domestic disputes, alcoholic events, sexual flirtations, and similar scenarios. Ask yourself where and

when violence is more likely, avoid those situations, and decline to attend events when any excessive alcohol/drugs are expected. If threats then arise, leave quickly.

Because threats to your person can emerge unexpectedly, your well-being always requires security awareness; i.e., alertness, foresight and prudence. Developing it is an essential for most of the types of security in this Guide.

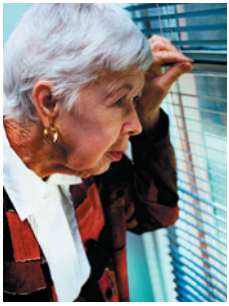
Defeating Surveillance

Criminals typically surveil prospective targets in advance to select the most promising and least secure. To defeat surveillance you need a good sense of what is normal in your neighborhood and alertness to what is not, especially near home, early in the day when movements are more predictable, and if an abnormality continues over time.

Examples of such abnormalities can include strange "children" nearby who do not play normally; "women" seeming to watch them or wait for an event that does not occur; "commuters" at stops when busses do not run or who do not get on one; "workmen" without the proper work tools or signs; "utility" vans from firms that no one recognizes; "people" in cars watching but distant enough to seem innocuous, especially if they use binoculars; and "tourists" who appear out of place or out of season.

Such "unusuals" are threatening if their timing is linked with your schedule, i.e., occurring just before or after you arrive or depart, or if the "people" involved seem to slow or alter their activity for a better view as you appear.

Children are often the first to see such anomalies. If you think you are being watched, therefore, consider having family members monitor from an upper window as you



arrive/depart, a common practice abroad. Since surveillance uses stationary and mobile means, your family may see both. In any such event, they should call 911. Only professionals can deal with such threats.

Maintaining a Low Profile

A low public profile helps reduce exposure to surveillance from criminals and hostile intelligence by making people more difficult to find, predict, and exploit, thus enhancing personal security and Operations Security (OPSEC).

Its implication is to avoid actions likely to attract personal publicity in lieu of those in school, social, business, or other *groups* that can exercise some control over publicity, and in which a person can decline to be identified. If media exposure is inevitable, you should at least ask that your affiliation with DoD, and your name, address and other personal data not be disclosed.

Train your family not to discuss such detail with unknown people, to deflect intrusive questions on your job and private life tactfully, and to treat phone calls as though others were listening. Decide with your spouse what to share or withhold from children too young to protect key data.

Pattern of Activities

Another measure to discourage surveillance and attack is to vary your pattern of daily activities; unpredictability makes prospective targets much less attractive because it exposes criminals to unknown risks.

Examples of what you might vary include meal and work times and routes, child drop-off and pick-up schedules, exercise regimes, shopping patterns, clothing, vehicles, and other routines. Use different entrances and exits, travel modes, and travel with other people. Vary your means of communication to complicate any monitoring or interception of your messages and schedules.

A related theme is to move in groups, establish buddy-teams, change from single to group movement, and use public transport unexpectedly. Take the Metro, carpool, drive with a neighbor, or let friends drive on random days.

Security on Foot

Before walking in a strange town, ask residents what parts they consider risky, avoid those, and create a safety plan. Identify police/military posts, hospitals, hotels, malls, and public complexes that might offer a safe haven. Avoid alleys, shortcuts, walking at night, and keep to busy well-lit streets. Say hello to local police. Walk purposefully, with a friend or a dog if you can, and on the side of the street facing traffic. If you think you are being followed, change pace or double back to check – and if you are, report it.

Try not to appear affluent, leaving behind briefcases that announce you as an executive in lieu of soft bags/packs. Put valuables under clothing in a money belt or pouch. Carry a whistle, a cell phone -- always a good idea for security -- or at least pocket change for a phone call. Tell family where you expect to be, check in periodically, and

set up simple codes to reveal if you are or are not under duress, e.g., "Honey, I've got (or lost) my breather."

If danger is confirmed, blow your whistle, yell for police help, call 911, or divert into the nearest haven -- whichever can get you out of danger more quickly. If assault appears imminent, you can also step into the street and flag down a passing vehicle. Doing that will of course expose you to unknown risks, but if that is the only avenue of escape, it may be your only option. This situation is the one exception to a very old and good rule: *don't hitchhike*. Then ask the driver to take you to a haven, not your home.

If you want to carry pepper spray, reconsider if you should be on foot at all, check local laws closely, and be aware that you run the risk of committing a crime, i.e., bringing a personal weapon onto DoD facilities or into some other NCR jurisdiction that constrains the carrying of weapons.

Defense Against Assault or Rape

Again, the best defense against these threats is to try to avoid where they are most likely, by avoiding:

- Isolated, poorly lit, or seldom policed areas, especially when alone, such as laundries, parking garages, parks, or wooded areas at night.

- Social interactions or dating with irrational, aggressive, or criminal persons, particularly where alcohol or drugs might be anticipated.

- Disputes in which the character/identities of people are attacked and they have no way to respond or resolve an issue without humiliation.

- Emotional political demonstrations, unrestrained/ unpoliced festivals, racial confrontations, and other turbulent or volatile public events.

- Clusters of young men, when you suspect the presence of alcohol, weapons, or public controversy.

If prevention fails, the general logic is (a) if attacked, escape; (b) if trapped, stay alive; (c) fight only in self-defense, (d) if so, seizing whatever is at hand as a makeshift club to attack the groin, eyes, or instep, and (e) memorize details so that the attacker can later be brought to justice. Attract help by any means possible -- shout "fire," blow a whistle, push panic buttons, or throw objects through windows. Your objective is to survive and escape.

Women must be especially cautious. The Department of Justice (DoJ) Bureau of Crime Statistics reports that 2% will suffer a violent crime every year, with rape a special concern. In over one-half the reported rapes, the rapist is a friend, relative, or neighbor, often with alcohol involved and no other people present.

Defense Against Stalking

The DoJ defines stalking as repeated behavior to harass or threaten victims, such as by following them, appearing at their homes or offices, phoning or leaving them messages/ objects, or vandalizing their property. Stalkers are usually men trying to develop a relationship with or frighten women -- often as part of domestic violence -- but they can be of either gender, motivated by sex/vengeance/other objectives.

Consult local police instantly if you think you are being targeted because stalkers are very persistent and often

dangerous. As defenses can be needed for long periods, you may need community help to implement them:

- Tell the stalker "no" once and only once, because any repetition or further discussion can be interpreted as extending communications.

- Refuse all contact with and packages from stalkers. Until they stop, have family screen visitors, calls, and mail. Establish buddy-teams to help you, and do not travel alone or where you could be surprised.

- Get a big dog, one of the most effective defenses, especially if it is trained. Increase home and vehicle security, per Sections 5 and 6, especially if the stalker shows anger -- often a precursor to violence.

- See Sections 9 and 10 to protect personal data and communications, help lower your profile, and increase your psychological distance.

- Take a self-defense class to learn how to become more aware of your surroundings, avoid confrontations, and recover self-confidence.

- Join a local stalking victims support group, which can advise on a key issue: how local anti-stalking restraining orders are enforced.

- Seek legal advice. If stalking is a felony, court orders are enforced, and violators usually go to jail, consider a restraining order -- but such orders can also worsen the problem if enforcement is lax.

- Therefore, document any stalking by photographing packages before return, keeping letters and phone recording tapes, and maintaining a log of attempted meetings, drive-by's, and other potential evidence.

- As a last resort, and especially if you see any signs that the stalker may be bent on vengeance, consider moving to another area, after briefing family, friends and neighbors of the stalking threat, requesting their aid to defeat it, and engaging police to assist.

The DoJ data show that 8% of US women and 2% of US men will be stalked at some time in their lives, and that some will be killed. As understanding of this threat evolves, you may want to visit Web sites under "Stalking," where new strategies are emerging to counter it.

Cyber stalking through harassing emails and faxes is a variant, often to solicit sex or initiate blackmail, drug, or other illegal activity. Because children are so vulnerable, counsel yours to seek advice if they get messages from unknown senders, and never to respond without consulting a parent. As understanding of this threat develops, guidance at such sites as www.usdoj.gov/criminal/cybercrime/cyberstalking is also emerging.

4: Security of Children

Threats to children can also range widely from the merely unpleasant, such as schoolyard scuffles, to the tragic, such as kidnapping or sexual assault. A unique threat to children, evident in the NCR as in other major cities, is the rising incidence of violent gangs in residential neighborhoods and schools.

From a security standpoint, children are an extension of the parent but far more vulnerable – and that vulnerability is a risk to the parents. When they are old enough to begin to understand threats and to act rationally, therefore, children should be included in family discussions of basic security, escape drills and rehearsals, and so forth -- but they also require special measures.

Young Children

- When young children are outside, place them in the specific care of a trustworthy person, and do not leave them unattended or alone. One parent should know where the children are at all times.

- Instruct children to keep doors and windows locked, not to admit strangers, and to call their parents if there is a knock on the door.

- If possible, place a child's room in a part of the home not easily accessible from outside, and lock any doors providing access to it from the outside,

especially in the evening. Keep interior doors to a child's room open to be able to hear any unusual noises.

- Set aside family time to talk about security, as your children grow older. Essential topics include how to (a) call 911, (b) report a fire or break-in, (c) escape in such events, (d) answer phones without disclosing key data, (e) deal with a knock on the door, (f) say "no" to strangers, and (g) deflect intrusive questions with generalities, e.g., "My Mom works on computers," not, "My Mom is a Pentagon counterintelligence officer."

- This Guide focuses on security not safety, but because children at this age seldom understand the risks of either, and training on both is often integrated, DoD parents might do well to consider how they could instill safety procedures in children at the same time. Many Web sites are available under "Child Safety" to help them do so.

Pre-Adolescents and Teenagers

- Do not allow children in this age group to leave home without advising parents where and with whom they will be, when they will return, and providing a phone number where they can be reached -- steps that will both improve security and discourage drug activity.

- An excellent step is to give them a cell phone for emergency use, and to train them in the use of speakerphone and other emergency features.

- Begin to rehearse children in this age group on measures in your security plans.

- Teach pre-adolescents and teenagers security awareness, and how to get help from police instantly if threatened on foot, in cars, or elsewhere.

- Counsel them when away from home to travel in pairs/groups, keep to busy streets, and never to accept rides from strangers -- even if such people claim that a parent asked them to "bring the children home." Teach children how to note personal and vehicle details of people making such solicitations, go to a safe haven, and call home.

- As sexual assault is a special concern for both boys and girls at this age, counsel them on that threat. Many, for example, many not be aware of the risks of a blind date. Group activities, particularly those requiring physical activity such as hiking, community service, sports, and so forth, are safer.

- Advise children 9-12 on the risks of gangs, many of which recruit preteen candidates. Indicators of gang presence can include special graffiti, tattoos, body rings, clothing, and select "hangouts." Anti-gang authorities and researchers, such as those at www.nagia.org,* www.ojjdp.ncjrs.org,* and others advise early intervention to offset peer pressure into gangs. Searching on "gangs" in local police Web sites such as www.co.fairfax.va.us/ps/police/ may also assist,

because officials report gang presence is growing in NCR high and middle schools.

Security in Schools

- Check that schools will not disseminate information on your children without parental permission. If your DoD duties are so prominent that your children might be kidnap targets, discuss with them and the school how their connection with you can be protected.

- Assess what level of publicity your children might have there. For example, if your son or daughter is a good athlete, do you agree for him or her to be identified in sports publicity?

- Establish with the school who has authority to pick up your children after class. Many schools now use signature cards to regulate this.

- Ask about a school's security plan. Laws in VA and MD require that every school have a Safe School Plan, and DC laws may include such a requirement in the future. If you have special expertise, ask if it would be welcome through the local police department, where volunteer assistance of this type is usually routed. Some NCR schools, for example, might welcome assistance in planning for the types of contingencies contemplated in Section 8.

5. Security of the Home

The principal threats in this arena are of burglary, and less often of personal assault. The aim of residential security is thus to deter prospective intruders, obstruct them, and if they do enter to delay them enough to allow residents to escape. What intruders most want to see are unoccupied and unlocked buildings, means of easy access/escape, and shrubbery that could conceal forcible entry. What they don't want to see are dogs, lights, alarms, anything to expose or delay them on-site, or a house on a cul-de-sac.

Consider the security of your home, therefore, in tiers, working from out to in. The outermost tier is a neighborhood watch system. The next includes home exterior and yard. The next tier is its physical structure. The in-most defenses are procedures by which a family lives. Try to strengthen all four.

Neighborhood Watch Systems

Criminals "casing" neighborhoods before attack often avoid those with a local watch system because it exposes them to risk. Watch systems discourage intruders equally well in single-family, apartment, and condo areas. Starting one requires friendly relationships, but once started it can function on near-autopilot to monitor and report on suspect strangers or cars, report alarms, enhance deterrence with signs, and advance security in other ways. Invite a police officer to brief neighbors on this at a local home.

Like EAGLE EYES -- the watch system for Pentagon/NCR facilities at www.pfpa.mil (click on AT/FP then EAGLE EYES) – a local program will have similar features to identify and report any suspicious surveillance, elicitation, tests of security, acquisition of supplies, persons or vehicles out of place, dry runs for attack, or deployment of assets to do so.

Home and Property Appearance

For a lived-in look, leave a car in the driveway with a dog bowl in sight. If you will be away in August when most break-ins occur, arrange to have trashcans moved, paper and mail stopped, lawn mowed, and a sprinkler turned on/off. Put clothes on a backyard line and leave on a radio.

Buy inexpensive timers to turn on lights at irregular times but don't leave on a sink light or close all the curtains -- usual indicators that people are away. Ask neighbors to keep an eye on your home while you're gone and, if it snows, to make tracks in your driveway -- as you should for them.

Electronic circuits are part of this illusion. For extended absences, ask your phone company to forward calls to your away number, and answer there as if you were home. For brief absences, set an answering machine to say you can't come to the phone just now and will call back when you can -- not that you're at Snowshoe or Ocean City. Turn off the ringer so a man on a cell phone at your back door can't hear it inside. On a home PC's "Out-of-Office Assistant" hit the "In the Office" button, saying perhaps that you will be in but not responding to email for a few days.

A parallel theme is to avoid ostentation. Don't put boxes for luxury items on the curb. When renovating, put stained

glass windows, multi-car garages, and parking for expensive vehicles in the rear. Conceal valuables from exterior view with blinds, curtains, or frosted glass. A sign in a window that electronic items have been etched and the contents of all rooms videotaped for fast recovery, can also help discourage burglars.

Reconsider activities that might also be seen as ostentatious. Burglars, also read social pages, but not for social reasons.

Exterior Lights and Alarms

Exterior cameras are a good deterrent since, even if inoperable, they imply exposure ahead. Lights are even more cost-effective. Consider installing motion-sensing lights high enough to be unreachable at exterior doors, at the corners to light the sides of a building, and in dark backyards. Low-end models, costing about $20 each, can give an illusion of occupancy with a glare of light. Higher-end models can also sound an alarm. Exterior door lights on timers can suggest that residents are moving inside.

Alarms based on motion-sensor or other technologies, costing $100-$500, also work well. Many offer panic buttons to a commercial security service, which will send guards or relay calls to 911. Those operating from phone lines or batteries do not need external power. Wireless systems offer very flexible coverage. All alarms, though, require programming and maintenance. To deter, alarms also need signs, loud output, and neighbor support -- unless organized many people simply ignore them. As there are many factors in selection, you may want to visit Web sites such as “Burglar Alarm Basics”* before you buy.

Physical Security

Survey the physical security of your home with one or two friends, and do the same for them. Ask how you would break in, list the deficiencies, and correct them. Sometimes a police officer can assist, if a block of homeowners requests it. Conduct your survey from the outside in:

- Consider fencing as a psychological deterrent. It won't stop a determined intruder but it will complicate access and imply a dog. Lock gates, especially into an alley that provides rear access.

- Remove names from doors/mailboxes so that no one in a car can call directory assistance, get the number for your name, and see who is home.

- Prune shrubbery to below window level for vision out to about 20 feet, and trees to prevent second story access. Lock up ladders/tools that might provide access. If you want shrubs next to your house, look first at pyracantha (firethorn) and prickly holly.

- Protect power by installing a lock on your fuse box and any exterior regulators or stand-by generators.

- Consider sealing off/replacing pet entrances and louvered windows, which are inherently much more vulnerable and difficult to secure.

- Because a garage offers concealment for forced entry into a home, reinforce any weak panels on garage doors, and install an electronic opener for about $150 to make it near impossible to force.

Burglars know that the initial code is usually all zeros, so change that quickly.

- Because most break-ins are from kicking in a door, get solid wood or metal-backed outer doors with peepholes. Replace cheap locks with quality hardware, and a cover plate to keep shims from being slid in to push the lock tongue back. Anchor lock housing and striker plate with 3" screws deep into framing lumber. Reinforce framing under the latch with a 1/8" x 2" x 2' steel strip, and install deadbolt locks, placing the latter at knee height for best protection against kick-ins.

- Ensure the slider of a glass door is on the inside track (glass doors are often installed backwards), and lock it in place with a pole in the bottom track. Prevent it from being lifted out with removable pins into the side frame or screws in the top track giving just enough clearance to move. Sliding doors must have locks, and are a good place for decals that you have an alarm or a vicious dog -- a threat you can make vibrant with a chain and a big dog collar on a nearby tree.

- Consider double-paned windows to complicate the cutting of holes, safety coatings to make them harder to break, and keyed locks that can resist a wire forced under the sash to pull back the rotating lock installed on most windows. As with sliding doors, use poles or pins along the sides, or eyebolts in the corners -- ensuring that all can be removed fast in case of fire. For high-risk basement, first floor, or street-level windows, decorative metal grills/accordions, warning decals, and unbreakable glass block can be excellent options.

- Lock the doors and windows of your home routinely, set up specific key controls, and don't leave home-keys with a car being serviced. Swap keys with trusted neighbors, and don't try to hide them outside entrances. Locks are only delaying mechanisms, but optimize their value with good controls, a locked-home policy, and family training.

- Upgrade the door and lock of one room as a safe haven where the family can take refuge for up to 10 minutes from violent intruders, call for help, and from which they can escape in emergencies. An upstairs bath with a cell phone, emergency numbers, flashlight, rope ladder, and a window from which to throw it, can be a good choice. The reliability of the doors, locks, and cell phone are a first priority.

- During any home renovations, ask contractors for advice on security upgrades. Once on-site, firms can often add many at little extra cost, and might do so free if allowed to show them to neighbors.

Dealing With Intruders

This scenario requires careful thought, pre-planning, and rehearsals because all key measures must be taken before and not after intruders arrive.

The best solution is prevention. Keep doors locked and don't open them to unknown/unexpected deliverymen, salesmen, utility workers, or others. If several arrive, direct all but the smallest to get back in their car and tell that person to stand back, show ID at the peephole, and give you phone numbers to check credentials. If still you are uncertain, tell them to leave or call 911.

This level of prudence is crucial for women, children, baby-sitters, and older people, easily overwhelmed at a door. A good rule is that when the parents are gone no one under 18 will open a door, and that parents or a trusted neighbor will be called if any unknown person knocks on the door.

A special problem is that the threat at the door may be a person seemingly close to the family, such as a pedophile neighbor, rejected lover, or spouse who lost a court custody battle. The best course is usually to identify such threats in advance, change locks and upgrade physical security, and set up firm rules for children and baby-sitters.

Once an outer door is opened, the utility of other means to delay intruders is in doubt. You can install panic buttons next to doors to sound alarms, and you should program phones with a 911 button in speakerphone to let police hear what is occurring and see the address -- but not all cell phones have this feature. A big dog can help discourage intruders. Shouting "fire" may also be enough to attract help and give family members time to escape.

However, there is no good response to a home invasion if you are surprised and trapped. You will have to decide fast whether to comply, negotiate, or resist. If by contrast you sense intruders first, perhaps in another room, try to barricade the door, call 911, yell that police are en route, and get out. Your purpose is to save lives, so don't confront or fight with intruders except in self-defense.

If physical security fails, escaping is always the best option, because the faster anyone can get out by any means whatever, the faster intruders are likely to leave -- they are then at risk of discovery. It is thus vital to spend time rehearsing escape plans, particularly with children.

Other Residential Security Measures

Security when returning home also requires alertness. Have your key ready for quick entry as you approach, but if you see a door/window open or signs of forced entry, don't enter. Call 911 and wait for police to clear your home.

Before letting utility workers or domestic help into your home, investigate their IDs, references, and employers closely.

Close the curtains in a room before turning on lights, and consider placing phones where they will not be seen from doors or windows when answered.

Law enforcement studies show that many people, when seriously frightened, cannot punch 911 on a telephone correctly -- but can with practice. Family members should thus practice about once a month with a phone on the hook.

Bomb and Hostage Threat Calls to a Home

Most such calls are hoaxes, but assume they are real until proven false. A key point is that deranged/illogical callers will often disclose valuable detail:

- *As soon as any threat is stated*, tell the caller you need to get pen and paper, put the phone down, quietly ask someone to go next door and call 911 for a line trace, and resume the call on speakerphone so that others may listen and help extend the call on-line. When it ends, call 911, evacuate, and let police search for/remove any suspected bomb.

- Write down exactly what is said. Request caller name, address, and phone number, saying you need those to ensure the warning is real. Ask for location, type, appearance, fuze, and timing of a bomb. Ask for whom the threat is intended, if demands can be met otherwise, and so on. Project calm, respect, and compliance as you listen for background noises that could later help locate the caller.

6. Security in Vehicles

Threats in a vehicle can range from surveillance and stalking to attempted shootings and other types of assaults. Because cars can be turned into cash so easily, however, most threats are essentially of crimes against property. The usual risk here is thus to your car keys and registration.

Security in this arena echoes many of the themes in Sections 3 and 5, but it includes others that exploit the mobility/protection potentials of a vehicle.

Defenses Against Car Theft

Look under "Most Stolen Cars" on the Web to identify those most at risk. It is nearly impossible to stop determined car thieves from stealing a car on a street because it can be towed or lifted. Owners of high-value vehicles should thus consider both anti-theft deterrents and recovery systems to find a stolen vehicle. Recovery systems are advertised for about $700 from www.LoJack.com* and other Web sites that claim recovery rates of 90%.

There are many deterrent systems, to include engine/ignition interrupters, steering wheel locks, electronic keys/alarms, and so forth, ranging in price from $100 to over $700, but competent thieves can defeat virtually all of them. The most successful appear to be those that modify the wiring harness to require that a unique module be inserted at the dashboard to link circuits and start the car, of which an example is at www.neverstolen.com.*

There are many simple measures that can defeat an amateur car thief, and slow down a professional; 50 of the best are at www.watchyourcar.org.*

Before a Car Trip

Exercise prudence: don't leave keys in any car that you want to keep. Try to park in well-lit areas, with the vehicle and the trunk locked, or park in a locked garage. If suspicious people are nearby as you approach, return to a building until they depart -- most attacks occur when people are opening a car door. Have a key ready as you approach, look inside before entering, and lock the doors. As you leave, think about your route, alternate routes, safe havens, and check in with your office/family via cell phone.

Before trips, inspect your vehicle and its fluid levels. If you think people may really be trying to harm you, alert PFPA and local police, then get in the habit of checking under the chassis, hood, dashboard, seats; and in the trunk, wheel wells, exhaust pipe, and fuel cap before you start. Two people can do this in about 60 seconds with a little practice. If you see anything amiss, even a prankster's firecracker, call 911 and let experts remove it.

Security On the Move

On the road, keep the car locked, with windows up so people can't jerk open a door, especially at stoplights or crossroads where most car-jackings occur. Don't stop needlessly, as slow-downs increase risk. Pay attention to cell phone emergency help numbers such as #77 posted on local highways. And under no conditions pick up hitchhikers, to whom a driver is totally exposed.

Avoid isolated roads/shortcuts where unobserved halts might be required, being wary of situations ahead such as “flagmen” with no tools, “cyclists” who fall in front of your vehicle, or “accidents” where the “victims” are watching you. If you do sense danger, blow the horn, turn on flashers, and back out. Don’t try to be a stunt driver in doing so, however, which all too often produces an exhilarating trip to a courtroom, a hospital, or a morgue.

As you drive, leave ample room between your vehicle and the one in front, keeping to inner lanes when you can, to avoid being forced off the road. If another driver takes hostile action or tries to force you over, drive to a safe haven, park in front not worrying about a legal space, and get inside quickly. Don’t confront the other driver. Report the other car’s license if you can, but not if it puts you at risk; your first objective is security, not justice. Alertness and preparation to escape are more important now than in years past, due to the rising incidence of “road rage.”

If you think you are being followed, change speeds or go around the block to check; if you are, again don’t go home but to a safe haven and call 911.

Security When Stopping

If your vehicle develops mechanical trouble, stay inside with windows up and doors locked until police arrive. To signal distress, display a sign, tie a handkerchief to the antenna, and put up the hood. When someone stops to help, don’t leave the vehicle -- ask that they call police or a service provider.

If you are involved in a minor collision at night or in an isolated location, don’t stop to inspect damage or talk to

drivers. Put on your flasher lights, drive to the nearest safe haven, and exchange accident information there.

Because Automatic Teller Machines (ATM) pose special risks, especially from 7:00 to 10:00 p.m. when half the ATM crimes occur, conduct actions there quickly. Drive on if lights are not working, the machine is balky, suspicious persons are nearby, or you see anything out of order. At a drive-in ATM, keep all car doors and windows locked except your own window, so people can't climb in with a greeting and a gun. Count your money later, not on-site.

When dropping someone off, wait until passengers have safely entered their residence or destination, because you are part of their security until they do.

7. SECURITY ON TRAVEL

Travel in the United States

The security measures in Sections 3, 4 and 5 apply equally at home and away, but other aspects also apply on travel:

- Share travel plans only with people who have a clear need-to-know, because burglars, car thieves, and others can exploit them and will sometimes pay cab drivers, waiters, and others to try to get them.

- Because airports/stations attract criminals and terrorists, travel light. To frustrate pickpockets, be alert to jostling, bring few valuables, secure them in a pouch inside clothing, avoid handbags, and carry wallets sideways in a front pocket. After check-in, don't linger near ticketing, where you are vulnerable, but move inside the security area.

- Try not to use a DoD address or home data on luggage tags in travel. Instead, use a friend's address or a Post Office box address. Put a 3 x 5 card with that data inside each bag, in case it is lost.

- As overnight parking at airports is also risky, go there by public transport if you can. If you can't, park under a good light close to well-traveled areas or a security station, ensure no theft-worthy objects can be seen in the car, and secure the faceplate of the radio/CD player elsewhere.

In Commercial Lodgings

- In budget hotels/motels, avoid rooms with no phones or deadbolt locks, or with sliding glass doors. As burglars prefer the first floor, and most car bombs are lethal only to the 3rd, ask for a room on floors 4-7, which are within reach of fire ladders.

- At better hotels, ask the bellman to remain as you inspect closets and bath. Keep your key with you, the door locked, and don't allow in any strangers or unexpected packages. Do not disclose name or rank when answering a phone. If you depart for the day, close curtains, turn on a radio/TV, leave on the lights, and don't turn in your key at the desk but take it with you.

- If a room was reserved in your name, change it to another when you arrive. Then tell the desk that you'll be sleeping in, place a "Do Not Disturb" sign on the door, and use side entries to come and go.

- Portable jamb locks to bar passkeys from opening a room or bureau drawer are at http://store.safetycentral.com/porcomdoordr.html* and at other Web sites under "Portable Locks." A doorstop alarm that can be wedged under a door and that will emit an alarm if forced is at www.magellans.com.* Such devices cost $10 to $30 each.

- If paged, an old trick of thugs waiting to rob people in elevators or stairways, don't respond directly but call the front desk first to check.

Travel Outside the United States

Travel abroad opens you to much greater criminal, intelligence, and terrorist threats, requiring stringent country-specific measures. Before departing on private or official travel abroad, and before any official travel orders can be issued, all DoD Military, civilian, and contract employees must receive a Level I AT briefing (see p. 1), and Area of Responsibility (AOR) briefing. Those with Sensitive Compartmented Information (SCI) clearances must also receive a third presentation. Your Security Manager can advise on how to meet those requirements. You may also want to consult:

- *DoD Antiterrorism Handbook*, DoD O-2000.12-H of 9 Feb 2004 is For Official Use Only, but pages 187-206 provide a superb list of generic personal security measures for travel and work abroad.

- *DTRA Security Passport for Safer Travel,* summarizes many of the key points in the pages of the *Handbook* above, and fits in a shirt pocket. It is available from DTRA at (703)-767-5939.

- *DIA Personal Protection Measures Against the Terrorist Threat*, at www.ncix.gov/whatsNew/index lists personal AT measures in more detail.

- The Department of State provides the most recent information on international threats at www.travel.state.gov, or at (202)-647-5226.

8. Security of Mail, Food, and in Disasters

Mail Security

Because the US Postal Service and express delivery services screen mail to civil addresses in much the same way as they do for mail to the Pentagon, the risk of contamination/bomb attack through the mails to a home is very low. As explosives can be disguised in any shape, however, it still makes good sense to be able to identify any suspect items delivered by hand:

- Restrictive, person-specific markings such as "Confidential for Mr. Dix," "Personal for Mr. Dix," or "To be Opened Only by Mr. Dix."
- Foreign or no return address, excessive postage, or a return address so poorly typed or written as to suggest its obscurity was deliberate.
- Incorrect titles, titles but no names, or addresses that are misspelled, or vague, e.g., "Directer, JCS Iraq Oporation." Any mail to a private address with an addressee's current DoD position title is suspect.
- Oily stains, discolorations, sponge-like feel, sweet non-food smells, or any substances or fluids coming from an envelope or package.
- Excessive weight for the container; envelopes that are thick or rigid; packages with internal wires or electronics; or any with a hole that appears to give access to an arming device or safety wire.

- Excessive tape or binding cords that seem to compress the package or envelope, especially for mail arriving at any abnormal hours.

- Mail with visual distractions to disarm caution, such as pornography or cash immediately inside the wrapping, or evident just underneath it.

Do not try to move or open mail with suspected explosives or contaminants, as most mail bombs are designed to be victim-activated. Evacuate the area, report the item to 911, and to PFPA at Eagle Eyes (see p.5), and let specialists investigate the item.

Food and Beverage Security

The potential for attack of DoD officials or their families by contaminating food and beverages is also slight because of the rigor of public health laws, the obstacles to acquiring/ handling poisons and toxins, and the difficulty of poisoning public water in the huge volumes needed to do harm.

The security of food and beverages before they are sold results from strict federal laws and inspections, care among producers and vendors -- who can be ruined by even a hint of food contamination -- and your anonymity as a buyer in a mass market. The only practical thing you can do when you buy is thus to check that security wrappings on food/ liquid containers are unbroken.

After food and beverages are purchased, however, their security will rest on routines in your family. Groceries, for example, should not be bagged and left insecure, especially with a name on them. Oversee preparation, serving, and sanitation. If you find unpurchased food items at home, ask how they got there. Don't let strangers linger in a kitchen.

If you suspect tampering with your supplies, call 911; such a situation may have wider implications, even if the cause is more likely to be children or pranksters than criminals.

In restaurants/bars, if you step away from a table, have someone watch your food and beverages to ensure nothing is added to them in your absence.

Preparing for Major Disasters and Fires

If a natural disaster or weapons of mass destruction (WMD) attack occurs when you are in a DoD facility, its emergency action plan will include you.

If, on the other hand, such events occur when you are not in DoD facilities, you will have to evacuate or shelter your family in place, a decision that will likely be dictated by circumstances. As it is not possible to predict which option may be required, you need to plan for both.

If you have little experience with disaster planning, you may want to review sites such as http://training.fema.gov/EMIWeb/CERT/. The Red Cross then has an excellent template to organize a private plan for such contingencies:

- Step One is to assess what might occur in your area. Events such as a WMD/RDD (radiation dispersal device) attack might, for example, occur near national symbols in the NCR, but would probably affect residential areas only in a downwind plume. The more likely risks -- dangerous because often overlooked -- are of winter storms, fires, flooding, toxic spills (near road and rail arteries), and tornadoes. Such events can also interrupt local electricity, gas, water, and telephone services.

- Step Two is to create an evacuation plan, if that should be required. Decide on several issues with your family. If you must evacuate:

  - Choose two places to meet if you must leave your home: one just outside in case sudden evacuation is needed, and the other outside the neighborhood if you or other family members cannot get home. Identify where pets could go if you must leave for some time.

  - Ask an out-of-state person to act as emergency point of contact (POC) to whom each family member can report status and check on that of others. Give family members cards with addresses and phone numbers of the meeting places and emergency POC.

  - As fires can move quickly and give little warning, install smoke detectors and fire extinguishers on each floor. When you change clocks for Daylight Savings Time, change batteries in the smoke detectors. Put a $30 rope ladder in every upper story bedroom, and practice using it in drills. A good checklist for actions during any fire is at www.ready.gov/explosions.

- Step Three is to prepare and rehearse a shelter-in-place plan. Teach the family how to turn off electricity and gas. Post local emergency numbers at phones and teach children how to call 911. Change the set-up of items that might cause injuries (see www.osha.gov), and consider taking a first aid course. Of primary concern:

- Prepare shelters in case you must seal the house and wait out an emergency. In floods or toxic spills, shelter in an upper story, for which your shelter might be the safe haven discussed in Section 5, p. 24. During WMD/RDD events or tornadoes, shelter in basements.

• Step Four is to pre-position supplies for Steps Two and Three. For example to shelter in place without heat or electricity for 5 days, a notional period for planning, you may want water, non-perishable food, a cooler for perishables, first aid kit, flashlight, medicines, battery radio, cell phone, contact numbers, glasses, limited cash, and tape/sealants to make a home airtight.

- Store such items in shelter areas, in water-resistant containers to protect against mold. Replace water every 3 months, food every 6, batteries every 12 and, check that the phone works.

- In case you are isolated with only what is in your car, put a kit in it with blanket, walking shoes, clothes, and other selected items.

- For grab-and-go situations, you may want a kit with contact data, aid kit, medicine, glasses, flashlight, and cash, near the front door.

• Step Five is to execute the advice of emergency management (EM) officials in your area, who will advise on Emergency Alert System (EAS) messages whether to shelter in place or evacuate. Don't try to recover children at schools, which will be executing

their own shelter-in-place or evacuation plans. EAS messages will come from:

- AM: WTOP (1500 AM), WMAL (630 AM)
- FM: WTOP (107.7 FM), WGMS (103.5 FM)
- TV: Channels 4, 7, and 26 (note: since cable channels vary by district, ask your cable provider which will carry EAS messages).

Implementing these five steps will help you and your family survive major disasters, and will satisfy the Department of Homeland Security request at www.Ready.gov that all citizens develop private emergency plans.

Many city and county EM offices now offer emergency text messaging direct to cell phones, pagers, and mobile devices. You can sign up for the Arlington County system, *Arlington Alert*, for example, under "Emergency Preparedness" at www.co.arlington.va.us.

9. Security of Identity, Social Security, and Credit Data

Identity and Personal Identification Numbers

The theft of Social Security, credit/debit, and related personal identification numbers (PINs) and passwords to create a fictitious identity threatens your security because it can enable people to empty your bank accounts, commit crimes in your name, and threaten you. In 2004, children, relatives, friends, and others with routine access to the home caused about half the reported theft, stealing an average of $15,607 per victim.

If you sense that any such data has been stolen, report it fast to your banks and credit card issuers, to the Federal Trade Commission's Identity Theft Hotline at 1-877-438-4338, and go to the FTC's Web site at www.ftc.gov, to create an Identity Theft Affidavit to give to all concerned.

You can't do much about hackers trying to break into central databanks, a problem that authorities can usually contain quickly, but you can eliminate the much more common and dangerous low-tech means of identity theft:

- To defeat theft of credit card data by a small handheld device, and to ensure that no extra imprints are made on blank charge slips, pay in cash or watch your card in use when paying in restaurants and stores.

- Don't give PIN numbers to strangers or let them "shoulder surf" to watch in person or with a cell-phone camera as you input data. If buying by debit card, sign the slip as if you were using a credit card.

- Likewise, be alert for "phishing" – anyone asking you by Internet, email, or phone to "verify" your key data, "standardize" it for a new computer program, or respond to official-looking but fake forms, especially from offshore. To check the latest such con games, see www.fraudwatchinternational.com.* Never give any such data to people whom you did not yourself call.

- To defeat "dumpster-diving." i.e., the searching of family trash for sensitive data, shred/burn all outdated bills, monthly bank or brokerage statements, "pre-approved" credit card offers (the latter can justify a request for your credit report), and sensitive medical files. Inexpensive shredders that fit on a wastebasket top sell for under $20. Secure data to be saved in a container.

- For the same reason, empty your mailbox so mail cannot be pilfered, or consider a door-slot or a mailbox lock. Tell the Post Office when you move, so that mail does not end up in the wrong hands.

- If monthly financial or other sensitive statements unexpectedly stop arriving, call the senders to see if they were asked to change your address, a frequent trick by identity thieves to access your data.

- When making online purchases, look for a statement that your data will not be passed on,

and an unbroken lock or key in the bottom of the browser window -- the vendor encrypts such traffic. A double-click on that will usually confirm that you are talking to the right company.

- Major credit card issuers are now increasingly offering password protection for credit card numbers. If yours does, apply for it.

- Refuse to give out personal data at sales counters, to those who ask to interview you by phone, or in product registration forms. Most of it goes to marketing offices, but it can also leak to people with more than marketing in mind. Releasing such data requires a leap of faith.

- Likewise, don't discard credit card, ATM machine, or transaction slips on-site; they can reveal key data, alone or compiled with other items. Destroy them, and avoid businesses that do not secure them.

Social Security Data

A Social Security Number (SSN) is even more sensitive because that and a birthday are often all one needs to open a fake bank account, create fake ID cards, and launch other actions. As the government cracks down on abuses:

- Be aware of who *must* have your SSN: only governmental agencies that manage tax and benefit actions, and financial institutions. That includes state motor vehicle, tax, education, and welfare offices; and banks, brokerages, and employers. Unless you are claiming benefits financed by

the government, it does *not* include doctors, lawyers, utility companies, or others. Give them alternate ID.

- Don't carry your SSN in wallets, glove boxes of cars, or other places of likely theft, and don't use it as a password or put it on checks. Do not allow employers/banks/others to put it on a monthly statement or use end digits for ID -- a key action to protect SSNs from data search firms.

Finally, take your name/address off major direct-mailing lists. Don't call or use the Internet, where many con artists are trolling for your data, but *write*:

The Direct Marketing Association
Mail Preference Service
P.O. Box 282
Carmel, NY, 10512

In summary, identity theft is very painful. New threats are evolving. Multiple layers of defense are thus essential. If you need to know more about this arena, check the Web under "Identity Theft," and sites such as http://www.usdoj.gov/fraud.htm. and www.pueblo.gsa.gov/scamsdesc.

Personal Data In the Public Domain

If you are not aware of how much data on you is already on the Internet, see www.SearchMil.com,* www.Google.com,* or www.AlltheWeb.com,* searching on your (1) name, (2) email address, (3) instant messaging (IM) nickname, (4) phone number, (5) title of photos in which you appeared, (6) school alumni Websites, (7) fraternity/sorority, (8) local volunteer groups, and (9) any networking or dating sites you may be using or querying. In an age

when activities are increasingly recorded 24/7, the results may surprise you.

More data on you is at (10) city/county real estate records, (11) marriage records in jurisdictions where you married, (12) voter registration rolls, and (13) departments of motor vehicles (DMV). The telephone book (14) is a commercial record, but often treated as if it were also a public record.

You will not be able to remove data from public records, but jurisdictions in most areas will move it off-line and block it from public release if requested, including state DMV and voter registration offices. You can usually remove data from privately managed Websites by writing their home page manager, and from phone books by paying slightly more for an unlisted number.

A more timely action, because recent data is more sensitive, is to ask before entering a new activity what public archive is likely to result from it. You need not appear in that picture of the choir if you don't want to do so.

Biographic Data on DoD and Public Nets

General bio-data on senior DoD officials is in the public domain because of their duties, but Privacy Act data on them and on all other DoD members is protected behind DoD firewalls and on ".mil" servers. If you need to post detailed data on yourself or others on a DoD net, ensure that it meets current DoD policy and security guidance, and ask your DoD net administrator how to put it behind a password or Public Key Infrastructure (PKI) protections.

If you must issue official bio-data for use at a public forum, check current policy, security, and also public affairs guidelines -- which change at times.

Protecting Your Credit Rating

The first rule of credit security is to manage finances prudently. Most financial threats are in fact self-inflicted. Live within your means. If you use a dozen credit cards, for example, closing all but two will help clarify cash flow, as well as reducing risks of identity theft.

The second is to review your monthly bank statement, to see that all purchases were in fact yours. Criminals will sometimes make small purchases first to see if they go undetected before making large ones.

The third rule is to check your credit report at least annually. Order a copy of your report from one of the three major credit-reporting agencies:

- Equifax: to report fraud, call 1-800-525-6285; to order a report, call 1-800-685-1111 or write P.O. Box 72041, Atlanta GA 30374-0241.

- Experian: to report fraud, call 1-888-397-3742; to order a report, call 1-888-397-3742 or write P.O. Box 9532, Allen TX 75013.

- Transunion: to report fraud, call 1-800-680-7289; to order a report, call 1-800-916-8800 or write P.O. Box 1000, Chester PA 19022.

If you see problems, call the fraud offices of all three, request a fraud alert, and follow up in writing or they will not be obligated to act. The alert will require them to take your name off the list of financially sound prospects that they sell to credit card firms, and require vendors to contact you before opening loans or accounts in your name. Report

the facts to your credit card company, other creditors, police where the theft took place and where you live, and give them all a copy of your Identity Theft Affidavit (see p. 41). Finally, keep copies of related documents until your good name is restored.

Even if no problems appear on your credit report, you can initiate a fraud alert as a preventive action – and many people do. This option is also free, and it should reduce the number of credit card offers in your mailbox.

A good option is to accept a "guard service" (also called a "credit monitor" or "financial alert" service) at your financial services provider. For under $100/year, often free if you open it on-line, such services can install per-day spending limits, send alerts if credit ratings change, require more PINs and passwords, stop people from opening accounts in your name, and take other actions to reduce credit loss/trouble. Another good option is to ask service providers to put your photo on all credit and checking cards -- and cancel cards from providers that do not.

Finally, if you are still in difficulty, seek advice from consumer attorneys. Data in late 2004 indicated 84% of credit reports had errors in them, 54% had data that was outdated or belonged to strangers, 34% showed accounts open that had been closed, and 25% had errors so serious as to bar credit for a home loan. Consult Web sites under "Credit Scores and Credit Reports" on how to dispute errors, resolve inaccuracies, and file lawsuits if needed.

10. SECURITY OF COMPUTING, MESSAGING, AND TELEPHONY

Protecting Against Spam, Viruses, Worms and Spyware

Your security also includes defending a home computer against "Spam" -- unwanted messages that can include "viruses" that destroy your software, "trojans" that can search for your identity/sensitive data, "spyware" (also known as adware) that can record your keystrokes and track your computing habits, and "worms" that can carry all three and export your data. Viruses often arrive via infected disks or emails, spyware via the Internet, and trojans and worms via a network or browser. If you use a Microsoft (MS) based personal computer (PC), consider these steps to defend yourself and your system:

- *Caveat Reader:* treat all ads direct to home computers as fraudulent. Unless a message is from a trusted entity, delete it and don't open or preview it. Fake messages may claim to be "returning" unopened mail, have vague but catchy titles such as "Love You," offer a come-on, or misspell title words to fool firewalls. Delete freely and fast.

- Likewise, don't open any email attachment unless it was expected. Spammers often steal address books, send an email to each person on it, and conceal spyware in an attachment. Delete without mercy all messages claiming to warn of a virus because many of them in fact carry a virus.

- Install a firewall. Examples of good firewalls are free at sites such as www.ZoneLabs.com,* and for sale at www.BlackICE.com,* www.symantec.com,* www.mcafee.com,* and other sites. Many let you control what programs may talk to the Web. Two-way firewalls will bar both incoming viruses and data an on-board virus is trying to export.

- If your PC has no firewall, shut down until it does, and never leave it on long because it could send a thousand emails on short notice. In 2004, DoJ showed that hackers could find and hijack unprotected PCs in about 20 minutes. A firewall is even more crucial for PCs that use cable modem, Direct Subscriber Line (DSL), wireless, or satellite links to the Internet, because such "always-on" circuits are so much more vulnerable.

- Likewise, install good software that routinely scans your files. At http://www.cert.mil, DISA offers leading firewall and virus scan programs free to DoD employees who access from ".mil" or ".gov" addresses, and encourages them to download and install it on personal systems (note: this benefit is not open to DoD contractors, unless the software is to be used on a DoD-owned computer system).

- Subscribe to the free/low-cost services that software vendors offer for online upgrades (also called "patches" or "hot fixes"), a critical step *because regularly updating their software is by far the most effective security measure that most people can take*. Apply updates immediately, because the update message can alert hackers to your weakness.

- If you buy on-line, do so only from official vendor Websites, not from pop-up or Internet ads. If you think you have a valid message from a vendor, call its customer support and check before opening it.

- You can delete pop-up ads that got past firewalls with excellent free programs from www.toolbar.google.com,* www.panicware.com,* or browsers from www.mozillafirefox.org,* among other sites.

- On your Web browser security setting (look under "Tools," "Internet Options," or "Preferences"), scroll up to at least "medium" to bar Web programs such as Active–X, JavaScript, or Java from operating or downloading without permission. They are a threat, as they can be programmed to do nearly anything on a computer that you can.

- Likewise, don't download free Instant Messaging (IM), music, movies, or other entertainment from the Internet. All are shared programs (also known as distributed or peer-to-peer files) that reach deeply into a computer, opening it to infestation. Such entertainment sites are often loaded with spyware and infringe copyrights, putting you at both technical and legal risk. Delete any such "freeware" your children may have installed, buy programs at reputable vendors, and advise the family.

- If your machine begins to act like an electronic billboard, re-directs you to other sites, displays unknown toolbars or icons, changes your browser or search engine, displays random error messages, acts sluggish, or certain keys don't work (often the Tab) -- spyware is very likely on board. Tools to erase it are free at www.lavasoft.de,* and sold

at www.Webroot.com,* www.Spybot.com,* and other sites. Linking Ad-Aware* at www.lavasoftusa.com/software/adaware/ * with SpyBot* is particularly useful. See www.us-cert.gov/cas/tips for a discussion of more recent threats if you are technically inclined.

- Because so many viruses aim for MS Outlook or Express, consider other email programs to reduce risks. If you must retain Outlook or Express, MS MailFrontierDesktop* at about $30/month is one option. If you have an email preview panel, disable it to prevent Spam from reporting back that you are in good health and ready to receive more.

- Consider also changing your Internet Service Provider (ISP) to one that blocks Spam by forcing senders to identify themselves before messages enter your PC, or by diverting messages with unidentified addresses to a bulk file for review. Your ISP help desk can advise on this point, and assist if a spammer has already entered your PC.

- Don't put your email address into a public directory because if it includes an "@" sign, spammers will find it. Instead, consider free services such as Hotmail* or Yahoo* that can be cancelled if Spam arrives, while holding a second address at your ISP where personal emails can be sent. Never publish a DoD address or you can open a whole NCR net to Spam -- and you may receive a security visit.

- For like reasons, "un-subscribe" from e-lists that do not assure email privacy; some will show privacy policy in the message frame, others you must query.

However, don't un-subscribe directly from obvious Spam. Instead, manually add the IP (Internet Protocol) address of the Spam sender into your firewall, a simple copy-paste step.

- Create strong passwords, with 8 to 14 letters, numbers, and symbols, and avoid names, street addresses, and other obvious targets for hackers.

- Store critical data such as passwords, encryption keys, and sensitive personal data on paper in a locked container, not on a computer. By the same logic, back up files and programs regularly on removable drives, disks, and writable CDs, that viruses and hackers can't reach.

In sum, if you use a PC linked to the Internet, you need layered defenses. More advanced options are at www.download.com,* www.microsoft.com,* other Web sites, and in phone books under "computer security consultant."

If you use a Mac computer and install the security updates that Apple issues, you can also get junk email, but need not yet worry about serious viruses, worms, or spyware, due to higher security of that system and the fact that hackers have so far been less attracted to the much smaller Mac "world."

Wireless Computing and Messaging

The huge popularity of wireless local area networks (WLANs) for mobile computing opens new risks because their medium is inherently insecure and their infrastructures more exposed than in hard circuits. Wireless laptops, "Blackberries," palmtops, and similar "personal" devices face such risks.

Those arise because service vendors manage traffic between sending and receiving PCs, and because home/office wireless nets often lack defenses. Wireless users assume that intermediate managers will not read traffic and that incoming traffic will not have viruses. Those can be big assumptions.

Be aware also that "Wi-Fi" networks for home use do not require account numbers and, like all wireless nets, are always "on." Anyone with a scanner on the "Bluetooth" (i.e. Wi-Fi) protocol can monitor such nets, wait for a cell phone, laptop, or "Blackberry" to chirp, and download its traffic/files. Such devices are most vulnerable in their "discoverable" or "visible" mode. It is thus best to turn off both the Wi-Fi and Bluetooth features when not in use.

A related concern is that when a wireless device transmits, it can expose a user's location to within a few yards, as both the transmission and the "cell" carrying it can be located. An adversary who steals a list of customer names from a carrier can locate and identify a sender from transmissions -- not normally a good situation.

Finally, the cramming of programs into tiny packages also entails tradeoffs. Cell phones and messaging devices, for example, have so few security features that many can be remotely turned "on" without indicating that status. This enables equipment at a distance to turn many into covert bugging or viewing units, open new channels on them, insert malicious code, infect the networks to which they link, and force unadvertised features to appear.

For all these reasons, you should apply caution in using wireless laptops and personal electronic devices. Several basic options can help minimize risks:

- Screen message content. Assume when you send wireless messages or retrieve stored emails that the world is listening and that you are operating a mini-broadcast station. Such traffic is no place for PINs, SSNs, passwords, or sensitive personal/DoD data.

- Likewise, don't store such data on mobile devices because of the risk that they can be penetrated, and the even greater risk of their being lost/stolen.

- Keep messages short to limit the time hackers will have to find and attack you, and to enter the nets to which your program gives access.

- Disable wireless devices and prevent all intrusions by removing the batteries, and replacing them only to listen to saved calls or call out.

- If Wi-Fi is crucial for your cell phone, mouse, keyboard, laptop, etc., configure such devices not to allow discovery of new connections, and alert you if they try to do so. Likewise, accept no files transmitted via Wi-Fi/Bluetooth channels.

- As the wireless net in a building may lack firewall/virus protections, ensure that your wireless devices have both. The software discussed earlier in this Section protects wireless as well as fixed computers, with variants of it available for handheld devices.

Such steps will help protect your devices, but if you install a home wireless net, you must take other measures

to protect the network itself. Some of the more feasible technical safeguards apply at your wireless network router:

- If it supports Wired Equivalent Privacy (WEP), a protocol for basic net security and privacy, enable that; if it supports Wi-Fi Protected Access (WPA), enable that instead since WPA offers more security.

- At purchase, ask the vendor to (a) change the default Service Set Identity (SSID) of the wireless router to one unique to you, (b) disable SSID broadcast, (c) change the local administrator password on the wireless access port to your own, (d) disable remote administrator access, (e) install the most recent firmware and security patches, and (f) not to include your name, address, or other information by which you could be traced in the new defaults.

- If a vendor will not do these things, do so yourself with instructions in the box or with technical help. If initial settings are not changed, a net is exposed to eavesdropping and manipulation.

The encryption of laptop and other wireless data traffic is possible with a "remote client" system for about $500/year, but you should research Web sites on "wireless security" or engage technical help before doing so, as technologies are changing and may require unforeseen tradeoffs.

Protecting Emails

Public emails, moving over fixed and wireless circuits, are insecure in both. Unencrypted emails are exposed to external monitoring, identity theft, relay to others, forgery, and modification of content -- both en route and while

stored on public servers. Even rights to privacy are in some doubt. In 2004, a US Appeals Court ruled that email service providers had the right to read or copy customer emails, although providers disclaimed any desire to do so.

It is wise, therefore, to tighten your email security:

- Because emails can be so easily intercepted and proliferated, edit them before sending to eliminate unwise content and sensitive data, an easy step.

- Next, call your ISP to check if its email system uses "Secure Socket Layer" (SSL) technology, which will ensure your computer is talking to the right server, and help secure traffic to and from it. If not, change your ISP to one that does use SSL.

- A Public Key Encryption system can take care of remaining risks. Of the two types, "PGP" technology* is more widely used, costing $50-$150/year. A 56-bit system will bar casual hackers. A 128-bit system will provide "strong" security. Examples of the vendors are at www.PGP.com* and www.VeriSign.com,* and other sites. Free programs are also available, but more complex to install. If you are not technically inclined, a vendor can help you set up the program.

- For 128-bit encryption, you need a Web browser from the year 2000 or later to crunch the data. Upgrade at www.fortify.net,* or get a free new browser at www.mozilla.org,* or other sites.

- The last step is a digital certificate, a computer ID card. You can get a free one at www.Thawte.com,* if your encryption does not include it.

The bottom line is that email confidentiality requires encryption -- and it costs to get it. The real issue is how much do you need it? Before you buy you may thus want to read a Web primer such as "Pretty Good Privacy"* and check what a DoD partner has to say about home computer security at www.cert.org/homeusers/HomeComputerSecurity/.

Emailing from Internet Cafes and Public Kiosks

Public computers pose greater risk because many will not allow you to close a browser when logging off, enabling a later user to see your login credentials, call up your sites, and continue your session. Such machines can also carry hidden programs to retain deleted messages, cached items, and record keystrokes -- especially overseas.

Employees on travel should thus avoid emailing from Internet cafes and kiosks if they can. If not, a few steps can reduce -- but will not eliminate -- risks at a public facility:

- Consider login credentials as compromised immediately at a public computer, and contact your ISP after messaging to change password and account data.
- Do not try to access official Web-based DoD email from any public facility.
- If you can, empty the computer trash bin, clear the Web browser cache, and reboot the machine, to try to clean out your login credentials and materials.
- Use SSL encryption from MS Outlook Web Access* or other vendors to help protect message content – SSL, though, will not protect login credentials.

Personal Websites, Web-Logs, and Instant Messaging

To meet Operations Security (OPSEC), Privacy Act, and other needs, DoD policy restricts what information you can release in unprotected media about DoD, to include information on other DoD individuals, but it leaves to you what to release about yourself and your family.

That can be a crucial decision if you post letters, resumes, or imagery on a personal Website -- and are of interest to stalkers or other criminals. Those sites can serve as target folders for attack or exploitation, and have been in the past. For security as well as privacy, you should remove such material from the Internet, find other means of distributing it, and close personal Websites.

Likewise, avoid Web-log, Instant Messenger (IM) and chat-board messages, all easily found and copied, allowing your views to be compiled over time -- Web-log "blogging" in particular opens you to major privacy and security risks.

Children should be especially aware that search engines can lock on IM and chat-board traffic to map a network of all those being messaged, exposing them to identification. They should report to you any threats in such traffic. Written threats are never a joke, even if so intended.

Finally, since Internet aliases are easily cracked, message partners may well know who you are, but you not know who they are, a very insecure situation. Advise and caution members of your family on such risks.

Home Telephone Security

Because public phone systems were designed for efficiency, not security, they are also highly vulnerable. All the old methods for bugging landlines are effective, newer methods do not require on-site devices, and equipment for both is readily available. You should thus be cautious about what you say over any unsecured line, especially if you have senior responsibilities.

There are several measures that you can take to reduce telephone risks:

- Think about what you say before you talk – that simple act can help you compose a conversation to avoid exposing sensitive data.

- Report to your local police for security review, and to your local phone company for technical review, any abnormalities such as:

    - A regular pattern of noises when calls go through, or in TV, radio, or home computer operations, when phones are "on."

    - A regular pattern of repeated wrong numbers/ nuisance calls. They may be efforts to determine who is at home, and when.

    - A pattern of anonymous calls or any calls with threats -- the latter may in fact qualify as crimes of assault, depending on the details.

- If you have children/baby-sitters who might reveal key data while you are away, give them a script at the phone to take caller name and number, say that you will call back, and politely but firmly hang up.

- Screen incoming calls with an answering machine. Put the recording in a friend's voice with only the number (no names or ranks), delete unwanted calls, and train your family to do likewise.

- Consider avoiding home use of the increasingly popular Voice Over Internet Protocol (VOIP) until industry standards/protection profiles have been strengthened for this mode of communication. At present, VOIP reveals both your telephone number and your Internet address.

- For about $5/month get an unlisted number, which will provide no more technical security, but will complicate efforts to focus on you.

- For personal privacy and safety, you can also join the national "Do-Not-Call" list to limit cold-calling and faxing to your home. Again, don't call or use the Internet, because there are fake sites, but write:

  The Direct Marketing Association
  Telephone Preference Service
  P.O. Box 282
  Carmel, NY 10512

Cell Phone Security

Traditional belt-worn pagers are only receivers, but cell phones are receiver-transmitters. The threats to cell phones are therefore like those on pp. 53-54 for wireless computing, because cell phones are also mini-computers and mini-broadcasting stations. Many can likewise be geo-located, penetrated for reading/downloading of files, activated remotely for covert bugging or viewing, and so forth.

Because customers are much more interested in convenience than security, amateurs can now easily monitor unencrypted analog cordless or cell phone calls. Digital cell phone calls, though, are encoded, use authentication, and are still difficult to crack, even if at growing risk as hackers focus on them.

A special hazard is that when they transmit, cell phones can be "cloned," i.e., have their ID numbers stolen for drug trafficking or other illegal ends. In addition to the wireless security options on page 54, consider several others.

- Try not to use a cell phone on interstate highways, airport access roads, or in airport parking lots, where police report that cloning is much more prevalent. Out-of-state cell phones are at particular risk.

- Review monthly cell phone bills and report erroneous calls to the service provider fast to limit cloning. Newer digital phones are more difficult to clone than analog models.

- When not using a cell phone, keep it turned "off," preferably with batteries removed. Tell callers that you will receive only voice messages -- then you make the live calls.

- Because a cell phone is so prone to loss/theft, do not store sensitive contact numbers/data on it, and call your service provider if you do lose it.

- Pay attention to cell phone news, where new features are emerging much more rapidly than security is advancing. As cell phones already reflect major voice, video, Wi-Fi, and other vulnerabilities, the security of likely new features is questionable. It would be wise to study the security of credit card swipe, mobile banking/ticketing, keyless entry, removable memory, internal hard drives, sender-to-receiver video, TV, and other likely innovations -- before purchase.

- Be aware that foreign digital cell systems use different technologies than those in the US, have less encryption, have been criticized for vulnerability to eavesdropping, and in some cases are infected. If you use rented cell phones abroad, raise your defenses accordingly.

From a technical perspective, encryption for analog cell phones is available but complex and costly. Again, do research or engage technical help before buying, as the Federal Communications Commission (FCC) bars some of the options advertised on the Internet, some commercial service providers cannot move the encrypted traffic, and technologies are changing fast.