and internal reorganization. USDA meat inspector William Lehman faced repeated attempts to transfer him from his lonely border inspection station in Sweetgrass, Montana, where he exposed and sent back millions of pounds of contaminated meat yearly that foreign producers have attempted to export to U.S. consumers. In 1997 Lehman retired rather than choose between transfer and termination. Managers at the Diablo Canyon nuclear plant also used transfers to enforce ignorance. Charles Stokes was the engineer who blew the whistle on falsification of results in the plant's seismic design review. When he and other dissenters were transferred away, the company brought in replacements who were both unfamiliar with the job history—and savvy enough to realize that they should not ask questions about unrealistic assumptions behind key calculations.

"Suffering through whistleblower retaliation teaches you a lot about your own strengths and weaknesses, about what really matters in life, about who your friends are, and about what human beings are capable of doing to each other in even the most civilized of settings. It is a life-altering experience."
—Justice Department whistleblower

On occasion, employers isolate whistleblowers from the evidence through a longstanding labor-management technique: lock them out. The National Institutes of Health took this approach with Walter Stewart and Ned Feder, popularly known as the "fraudbusters" because of their persistence in acting on concerns raised by those challenging fraud in scientific research. In their official capacity at NIH, they became a magnet for scientific whistleblowers and eventually compiled evidence on some 100 cases involving alleged fraud in taxpayer-supported medical research on issues such as AIDS, cancer, and Alzheimer's Disease. After shutting down their laboratory on a pretext, NIH imposed a gag on the two scientists, literally locked them out of their lab, and stationed a guard at the door. In 1995 NIH moved the records for these cases of alleged fraud to a warehouse, also under lock and key, where they continue to gather dust. In their new positions, Stewart and Feder were banned from continuing the watchdog duties that previously had official approval.

Depriving scientists of access to their own research is a common tactic for enforcing ignorance in that profession. When Dr. Mary Ann Marrazzi developed a bulimia and anorexia nervosa treatment that was more effective in 18 of 19 patients than standard treatment, a senior scientist who lacked subject matter expertise took over a branch of her research, damaging Dr. Marrazzi's credibility. When Dr. Marrazzi challenged the move, she was denied access to her laboratory and records by her university employer. The study, meanwhile, stalled.

Similarly, revoking an employee's security clearance is both a tactic of retaliation and a technique for imposing ignorance on some three million workers whose jobs depend on clearances for access to information. In addition to being forced to undergo a psychiatric examination, Department of Energy scientist Marlene Flor had her security clearance suspended to neutralize her whistleblowing. Without her clearance she no longer had access to evidence needed to prove her charges.

Prevent the development of a written record

When a policy is indefensible, the goal is to restrict debate to an oral dialogue. This can be enforced through peer pressure, overscheduling to ensure that there is not time to construct a written record, or even a gag order if necessary. Managers recognize that it is difficult to be accused of revising an oral history, and verbal agreements diffuse accountability in the event of a serious problem.

Along with other tactics, this technique was used in the Diablo Canyon case. In 1985 the NRC's internal affairs unit, the Office of Inspector and Auditor (OIA), reexamined the peer review process that had overruled NRC engineer Isa Yin and Diablo Canyon whistleblowers about key design questions on which the plant's license was legally conditioned. Thorough documentation

and an adequate record had not been compiled, however. In its report OIA concluded that due to a lack of available supporting information, it was "unable to assess the validity of [peer review] conclusions" on key issues. More generally, OIA reported that it "did not find sufficient documentation to demonstrate that [the NRC staff] had verified the quality of the design control program, either in a direct inspection or in licensing review." In other words, the safety of the plant was (and remains) unknown.

Rewrite the issues

One of the more subtle bureaucratic gambits is to trivialize, grossly exaggerate or otherwise distort the whistleblower's allegations—and then discredit the employee by rejecting the validity of the resulting "red herring." The government's Office of the Special Counsel and Offices of Inspector General have fine-tuned this technique. In some cases, those investigative bodies will exaggerate charges until they are no longer credible. A whistleblower charging that his or her superiors overlooked problems on the job, for example, will find his or her claims exaggerated into allegations of willful misconduct. The government then finds that, although mistakes were made, the employer committed no intentional violations. The charges are dismissed, the whistleblower is discredited and the targets of the investigation promptly issue public statements that they are pleased to be exonerated.

Rewriting the record can degenerate into outright censorship. This may involve deleting evidence and/or issues that are too hot to handle—and therefore simply vanish from the ensuing report of investigation. In other cases, the findings are "massaged" through edits that ensure that they will not be interpreted as significant.

An investigative report—even one diluted by rewritten allegations, censorship and neutered recommendations—can still be damaging to wrongdoers. As a result, a related bureaucratic technique is to issue a press release declaring that the investigation had concluded that there was no wrongdoing—but then refuse to release the report containing the record of the investigation. The

Office of Research Integrity at the Department of Health and Human Services, for example, has a formal policy of not releasing reports on its investigative targets when it finds no wrongdoing, unless the subject of the investigation consents.

Study it to death

A related tactic is to launch an investigation that never ends, leaving the allegations of wrongdoing unresolved. Since 1988, now-retired Nuclear Regulatory Commission whistleblower Larry King has been attempting to ensure corrective action on nuclear safety violations that he argues could literally blow the containment lid off a nuclear plant in the event of an accident. Although his agency agreed the rules were broken, it first ordered multi-year engineering reviews to see if the engineering standards could be safely changed after the fact. After concluding that the rules were valid, the Commission asked for the utility-owner's side of the story. The utility's lawyers have been arguing the point for years, a profitable debate they would like to continue indefinitely—and one that is also less expensive for the plant owner than actually fixing the problems.

Scapegoat the small fry

Just as bureaucracies may trivialize allegations of wrongdoing by rewriting them, they may lower the scandal volume by shielding agency leadership from accountability. The reports of the Office of Research Integrity (ORI) at Health and Human Services, for example, rarely claim credit for successful scientific fraud prosecutions against department heads or laboratory chiefs at universities and biomedical research facilities. The ORI more frequently targets graduate students, laboratory technicians and an occasional assistant professor—those who do not have a support constituency or who were only following orders from higher-ups.

In 1983 the Office of Special Counsel (OSC) learned of multi-million dollar procurement misspending. Evidence raised questions about whether the Secretary of Defense participated in or

knew of alleged retaliation against the whistleblower, an auditor who had uncovered the scam. The OSC chose to prosecute a mid-level official and keep the cabinet official out of the case. In the end, the mid-level official escaped accountability after a court ruled that he had been following orders, not making reprisal decisions.

CHAPTER THREE

Where and How to Blow the Whistle

Once you have weighed the risks and rewards and decided to blow the whistle, you are faced with another dilemma: Where should you take your story? To government officials? The media? What avenue is most likely to expose and correct the wrongdoing you have revealed? Which is best able to protect your interests and concerns?

Whistleblowing outlets range from agency hotlines to independent oversight offices to Congress to non-profit organizations. These outlets are not equal. Some provide greater confidentiality than others. Some are well-positioned to expose wrongdoing; others tend to discourage dissent. Still others are known for taking action against whistleblowers. You should be aware of the advantages and disadvantages of each alternative before you choose. We will explain how each whistleblowing outlet is supposed to work and then describe, through past examples, how it actually functions.

Because every whistleblowing situation is unique, it is important to study each outlet to determine your best option. On balance, GAP's experience suggests that non-profit groups, the media, and false claims suits are the most effective channels for

exposing and addressing wrongdoing, given the current state of the federal bureaucracy and today's political climate. Bear in mind that even if you launch your challenge through nongovernmental avenues, it is generally necessary to find some sponsor from within a formal government institution. For example, a False Claims Act lawsuit can become too expensive for a whistleblower to pursue if the Justice Department does not adopt the case. Similarly, a congressional ally can be an invaluable partner for a whistleblower seeking to expose misconduct through the media or a non-profit group.

Perhaps most significant is knowing where *not* to blow the whistle. Trusting the wrong audience can seal your professional fate, trigger a cover-up of the wrongdoing you seek to expose—or both. The list of whistleblowing outlets below starts with institutions that often have proven to be a threat rather than a resource for whistleblowers.

OFFICIAL CHANNELS

Federal Hotlines

In 1979, the Secretary of Defense established the Department of Defense hotline as an avenue for the Inspector General's office to learn of potential wrongdoing or mismanagement. Today nearly all federal agencies and departments have hotlines, and the Army, Navy and Air Force each have an individual hotline. In an effort to institutionalize the process of reporting misconduct, the President's Council on Integrity and Efficiency (PCIE) recommended standards for receiving, controlling and screening allegations for each federal agency. These standards direct that:

- a simple, well-publicized system be developed for agency employees and other interested persons to submit allegations of fraud, waste, abuse and mismanagement while preserving anonymity when possible and if desired;

- a retrievable record be maintained of each allegation received;

- each allegation be screened as soon as possible, based upon the nature, content, and credibility of the complaint, and an appropriate decision be made—based in part on existing resources and priorities—on whether to refer the complaint for further inquiry on each allegation; and

- the rationale for the decision on each allegation be documented in the record.

With these standards as guidelines, hotlines are supposed to operate according to a common procedure. An employee can call the toll-free hotline and report an allegation of fraud, waste or mismanagement. The allegation is reviewed to determine if follow-up is necessary. If it deserves further review, it is sent to an investigator who researches the allegation in the field. If the investigation verifies the charge, corrective action is taken and the case is closed.

In theory, the process sounds straightforward and simple. In practice, it is anything but clear-cut; there are far too many gray areas and breakdowns in federal hotline investigations. The essential measure of the effectiveness of hotlines as a whistleblowing mechanism is their track record in producing results. It is abysmal. Even the best hotlines, such as those run by the General Accounting Office or the Department of Defense, investigate less than 20 percent or fewer cases within a year of the complaint, and substantiate or purport to take any corrective action on less than 10 percent. Hotlines provide an opportunity to make sure the system has received a warning about wrongdoing. But for those whistleblowers who seek to make a difference while avoiding retaliation, hotlines are in most cases worthless at best.

One important reason for the shortcomings and breakdowns in hotline systems is structural: investigations into alleged misconduct are compromised, intentionally or unintentionally, by conflicts of interest when an institution investigates itself. The problems are numerous.

Standardization of hotline procedures has not been achieved. In a report by the President's Council on Integrity and Efficiency

(PCIE), DOD received top billing as the best-run hotline, but the PCIE found faults even with DOD's system, and admitted that many of the others do not meet operational standards. In an effort to improve and encourage the uniform handling of hotline calls, the PCIE set up training courses available to federal, military and private industry hotline operators.

Two areas of concern addressed in the PCIE training courses are confidentiality and case follow-up. Confidentiality issues are inherent in the hotline system. Anonymity is a presumed goal of any employee choosing to blow the whistle through a hotline. But how does a whistleblower provide sufficient information to support his or her allegations without giving away details that identify him or her within the agency? The balance is hard to strike, often leading to one of two problems: the information received is either too vague to produce an investigation, or is traced back to the only person who could possess that information.

At some hotlines, the principle of confidentiality is treated with outright disdain. In one case, a whistleblowing scientist at a U.S. nuclear facility was terminated after he contacted the Inspector General hotline with evidence of wrongdoing. The Inspector General there had sent his "confidential" information straight to the whistleblower's supervisor.

A spokesperson for the DOD Inspector General hotline (who asked not to be identified) believes many military hotline operators are more interested in discovering who the caller is than in determining whether the allegation is true. In an atmosphere in which discipline, conformity, and unquestioning obedience to orders are prized above all else, it should come as no surprise that a whistleblower could be regarded as a traitor.

Randy Taylor, the Chief of Military Police at the Naval Air Station Bermuda, made his first mistake in challenging sexual coercion and massive spending abuses at the base by contacting the Navy Waste, Fraud and Abuse Hotline with another officer, Tom Coggins. Although the hotline is supposedly confidential, word quickly got back to his superiors, and he began to receive veiled threats of retaliation.

Or take the case of John Kartak. After 19 years in the Army, he was assigned to a recruiting station in Minneapolis. There he found that unqualified applicants were recruited to meet quotas. High school diplomas were forged and criminal records were concealed to permit the enlistment of marginal recruits. Kartak refused to cooperate in this misconduct, and called the Army hotline to blow the whistle. Kartak's "reward" was repeated harassment. His supervisors ordered him to submit to two psychological evaluations and eventually to involuntary commitment. One of his superiors told the Department of Veterans Affairs hospital, "He has lodged numerous complaints recently. . . . I find his behavior highly unstable. I am concerned that he may do something to harm himself or others." Kartak was also ostracized, threatened, and intimidated by his co-workers.

"Hotlines that supposedly guarantee anonymity can turn out to be direct channels to the reprisors themselves. If you're going to blow the whistle, figure out how to get an investigation of the wrongdoers without becoming the one investigated."
—Justice Department whistleblower

Kartak was vindicated when at least 58 people in the Minnesota recruiting office were found guilty of illegal acts ranging from forgery to drug-dealing. But the price of Kartak's vindication was high—and the abuse of the hotline system's confidentiality was evident.

Case follow-up is another area the President's Council on Integrity and Efficiency emphasizes in its training courses. The PCIE would like all agencies to adopt the procedure used by the DOD and General Accounting Office (GAO) hotlines. Those hotlines assign all callers case numbers so that they can call back later to find out what action was taken on their allegations. This system maintains the anonymity of the whistleblower while permitting him or her to follow up. The details of the case are not disclosed to the caller, but s/he is told whether the case was closed and whether the allegation was substantiated.

For a full report of a closed case the whistleblower must file a request under the Freedom of Information Act (FOIA). The problem is that this process can jeopardize his or her anonymity: in order to file a FOIA request, the whistleblower must identify him or herself. The requestor's name will be sent to the Inspector General investigating the report and can make its way back to the very people responsible for the wrongdoing. This kind of "Catch-22" can lead to serious reprisals.

Nancy Kusen discovered how the FOIA "Catch-22" works. Kusen was a contract administrator for the Defense Contract Administration Service (DCAS) who raised concerns about overcharging and alleged shoddy work by a Navy contractor. She complained first to her superiors, and when no action followed, she called the DOD hotline. The call led to an investigation by the Defense Criminal Investigative Service, which substantiated many of the complaints but found no criminality. At the same time, Kusen became the target of reprisals ranging from lowered performance evaluations to denials of promotion and repeated harassment.

Kusen filed a FOIA request to learn the status of her case. Records show that her request was referred to the Defense Contract Audit Agency (DCAA), which, in turn, asked the contractor's parent company if it objected to the release of the audits. The DCAA included a copy of Kusen's FOIA request containing her name, address and home phone number. According to the DCAA it is "routine practice" to include the FOIA request.

The FOIA request that disclosed Kusen's name to the contractor's parent company provided positive identification that she was the whistleblower, enabling them to single her out for harassment. In Kusen's case, the harassment had begun shortly after her initial call to the DOD hotline, convincing her that the hotline revealed her identity to DCAA and triggered the chain of disclosure. Her experience with the FOIA request serves as a warning to other whistleblowers.

Kusen's case contributed to the caveat now offered by the Inspector General's office to FOIA requestors: "Your confidential

status as a hotline caller does not apply to requests under the Freedom of Information Act." Without filing a FOIA request, however, you cannot determine whether the government investigated your charges in a thorough manner. Whistleblowers can try to avoid this structural "Catch 22" by having a trustworthy third party, such as a non-profit group or reporter, make the FOIA request.

Other problems with hotlines were noted in a General Accounting Office report on the DOD hotline. The DOD has taken some steps to address these concerns. It is likely, however, that these problems plague many hotlines. According to the GAO, four problems pose recurring concerns: 1) investigator objectivity, 2) insufficient documentation on case files, 3) incomplete investigative reports that do not comply with DOD reporting requirements, and 4) limited action on planned follow-up to solve identified problems.

In an effort to correct the problems identified in the GAO report, the DOD has started a Quality Assurance Review. The review checks the files of DOD field investigations to ensure that the summary report matches the investigative report. DOD also claims that it is more carefully reviewing cases it refers to its own agencies, the military services. This is important, because whether it is done advertently or inadvertently, the hotline system can pass information back to the relevant agency—which can send it right back to the program manager who may be involved in the fraudulent or wasteful activity. This can lead not only to reprisals against the whistleblower, but to a cover-up of the wrongdoing. In other words, the system structurally is vulnerable to serving as an early warning device for those with a motive to conceal the alleged misconduct.

The record on government hotlines speaks for itself. The odds of reporting fraud, waste, or mismanagement to a hotline and ensuring that it is investigated and corrected are small. Hotlines may be a vehicle for those who seek a clear conscience for putting the system on notice of significant wrongdoing. They are not a safe, reliable channel for whistleblowers who want to make a difference.

Corporate Voluntary Disclosure Programs

Corporate voluntary disclosure programs are the private-sector equivalent of government hotlines. These programs operate as part of corporations' internal systems of oversight and enforcement, often through in-house "ethics" offices for disclosures by company employees.

Corporate voluntary disclosure programs became popular during the 1970s as a way for the Securities and Exchange Commission to address illegal, shareholder-financed political contributions or bribes at home and abroad. In the 1980s they became common as an alternative to direct government investigations of whistleblower charges in the nuclear power and defense industries. They are a major element of corporate compliance programs, which are reviewed as part of the sentencing guidelines for legal violations by corporations. These voluntary disclosure mechanisms permit companies to act on their duty to identify, disclose and correct violations of institutional responsibilities. But they have proven no more reliable than the good faith a corporation brings to the process.

Structurally, corporate voluntary disclosure programs are vulnerable to the now-familiar conflict of interest inherent when an institution is responsible for disclosing its own misconduct. To illustrate, the investigations often are conducted by attorneys whose professional duty is to the client corporation—rather than to the public. The same attorney who interviews whistleblowers and serves as a liaison between the corporation and the government during a voluntary disclosure may later act as counsel for the defense in the event of enforcement action.

As a result, voluntary disclosure programs have failed to serve as an effective substitute for external oversight, and too often serve as a shield for liability. Summarized below are lessons learned from a review of "whistleblower" cases from corporate hotlines and voluntary disclosure programs since 1979. Programs have been:

- incomplete in scope because institutions set the boundaries for investigations, which at times have been limited to exploring the "tip" of the misconduct and screening out the "iceberg."

- incomplete in findings of fact after the investigation, because companies have elected not to disclose the most significant instances of fraud or abuse.

- inadequate substitutes for government fact-finding, because regulatory agencies have abdicated all but a monitoring role, and are further limited to the boundaries for relevance defined by the firms.

- inadequate even for government oversight, because firms can and do rely on program procedures and the attorney-client privilege to withhold key records in corporate investigative files from government auditors.

- vehicles to delay formal proceedings while a company's self-investigation proceeds—taking 2.8 years on average and over ten years in many of the cases surveyed, according to a 1996 General Accounting Office study. This delay also creates a window of vulnerability for evidence uncovered by potential defendants in the interim that might later be threatening if included in a public record for law enforcement proceedings.

- vehicles for advance discovery for any future litigation, which at worst creates opportunities to intimidate or influence witness testimony, and at best provides early knowledge of—and a corresponding opportunity to rebut—significant, threatening testimony.

- vehicles to lock in secrecy of corporate wrongdoing: unlike the 1970s Securities and Exchange Commission program, investigative files are not available for public scrutiny after the fact under the Freedom of Information Act—or even, as in the case of mismanagement on the Alyeska oil pipeline, disclosable in the legal discovery process. The trend in some state legislatures of passing "environmental audit privilege" laws

is a way of institutionalizing corporate barriers against the public's right to know.

- vehicles to divert the government from more direct investigation of cases in which it has not waived its normal enforcement authority and access to evidence, because oversight of voluntary disclosures has been institutionalized as the highest priority at Offices of Inspectors General.

- openly advocated in industry speeches as a way to avoid harsher government enforcement action (attractive only if a firm fears it will be caught anyway)—despite official disclaimers that the program's purpose is good corporate citizenship.

In short, these programs can be useful structures for a company that wants to do the right thing. But for those that don't, they offer an easy way to cover up misconduct. They are no substitute for independent accountability.

Incentive-Suggestion and Other Cash Awards Programs

After embarrassing disclosures of spare-parts costs several years ago, the DOD and its armed services claimed to be serious about establishing suggestion programs to save money. They began to reward individuals for suggesting ways to reduce spare-parts overpricing. The Navy reports that such calls to its pricing hotline have saved millions of dollars. These claims of success, however, should be placed in perspective: the Navy annually spends *billions* on spare parts.

The Service Suggestion Programs generally follow a simple structure. Personnel may submit a suggestion in writing to the Price Monitor/Installation Resource Management Office at the base. After preliminary review, the suggestion is sent out for investigation. If the suggestion is adopted, the caller receives a percentage of the savings ranging from $5-25,000. Any award of $25,000 must be approved by the President.

The design of the programs eliminates anonymity, which means the caller may be subjected to harassment from superiors who prefer the status quo. Again, the problem is systemic. Official policies and regulations guiding the procurement of such parts often are designed to maximize spending. The reason is political: agency higher-ups must make sure that the budget is spent every year in order to justify more money the following year for the bureaucracy.

Airman Thom Jonsson found out the hard way that the Air Force preferred the status quo to his suggestions for saving money. Jonsson was working for the maintenance and supply section of the C-5A cargo planes at Travis Air Force Base in California. In the course of his duties he discovered that many spare parts were purchased at extraordinary prices, including the now infamous $7622 coffee brewer. Another example was a $670 armrest pad, which Jonsson determined could be manufactured on base for $25 with no rearrangement of machinery or personnel.

In January 1984, Jonsson submitted his money-saving proposal to his base's Zero Overpricing Program representative. In April, Jonsson received notice that his proposal was "not in the best interest of the Air Force." He resubmitted his suggestion and waited for a response. By August 1985 he had heard nothing and decided to contact the Project on Military Procurement (now the Project on Government Oversight, or POGO), a non-profit watchdog agency. After POGO staff evaluated his claims and discussed Jonsson's goals with him, his allegations were brought to Senator Charles Grassley (R-IA), chair of the Senate Judiciary Subcommittee on Administrative Practices and Procedures. The subcommittee asked Jonsson to come to Washington and testify at hearings. Jonsson went to the Capitol on his own time and testified in civilian attire about the excesses he had witnessed on the C-5A spare parts. The hearings generated substantial publicity, which helped discourage retaliation from the Air Force. Eventually, Jonsson was granted a cash award for his suggestion.

A year later Senator Grassley asked Jonsson if the prices of the spare parts, including the armrest, had gone down. Jonsson reported that they had barely changed. When a press conference was scheduled to expose this information, the Air Force began to

harass Jonsson. He was denied routine leave, assigned a "babysitter" to make sure that he "didn't get into trouble" and subjected to an attempted arrest on the ironic charge of illegal destruction and disposal of spare parts. Several members of Congress protested loudly, with Senator Grassley, Representative John Dingell (D-MI) and then-Representative Barbara Boxer (D-CA) stepping in to protect Jonsson from harassment. His case serves as an important warning of the risks posed by incentive-suggestion programs to would-be whistleblowers, most of whom cannot expect a squadron of legislators to defend them.

The DOD Inspector General Cash Award program is different from the incentive-suggestion programs in several ways. Rather than systematically providing cash awards to anyone who suggests a viable way to reduce costs, the Inspector General Cash Award program is designed to give rewards to selected individuals who draw recognition because their disclosures save money. The weaknesses of the program are similar to others described here, however, and the program is by no means risk-free.

One would like to think that after you had been publicly recognized and honored for saving the government money, your superiors would not have the motivation or the nerve to harass you. But after your moment of glory has faded and you revert back to your regular employee status, you may be left facing the very officials you accused of wrongdoing. Indeed, your vindication may make it harder for them to forgive and forget.

More striking than the program's potential abuse, however, is its record of irrelevance. In the program's first six years, 38 people received $46,000 in cash awards for saving over $36 million. To put these results in perspective, keep in mind that during the same time period (fiscal 1984-1990), overall Pentagon spending levels approached two trillion dollars.

Inspectors General

The primary conventional channel for investigation of employee concerns is the Office of Inspector General (IG). Each agency has one, either by that name or another. These offices are

responsible for investigating and reporting on alleged misconduct by the agency or its employees. The IGs at most major agencies—a total of 62 as of mid-1995—are covered by the Inspector General Act of 1978 and subsequent amendments.

Employees who are considering disclosures to an IG should first determine whether their agency's Inspector General is statutory or non-statutory. Structurally, the distinction is quite significant. Statutory IGs can be nominated and dismissed only by the President. Non-statutory IGs are hired and fired by the agency chief—whose programs they are investigating. Agency heads can comment on but not change the text of reports submitted by statutory IGs. By contrast, agency chiefs have editorial censorship rights over reports by non-statutory IGs. Statutory IGs have the authority to investigate agency reprisals against their witnesses. Non-statutory IGs can investigate only what the agency chief permits.

For potential whistleblowers, the implications are clear: the risk of retaliation is far greater if your agency has a nonstatutory IG. Consider the work of the Department of Justice's Office of Professional Responsibility, which for years served as the non-statutory equivalent of an IG (a vacuum which has since been filled). Up to ten percent of the office's referrals each year were to investigate and identify for possible criminal prosecution the source of "leaks"—usually anonymous whistleblowing disclosures.

Whistleblowers should also keep in mind that Offices of Inspector General are in many cases mini-bureaucracies, and can be vehicles for the full range of bureaucratic waste, fraud and abuse. The Department of Labor Office of Inspector General, for example, has over 500 employees and a budget of more than $70 million. The office has been mired in controversy over cover-ups, whistleblower reprisals, and questionable travel expenditures. Similarly, Congress and the press have found evidence of repeated wasteful spending by the Inspector General for the Environmental Protection Agency.

Most importantly, IGs at best have a mixed track record of responding to whistleblowers. Even offices with statutory inde-

pendence may be led predominantly by employees grounded in the "old school" traditions, from a time in which the Inspector General served as management's eyes and ears. That meant that when the agency chief wanted to get the facts and act against wrongdoing, the IG performed as a law enforcement agency. But when the agency leader wanted to cover up a problem, the IG performed a damage-control operation, issuing a report that assembled the case for the defense.

That tradition continues, and structural incentives sustain it. Even statutory IGs receive their performance appraisals and merit bonuses from the department chiefs whose operations they are charged with keeping honest. Whistleblowers from the EPA's IG repeatedly have exposed their office as a damage-control operation that shredded evidence of misconduct involving government contracts. NASA's Inspector General retired under fire; he was under investigation for allegedly leaking evidence to targets of an open investigation, including NASA personnel. NASA's Administrator arranged for the Inspector General to keep his $120,000 annual salary during the next year, while he served as a management consultant to a local community college. The GAO later found that the Inspector General's actions "constitute a failure to exercise due professional care and could be viewed as an impairment of his office's execution of investigations."

"If you go to the Inspector General, expect your boss to know about it by the time you get back to work."
—Environmental Protection Agency whistleblower

An IG's genuine independence from the agency it oversees is necessary but not sufficient to ensure accountability. No satisfactory answer yet exists to the question, who watches the watchdog? The potential for conflicts of interest is great. And the conflicts can get personal: a 1992 Senate Government Affairs Committee report found that the National Archives and Records Administration (NARA) IG failed to recuse himself from investigations involving his own alleged misconduct in his prior job as a

NARA procurement official. After reviewing the IG's overall record, the committee found that "[h]is conduct raises questions about his own compliance with agency standards of conduct and code of ethics which an Inspector General is required to oversee as the 'agency watchdog.'"

A 1993 GAO report pointed out repeated instances of statutory IGs routinely returning cases for investigation to the agency charged with alleged misconduct. A July 1990 review by the staff of the Senate Governmental Affairs Subcommittee on General Services, Federalism and the District of Columbia found a pattern of IG wrongdoing that included: 1) IGs personally implicated in corrupt acts; 2) wrongful disclosure of confidential identities and sharing of confidential information with agency personnel; 3) improper destruction of evidence; 4) initiation of phony investigations of whistleblowers and intimidation of witnesses; 5) whitewashing of final reports by distorting or ignoring both fact and law; 6) improperly-conducted investigations through failure to follow up on relevant evidence and witnesses, or to question witnesses in confidence; and 7) refusal to investigate strong cases.

The most serious misconduct occurs when an IG wittingly or unwittingly serves as a hatchetman against whistleblowers. In GAP's experience, it has not been uncommon for an IG's office to implement one of the prime tactics of retaliation—directing the spotlight at the whistleblower rather than at his or her allegations of wrongdoing. In a disturbing number of government agencies, IGs have a history of failing to pursue the evidence of misconduct gathered by whistleblowers and instead searching for information to discredit and retaliate against them. In fact, GAP has represented whistleblowers from Offices of Inspectors General who suffered retaliation for refusing to participate in hatchet-jobs or cover-ups.

Gordon Hamel, who blew the whistle on misconduct at the President's Commission on Executive Exchange, learned the retaliatory power of IGs the hard way. After an Office of Personnel Management (OPM) probe confirmed the substance of Hamel's allegations, the OPM's IG opened a case and eventually wrote a

report that rebutted the allegations—and provided grounds to fire Hamel. The OPM Inspector General and an IG investigator stated in sworn congressional testimony that they were unaware of the agency's attempts to terminate him. Four months earlier, however, that very investigator had authored a memo—received by the IG—indicating that the White House was waiting to fire Hamel "at the earliest possible time after our report is issued."

Many IGs have long histories of targeting whistleblowers. The Department of Energy Office of Inspector General is a case in point. Repeatedly, those who make disclosures of wrongdoing to the DOE IG's office have found themselves on the receiving end of an investigation. Often the whistleblower's confidentiality is breached by the DOE IG, resulting in the employee's termination.

At the Hanford Nuclear Reservation, the DOE IG was assigned to investigate whistleblower Ed Bricker's allegations of harassment for his numerous public disclosures of safety and health violations. Instead of investigating Bricker's claims, the DOE IG teamed up with Bricker's employer, the Westinghouse Hanford Company, to make Bricker himself the target of the investigation. GAP attorneys uncovered memoranda to the file indicating an agreement between Westinghouse and the DOE IG—made well before the investigation had started—that they would not find any merit to Bricker's claims. Furthermore, it was later revealed that the DOE IG attempted to persuade a personal friend of Bricker's to wear a hidden-body microphone in an attempt to gain incriminating information on Bricker. Plans to proceed with the wiring were eventually put to a stop by the U.S. Attorney's office.

The DOE IG's performance at Hanford was not an aberration. One of the more harrowing stories involves a whistleblower at the Knolls Atomic Power Laboratory, a DOE site in New York. There, the IG investigated allegations of wrongdoing in the operation of several nuclear reactors near populated areas. The IG agents took numerous statements from workers at the plant. The interview statements were allegedly altered, according to a confidential IG source, to remove any favorable or supportive evidence

of the whistleblower's allegations. These altered statements were then used to support a well-publicized finding against the whistleblower. When the whistleblower filed a Freedom of Information Act request for all of his files, the records were allegedly shredded to hide the fact of the illegal alterations. At the same plant, a health physicist contacted the DOE IG and was terminated immediately by his supervisor, who took him to task for daring to contact the IG. The IG did nothing to investigate or protect the scientist.

To some extent these traditions are changing. Further, it is unfair to generalize. Nearly every Office of Inspector General justifiably can take pride in winning numerous tough cases. The U.S. Department of Agriculture IG provides one example of an IG office that has produced promising, if mixed, results for whistleblowers. In 1994, the USDA's Office of Inspector General conducted a hard-hitting investigation into misconduct that ultimately forced the Secretary of Agriculture's resignation and sparked appointment of an independent counsel. The USDA IG also has conducted numerous audits exposing the inadequacy of the Forest Service's timber theft and law enforcement programs. Such positive developments, however, should not unduly raise whistleblowers' expectations. Even at USDA, the track record is spotty. Forest Service whistleblowers at USDA have complained of brush-offs from the IG's office, unless there is some powerful political or media constituency to make their concerns a priority. Even hard-hitting USDA IG reports often have a limited impact on agency operations: the Forest Service has a long-established pattern of paying lip service to IG recommendations but making no fundamental changes.

On balance, whistleblowers are well-advised to seek expert advice or retain an attorney—even if only for coaching purposes—before going to an Inspector General. You should clarify precisely how the IG will conduct the investigation before sharing your concerns and evidence. At least until there is a solid track record to establish trust, you should politely insist that all agreements, plans, and schedules be pinned down and confirmed in

writing—rather than agreeing to handle matters informally or relying on what appears to be a common understanding to guide the office's subsequent actions. Above all, you must be permitted to review your statements and any summary of your allegations to ensure their accuracy and completeness. Finally, as we discuss in the next section, under some circumstances it may be wise to approach the IG armed with the extra credibility of a "substantial likelihood" finding and order to investigate from the Office of Special Counsel.

Office of Special Counsel (OSC)

The Civil Service Reform Act of 1978 created a formal whistleblowing disclosure channel through the Office of Special Counsel. This responsibility exists independent of and parallel to a separate duty by that Office to defend federal employees against personnel practices that violate the merit system.

The Special Counsel has 15 days to screen whistleblowing disclosures from federal employees, applicants or former employees before deciding whether to order agency chiefs to investigate those challenges that have merit. The Special Counsel may refer for agency investigation any disclosure that reflects a "reasonable belief" of illegality, gross waste, gross mismanagement, abuse of authority or a substantial and specific danger to public health or safety. If the OSC judges that the disclosure satisfies only this minimum standard, then the agency chief can respond however s/he chooses.

If, however, the OSC determines there is a "substantial likelihood" that the whistleblower's charges are accurate, a more intensive reform process is triggered. The OSC must refer the charges, and the agency head has 60 days to investigate and reply. The Special Counsel can, and generally does, grant time extensions to this deadline. The agency must reply through issuing a report whose contents are specified by statute, including the issues and evidence that were investigated, the methodology for the probe, a summary of the evidence obtained, findings of fact and law, and a summary of corrective action to solve any

verified problems.

The whistleblower has a right to submit comments, after which the Special Counsel evaluates the report to determine whether it is complete and reasonable. Congress has instructed that the Special Counsel should not approve a report unless it has satisfied those criteria under a "clear and convincing evidence" standard. Then the report is sent to the President and Congress, along with the employee's comments. The Special Counsel must maintain a copy of each report and comments in a public file. Researchers, reporters, investigators and members of the public can review the resolution.

The purpose of the OSC whistleblowing disclosure channel is "to encourage employees to give the government the first crack at cleaning its own house before igniting the glare of publicity to force correction." Indeed, if administered in good faith, the Reform Act mechanism offers strategic benefits for a whistleblower to be effective in challenging misconduct. It offers an opportunity to gain the legally-binding judgment of an objective third party that the whistleblower's charges must be taken seriously. At a minimum, it promises to maximize the public whistleblower's credibility and help to reduce isolation. The OSC evaluation that there is a "substantial likelihood" the allegations are well founded is the bureaucratic equivalent of a "Good Housekeeping Seal of Approval" for that particular disclosure.

What is the Office of Special Counsel's track record for meeting its promise? At times, the combination of OSC support for a whistleblower's challenge and serious evaluations by the Special Counsel at the end of the process have helped to improve the quality of agency reports in response to whistleblowing disclosures. The Nuclear Regulatory Commission, the U.S. Department of Agriculture and the Department of Health and Human Services have confirmed the validity of employees' dissent in key cases, and have taken serious corrective action. On occasion the Special Counsel also has held agencies accountable for inadequate reports of self-investigations. In the case of Dr. Wilfredo Rosario, who challenged the USDA when it released beef carcasses—de-

spite evidence of tuberculosis—for human consumption, the Special Counsel twice flunked the agency report and sent USDA back for further investigation and disclosures.

Unfortunately, the Special Counsel seldom makes the approvals necessary to put an agency on the spot. In March 1995 congressional testimony, Special Counsel Kathleen Koch reported that the OSC made referrals for full or partial agency investigation only eight times out of 148 reviews of whistleblowing disclosures. The OSC's annual report for fiscal 1995 reveals that out of 333 whistleblowing disclosures, the office forwarded only two for agency investigation, one of which reflected a "substantial likelihood" finding.

"When I was first interviewed by OSC investigators, they were determinedly disinterested. I kept trying to give the investigators documentary evidence and they kept giving it back to me."
—Defense Department whistleblower

In addition, even full referrals generally produce only cosmetic reform. The OSC's seal of approval seldom overcomes the conflict of interest inherent when the agency targeted by the whistleblower is left to investigate itself. Good-faith agency responses have been the exception, rather than the rule. Further, the OSC typically accepts as reasonable and complete whatever report the agency produces. As a result, an OSC whistleblowing disclosure is often merely an opportunity for the agency to cover up the evidence, perfect its defenses and then issue an official self-exoneration to be approved by the Special Counsel—all before serious investigations by Congress, the media or other outside groups can be mobilized to ferret out the truth. This basic structural flaw is analogous to that of hotlines, but here the stakes are higher and the setbacks can be more severe.

Army scientist Aldric Saucier's case offers an illustration of the OSC's low standards. The OSC accepted as reasonable and complete a report by the Pentagon's Office of Inspector General that found no misconduct after investigating Saucier's charges

that the Star Wars missile defense system did not work as advertised and that the Pentagon was knowingly underestimating (by 19 times) the costs of the ballistic missile defense system's next phase. The report passed muster with the Special Counsel despite the fact that the Inspector General had: declined to investigate any misconduct except explicit illegality; rewritten the allegations; failed to summarize significant evidence; lost other significant evidence; failed to interview the primary witnesses for Saucier's dissent; rewritten statements from supporting witnesses who were interviewed, to weaken their support for Saucier; refused to seek evidence that Saucier identified as critical; failed to check the veracity of testimony by agency personnel despite evidence of false statements; and refused to pursue evidence of document destruction, including incidents involving evidence initially requested by the Inspector General.

On balance, these flaws in the system mean that an OSC whistleblowing disclosure is likely to be unproductive or even counterproductive—unless it is part of a larger strategy involving other institutions. As one part of a broader legal campaign, an OSC disclosure can be helpful. It has been in this context that OSC disclosures have been valuable elements of GAP whistleblower initiatives in food safety and other arenas. Ironically, a striking example again involved the Star Wars disclosure of Pentagon whistleblower Aldric Saucier. Despite the Inspector General's whitewash, Saucier's disclosure was significant in formally ending the Star Wars program, and decisive in eliminating one flawed component (called "Brilliant Pebbles") of the anti-ballistic missile defense system. The Pentagon and defense industry had intended Brilliant Pebbles to be the vehicle for sustaining tens of billions of dollars in pork-barrel spending well into the 21st century. What proved successful for Saucier's whistleblowing effort was the combination of extensive media coverage, congressional oversight, coordination with public interest groups, *and* an OSC "substantial likelihood" finding.

Before the Whistleblower Protection Act of 1989, the OSC channel was in many cases treacherous for whistleblowers. On

numerous occasions the Special Counsel ruled that a whistleblower's challenge was unfounded—but then sent the record of the complaint to the agency chief regardless, and without the employee's consent. These "informal referrals" meant a double whammy: they provided both advance warning of serious dissent to the agency and an invitation to retaliate with impunity, since the Special Counsel's ruling meant the dissent did not qualify as legally-protected speech.

The 1989 law made the OSC a safer channel for whistleblowing disclosures, by generally forbidding the Special Counsel from forwarding the employee's charges or revealing his or her identity. The OSC may not reveal the identity of a whistleblower "without such individual's consent unless the Special Counsel determines that the disclosure of the individual's identity is necessary because of an imminent danger to public health or safety or imminent violation of any criminal law." Because the OSC's failure to order a referral implies that your disclosure is not protected by the Whistleblower Protection Act, this safeguard can make a real difference in preventing reprisals. Should you pursue this channel, therefore, it is important that you wait to approve release of your identity, at least until the Office refers your charges for investigation.

Unfortunately, the law did not make the Special Counsel a more effective outlet for disclosures. The OSC's referral rate remains abysmal. Further, the OSC still tends to favor the tactic of scapegoating the small fry. In 1993, for example, the OSC informally agreed there was a "substantial likelihood" that a whistleblower was correct in alleging that military radar jammers were not airworthy—but refused to order an agency investigation unless the whistleblower agreed to delete the names of Defense Secretary William Perry and then-aide John Deutsch (who continued to try to sell the equipment despite a congressional ban). When the employee did not consent to diluting his charges, the OSC refused to take any action, and did not order an investigation at all into the whistleblowing disclosure.

CONGRESS

Whistleblowers often have been successful in using the constitutional system of checks and balances, triggering legislative oversight of Executive Branch abuses. Members of Congress, however, are pressured by all types of constituent groups, including major contributors in their states or districts. Members also often want to retain good relations with the Executive Branch, unless there is a compelling reason to challenge the bureaucracy. For these reasons, it is important to do some research before blowing the whistle to your local member of Congress. Some questions you might ask include:

- Is your employer a big supporter or major campaign contributor to this member of Congress? The member may be reluctant to do battle with an organization that helped put him or her in office or is a major player in his or her district.

- What are the member's views toward your particular agency or company? Does the member have a history of relations with or positions toward the agency or company?

- What is the member's past track record in battling the system on behalf of other whistleblowers? Call those people to see if they were satisfied with the congressperson's tenacity in challenging wrongdoing in the system and protecting their right to blow the whistle. If the office does not have a strong record of supporting whistleblowers, you may think twice about entrusting your story to that member.

Many members of Congress simply pass complaints about the bureaucracy back to the agency for self-investigation. As we have explained, this action is rarely successful, because the matter is often channeled to the perpetrators of the misconduct. To make matters worse, a member of Congress may not protect your identity even if you request it, because of a congressional staffer's inexperience in dealing with the bureaucracy, or the individual member's unwillingness to stand up to a powerful agency or corporation.

Whistleblowers often make the mistake of thinking that their best allies in exposing fraudulent activity are the authorizing and appropriations committees in Congress that allocate funds for the bureaucracy. Although some congressional committees have vigorous oversight staffs, many committee members are captured by the same influences that pressure any congressperson or agency decisionmaker.

For example, the Pentagon procurement scandals in the 1980s demonstrated the cozy relationships between some members of congressional committees and contractors. The National Security Committee in the House and Armed Services Committee in the Senate have many members who seek positions on the committees because of large defense contractors or military installations in their states or districts. An analogous dynamic exists with the Agriculture Committees. Honoraria, or payments for speeches, are a similar concern. In 1987, the Chairman of the House Armed Services Subcommittee on Procurement and Military Nuclear Systems received 80 percent of his yearly honoraria from speeches to defense contractors. His was not an isolated case: six of the other 18 members of his committee also received more than 50 percent of their yearly honoraria from defense contractors.

Keep in mind also that as an institution, Congress can prove as unwilling to hear bad news as agencies in the Executive Branch. It is true that some of the major scandals of the 1980s were exposed with the help of certain congressional committees. All too often, however, Congress as an institution fails to take the lead in passing meaningful reforms once the headlines fade.

The Congressional Accountability Act, one of the first laws passed from the 1994 "Contract with America" advanced by House Republican leaders, is an example of the limits of reform. Supposedly, the Act applied employee rights laws to congressional staff—laws ranging from race and sex discrimination to civil service merit system protection. Unfortunately, the implementing procedures skipped over the Whistleblower Protection Act. There is no disclosure channel for staff who want to blow the whistle on

a member of Congress who takes a bribe or otherwise violates the law. Nor can a staffer exercise the whistleblowing defense to challenge a retaliatory firing.

That said, there are many individual members of Congress who are sincere champions of whistleblowing. Many more will respond if your dissent is supported by a solid constituency base, or promises opportunities for media and other political visibility on an important public issue.

In addition, key members of Congress have at times provided the clout to protect individual whistleblowers from reprisal. This protection can be extremely important. Although it is technically unlawful to interfere with or harass a congressional witness, the Justice Department rarely enforces this law—which emboldens agencies to strike back at whistleblowers for their disclosures to Congress.

Sustained congressional protection of individuals is the exception. You should not assume that you will be able to secure such protection, particularly for what may be a multi-year harassment campaign against you. If you plan to go to a member of Congress, first check that individual's record very closely. If you are counting on a congressional shield from ensuing harassment, pin down whether and how far the congressional office is willing to go.

Tips on Contacting Members of Congress

The following are some suggestions on how to establish contact and work successfully with members of Congress.

1. ***Before you write to members of Congress, make sure that you have thoroughly checked their track records.*** Do not divulge any information to them before you take this important step. Find out if they have helped whistleblowers in the past and if they followed up once the headlines faded. You can do this by researching their past work in back issues of newspapers. If you find that they quickly dropped the matter, you need to be wary.

*2. **Keep your letter short.*** Many staff members do not have the time to read more than a page. If it is impossible to condense your letter to two pages or less, it is a good idea to prepare a one-page fact sheet or an executive summary. At the beginning of your longer letter, flag the fact sheet for the staff member.

*3. **Make it clear early in your letter whether you consent to having your name or documents shared with anyone in the bureaucracy.*** Otherwise, your letter is likely to be processed right back to the agency for which you work (or that oversees your private-sector contractor). Also, make it clear to your reader whether or not you need to remain anonymous. If you want to preserve confidentiality, request that the recipient take the precaution of talking to you before acting on your letter.

*4. **In a clear and concise way, state your factual case in the beginning.*** Enclose the most important documents, but do not send a large stack. Make a list of other documents that you have and *do not send originals.* Keep your story clear of jargon, and do not assume that the staff member who reads the letter will understand how your agency or company works. Again, if you need to send a longer statement, separate it from your cover letter or fact sheet. The short version should be no more than a two-page summary.

*5. **Focus on the public-interest issues raised by your allegations.*** It is all right to talk about harassment or retaliation, but put it at the end of the letter and don't dwell on it. A congressional office is much more likely to offer a legislator's support if there is something in it for the public—and not simply for you. Particularly if you are not a constituent, it is in your interest to be perceived not merely as a individual victim of injustice, but as an important source of information on an issue of concern to the voters, such as a public health or safety hazard you are exposing.

*6. **Offer guidance for follow-through.*** At the end of your letter, make suggestions on where congressional staff might go to pursue follow-up investigations or further corroborating documentation. Let the recipients of your letter know if there are any investigative agencies working on your case, and whether you think they are successfully uncovering anything of value.

*7. **Make sure that staff members have a way to reach you during working hours.*** If you can't talk to them from your workplace, find a discrete way for someone to take a message for you and return the call from an outside telephone during your lunchtime.

*8. **If you have not received a reply within two weeks, call the office in Washington and ask to speak to the Legislative Assistant who covers your issue area.*** Ask whether the staffer has received and had a chance to read your correspondence, and if so, whether you can be helpful in answering any questions. Congressional staff members are very busy and the most successful whistleblowers know when to keep calling a staff member and when to wait. Do not be a pest, but make sure that you do not fall through the cracks. Do not demand excessive attention, and be polite at all times.

*9. **Offer to act as a "ghost writer" in drafting communications for congressional staffers who are open to pursuing your allegations, and are interested in a working relationship with you.*** That ensures that the accuracy of your message will not be threatened by having it pass through another person with less background on the issue. Further, it is less burdensome for a staffer to revise and edit what you write than to draft the material.

*10. **Watchdog groups have good working relationships with various members of Congress and you may be more successful going through them.*** These watchdog groups can play the role of advocate for you and sometimes can keep your identity anonymous. They may know more about the member's relationship with your company, industry or agency, and his or her record on whistleblower cases. You may want to team up

with the advocacy group for meetings with a legislator's staff, in order to draw support from the organization's credibility or clout on Capitol Hill.

FIGHTING FRAUD: THE FALSE CLAIMS ACT

The False Claims Act offers an avenue for whistleblowers exposing fraud. Nicknamed the "Lincoln Law," the False Claims Act was passed during the Civil War. By facilitating a partnership between whistleblowers and the government, it has become the nation's most effective resource for citizens to challenge fraud in government contracts. Through this law, individual whistleblower "relators"—employees or nonemployees who are original sources of evidence of fraud—can challenge government contract fraud directly before a jury of taxpayers.

President Lincoln knew that standard government oversight mechanisms could not keep pace with unscrupulous defense contractors who were capable of producing weapons that were more dangerous to Union soldiers than to the enemy. In 1863 he discovered that the same horses were sold to the cavalry two and three times, and that sawdust was added to gunpowder. Union guns were backfiring and killing federal soldiers, instead of confederate troops. As a result, Lincoln won the right for citizens to serve as the government's eyes, ears and reinforcements through False Claims Act, or *qui tam*, lawsuits. These are private attorney general actions, literally those filed "in the name of the king." Through *qui tam* suits, whistleblowers can force the return of fraudulent earnings to the Treasury, and keep a portion for themselves. Unfortunately, the law was amended during World War II at the behest of military contractors and gradually eroded by the Supreme Court, until it lost much of its effectiveness. But by 1986, renewed interest in the prevention of fraud and waste and determined leadership by Senators Charles Grassley (R-IA) and Rep. Howard Berman (D-CA) led to an amendment that put the teeth back into the False Claims Act.

The Act allows individuals to sue private firms on behalf of the federal government when they believe there is fraud involved in contracts. There is a six-year statute of limitations for the whistleblower to act. Contracts have been defined broadly to include corporate commitments in exchange for government licenses or regulatory approval required by law. This means, for example, that a whistleblower "relator" can challenge a government contractor's fraudulent cover-up of violations of environmental or other laws in which compliance is a condition of the contract. The whistleblower can ask for three times the dollar amount of the fraud to be returned to the government, as well as $5-10,000 for each false claim. After a whistleblower initiates a suit, the Justice Department has 60 days to investigate the claims and decide whether it will take over the case, or let the whistleblower prosecute it alone. In practice, the Justice Department often takes six months, a year, or longer to decide. The entire cycle for a False Claims Act suit may range from two to five years or more.

If the government takes over a case and proceeds to recover money for the taxpayers, the whistleblower is guaranteed a "finder's fee" award of 15 percent of the recovery. If the government joins a suit to which a whistleblower has substantially contributed, the incentive award can increase up to 25 percent of the amount recovered (although the government has never agreed to the maximum). If an individual prevails without government intervention, s/he receives an award of 25 to 30 percent of the amount recovered plus attorney's fees. The average amount recovered by relators is 18 percent of the funds returned to the Treasury.

According to a 1996 report by Taxpayers Against Fraud (TAF), a non-profit organization that champions the False Claims Act and helps screen cases for private attorneys, roughly 1400 suits have been filed since 1986. The statute is becoming increasingly popular: in fiscal year 1987, relators filed 33 *qui tam* suits; by fiscal 1995 the number had skyrocketed to 278. Initially most of the suits involved Pentagon contracts; over time, the balance has shifted to contracts in health care and other areas. The Act's

scope is still evolving, as it is applied to violations of environmental and other laws whose compliance is built into government contracts.

More importantly, the record shows that the law obtains results. TAF's 1996 study revealed that since the 1986 amendments, the Justice Department has obtained some $3 billion in fraud recoveries through whistleblowers' use of the False Claims Act. Of the $3 billion recovered by the government, roughly two-thirds came from suits initiated by the Justice Department, and one-third—$1.13 billion—came from whistleblower *qui tam* suits. The deterrent effect may be even more significant. Although this effect is impossible to measure precisely, an economic study commissioned by TAF estimated that the Act has deterred some $295.8 billion in fraud since the 1986 amendments. By contrast, in 1985 the Justice Department's entire fraud effort garnered only $27 million. The Act has also outdone corporate voluntary disclosure programs: a 1996 General Accounting Office (GAO) report found that voluntary disclosure programs have recovered only $215 million for taxpayers.

Not surprisingly, the Act's success has earned it powerful enemies among large contractors, such as General Electric, who repeatedly have been caught. Several defense companies struck back by attempting to have false claims cases against them dismissed on the grounds that the law is unconstitutional. So far all attempts have failed.

In 1993, a coalition of 22 contractors, nicknamed the "fraud lobby," launched a campaign to gut the law. Since 1990, 20 of 22 members had pleaded guilty or paid fines totalling $566 million for fraud; $125 million of this came through the False Claims Act. Seventeen out of 22 were multiple offenders. During their legislative efforts, the lobby's members faced 28 active, unsealed *qui tam* suits. As Senator Grassley summarized, "They hate [the Act] because it is very effective at exposing their fraud."

The fraud lobby's legislative campaign failed—but not without stirring up significant debate over the law within the Justice Department and Congress. The Justice Department served to an

unnerving degree as industry's advocate at the outset of the legislative battle, backing proposals to impose various limits on False Claims cases—and even proposing that civil service employees be barred from pursuing cases under the Act.

Although the False Claims Act withstood this assault by the fraud lobby and its backers, the debate they initiated is far from over—and whistleblowers interested in pursuing this legal avenue would do well to follow it. In brief, the debate centered on industry's plan to ban relevant citizen suits once a company announced it was investigating itself through a voluntary disclosure program. The goal was to restore corporate and/or government monopolies on uncovering and challenging fraud. Industry's concern about a conflict between the False Claims Act and voluntary disclosure programs, however, is unfounded. A 1996 GAO report found that only four out of 129 voluntary disclosures involved overlapping *qui tam* suits. The GAO concluded that the two disclosure channels complement each other, and that *qui tam* suits help to keep voluntary disclosure programs more honest.

Equally misguided was the Justice Department's proposal to curb government employees' rights to use the False Claims Act. The proposal was motivated by the concern that public employees would bypass the chain of command to seek fortunes through False Claims Act suits. No defensible examples of this exist, however. The most publicized case involves Navy auditor Paul Biddle's suit against research fraud. Biddle went through the agency chain of command, the Defense Contract Audit Agency, Health and Human Services, NASA's Inspector General, the Air Force, and Congress. He finally turned to the False Claims Act only after learning that the Navy had limited its investigation to two of the ten years of fraud he had uncovered.

As the judge explained about another widely-maligned government employee whistleblower, Leon Weinstein, and his public interest partners: "Ultimately, what appears to have happened in this case is, after seeing no effective action taken by the government, relators filed this suit. This appears to be exactly what Congress intended, regardless of whether the relator is a govern-

ment employee or not." Far from withholding evidence, Mr. Weinstein received a letter of commendation from the FBI Director for his work on the case as a government employee before filing a false claims suit.

In the end, the campaign to neutralize the False Claims Act was the catalyst for a media spotlight on whistleblowers and on big business fraud. The fraud lobby could not find any office to introduce its proposals. Almost certainly, the fight is not over.

Understanding the background of and controversies over the False Claims Act is important for any whistleblower considering the Act as a legal avenue. But it is only the first step. Filing a false claims suit is a big, and expensive, move. You need to find a competent lawyer who has the financial resources to fund a case that could run into five or six figures in costs and fees. If the government decides not to take your case, you and your lawyer must be prepared to go through the long and expensive process of legal discovery in order to continue the lawsuit. Don't underestimate the ability of a company to finance a large number of lawyers to fight you. You and your lawyer must be mentally prepared to follow through on a case that could drag on for years. In some cases, a law firm will agree to limited representation—filing a complaint and advocating that the Justice Department take over the case, but not committing to litigate independently if the Justice Department turns it down.

The high costs of litigation are perhaps the greatest constraint facing whistleblowers who seek to file false claims suits, but they are not the only consideration. To follow through, you will eventually have to go public in a false claims suit, and there is a chance that you could be permanently blackballed in your field. The whistleblower protection clause is an important part of the False Claims Act, but it will take time and money for a lawyer to go to court and fight for your rights.

The Act imposes other limits. During the 60 days to more than a year that the case is "under seal" for Justice Department review, you cannot discuss the evidence. This estimated time lag is conservative; delays have exceeded five years. Ironically, this

means that after filing a false claims suit, you are gagging yourself from public dissent until the Justice Department makes a determination. You must make any media disclosures *before* filing the case: courts will dismiss a case if a whistleblower "breaks the seal" by talking to the press. If you do speak to a reporter before filing a false claims suit, beware that if the reporter does not credit you with exposing the fraud, you may be disqualified from credit as the original source of the evidence, and thus be ineligible to file suit.

Similarly, the government can engage in the False Claims Act equivalent of plagiarism. Even if the government is ignorant of the fraud before you expose it to relevant officials, the Justice Department can beat you to the punch by filing a False Claims Act suit on your own disclosure, and you will be disqualified. The lesson to be learned is to be ready to file expeditiously and then remain mum after making any disclosures to the government or the public.

Other factors may limit the effectiveness of using the False Claims Act to blow the whistle, particularly in cases in which the government itself has acquiesced to the company's wrongdoing. Often, when a favored contractor finds itself in trouble over procurement, the government agency is more interested in hiding the problem than solving it: scandals in government contractor programs can create problems for the government's program managers. Therefore, a government agent may hand out waivers, contract changes, or some other form of approval for the company's misconduct, even though it formally violates the agency's regulations. The Justice Department, moreover, rarely prosecutes a government agent for giving waivers, and often uses the waivers as an excuse not to prosecute the companies.

One way to counter this threat to your legal challenge is to forego alerting company leaders or government program managers. Silence on your part, however, brings risks. To begin with, blindsiding your employer or the relevant government agency may not be the most efficient way of challenging problems, particularly when a contractor's leadership is acting in good faith and

would take responsible corrective action if given the chance. Further, this approach can draw a severe backlash and damage your credibility. Equally significant, without some formal record of your prior opposition to the fraud, you may become the scapegoat for the company, the government, or both. If you are convinced that corporate and government bureaucracies are not acting in good faith, another solution is to find a lawyer willing to take on the government agent involved in the wrongdoing as well as the company: bureaucrats do not have the legal authority to obligate the government against its own rules and regulations.

A final note of caution is to be sure that you know and understand the rules and regulations that you believe are being violated. Government regulations are sometimes written so loosely and vaguely that it is difficult to prove illegality. An illustration of this problem is the case of the now infamous $435 hammer. After Congressman Berkeley Bedell was tipped off to the overpriced hammer by a whistleblower, he asked the Navy to audit the program and expose the fraud. The Navy responded that the price for the hammer was "exorbitant but legal," because the company used "government-approved purchasing and estimating systems."

THE NEWS MEDIA

One of the most obvious whistleblower outlets is the news media. Indeed, it can be very effective when handled properly through a responsible reporter. The media is indispensable for making a difference when the political stakes are high. None of the success stories listed at the beginning of this handbook could have occurred without the active role of the media.

At first blush, going to the media to blow the whistle appears to be the easiest and quickest way to warn the public about a threat to their health and safety, or to let taxpayers know their dollars are being wasted. But as in any field, there are groundrules in media work that participants should know and respect. Not all whistleblowers do, and those who do not are generally less successful. Keep in mind that not all reporters are willing to take

the time and effort necessary to publish your allegation, or to maintain the anonymity of their source. Going to the media is a serious and significant part of the whistleblowing process. It may not be sufficient, but it is generally a necessary part of any effective whistleblowing effort. It is worth your time and attention to design a careful media strategy.

To protect yourself, you need to choose a reporter carefully. That involves doing some research. Identify journalists who cover your area of expertise for each of the major newspapers and radio or television networks. There are several excellent media guidebooks that can help. Computer searches of periodicals at your local library can also provide leads. Once you have identified a number of reporters who cover your area, research some of the stories each has written in the past. If you are thinking about working with a broadcast journalist, you may have to request videocassettes of some of their work, because most libraries do not routinely keep this kind of material on file.

It is important to develop an idea of how a reporter will handle your story before you make contact. If you find that the reporter's past stories seem largely to echo reports from the relevant government agency or corporate public relations office without adequately questioning statements or assumptions, that journalist is not likely to ask the tough questions or conduct the thorough investigation you may need. Keep looking until you find one whose track record and way of doing business reflect what you hope to achieve by blowing the whistle.

You must also decide whether to contact a local reporter or the national press. There are advantages and disadvantages to each. A local reporter will be more interested in your story because of its home-town implications, but may also face more pressure to stay away from your whistleblowing allegations, if the government agency or company has a powerful economic base in the local area. Another advantage to the local approach is that those reporters are better able to follow up on leads: they generally have immediate access to witnesses who can back up your claims and perhaps provide more documentation. If you do land

a good local media story, it will get the attention of the company or bureaucracy. But if the story does not make a significant enough splash in Washington DC, the net effect once again may be detrimental: the news may trigger a cover-up or reprisals against you, rather than serve as a catalyst for corrective government action.

A national story inherently has the greatest potential for impact, but it is often hard to get the national press in Washington to pay attention to issues that do not have a clear and immediate effect on the political scene in the capital. To be confident that a national outlet will be interested in your story, you must be able to identify the ways in which your allegations directly involve or affect a large government program or agency, or a major corporation. Keep in mind, too, that it may be more difficult for reporters in Washington to verify your story from there; you should not assume that Washington reporters will have the time or the money to travel to your area.

In some cases, your best approach to the local/national question is a compromise: consider working with a local paper that is part of a national newspaper chain with a Washington office or a national newswire connection. This will give your story a hearing beyond your local news orbit. Newspapers in a chain are also less likely to be intimidated by local political or economic pressures, and your story may appear nationwide. Well-known chains include the Cox, Gannett, Hearst, Knight-Ridder, Newhouse, Scripps Howard and Thompson syndicates. Examine your local papers (particularly the front or editorial pages) to find out if any of them belong to a chain that has a national office or are on a major newswire such as *The New York Times* or *The Washington Post/Los Angeles Times* newswires. The Associated Press, United Press International and Reuters are news services that sell stories to papers throughout the nation. The Associated Press is the biggest, with news bureaus in every state.

Another important consideration in selecting a media outlet is how time-sensitive your information is. Are you trying to ward off an imminent disaster, or do you have the luxury of allowing the reporter more time to research and develop your story? If you have time to spare, a magazine writer, broadcast producer for a weekly investigative show or an investigative reporter may be your best option. If you need immediate turnaround, network news or a daily newspaper reporter are good choices.

Once you have selected a media outlet and reporter, it is important to understand how best to approach the reporter or broadcast producer, and what s/he can and cannot do for you. Before providing the reporter any information, be sure to clarify and reach agreement on the terms of your working relationship. Whistleblowers often have unrealistic expectations of reporters, and this can undermine your ability to work together effectively.

One of the most important issues to clarify with a reporter is whether you expect anonymity. A good reporter will not reveal his or her sources, even before a court of law. Before you tell your story to a reporter, you must set clear rules for how you want to be identified.

> *"It makes all the difference whether you blow the whistle to an audience that is hungry for your information, instead of threatened by it."*
> *—Department of Agriculture whistleblower*

Always specify the terms of your communication with the reporter. Be clear about whether or not you are speaking "on the record." If so, the reporter can identify you by name and position in the government or industry. If you choose to speak "on the record," be sure to make it clear that you are speaking only for yourself, and not as a representative of your government agency or company.

You can decide to speak "off the record," which means that the reporter cannot use your name, but can characterize your position (for example, a quality engineer in the MX program). Unless you are careful, such characterizations can be very revealing to those people who may try to identify the source of the leak. You should come to a mutual agreement on such characterizations in advance.

When you provide information "on background," the reporter