SELECTED ISSUES IN COMPLIANCE PLANNING FOR DOE CONTRACTORS

John C. Person
Person & Craver LLP
Washington, D.C. (USA)
(202) 466-4434 (phone)
(202) 833-8491 (fax)
JPATTNY@aol.com (e-mail)

ABSTRACT

The purpose of this paper is to identify a selected set of laws, regulations, and departmental orders that require compliance by the Department of Energy (DOE) contracting community and to propose administrative processes and controls for maximizing such compliance. The reason for advancing this topic at this forum is that the DOE contractor[1] is one of the most heavily regulated entities conducting business in America today. The downside to non-compliance with the applicable regulatory scheme can be enormous – in addition to the monetary fines and penalties are the potentially far more damaging non-monetary penalties of a tainted reputation, negative "past performance" ratings, or the corporate "death sentence" of suspension or debarment. In addition, the "business judgment rule" that protects corporate officers and directors from liability has evolved to require such persons to affirmatively seek out potential non-compliances as a condition to invoking the protections of the rule.

The first layer of regulation is that which applies to all companies *qua* corporate entities doing business in the United States. Such regulations, among other things, would include workplace safety and employment requirements. The second layer of regulation is that which applies to government contractors. In this second layer of regulations are procurement integrity requirements along with a family of anti-fraud provisions. The third layer of regulation on the DOE contractor includes the maze of environmental regulations that confront both environmental remediation contractors and waste processors – two functions that are at the centerpiece of the DOE Weapons Complex cleanup program. The fourth layer of regulation is that which governs the nuclear safety aspects of working in a radioactive environment. Together, these layers of regulation present a patchwork of overlapping requirements that can present a trap for the unwary and uninitiated. While an affected company would want to undertake its own risk assessment to determine in which of these layers of regulation the company faces the most exposure, it is fair to say that a DOE contractor's compliance program would address regulatory issues in varying degrees for each of these layers.

REGULATORY REQUIREMENTS AFFECTING COMPANIES GENERALLY

Companies that do not contract with the government or do not perform work on DOE Weapons Complex sites still face a myriad set of regulations with which they must comply. For example, all companies must comply with workplace safety regulations. Violations of occupational health standards can result in significant civil penalties, and, in

the most egregious cases, criminal prosecution[2]. Another set of regulations that apply to all companies are those that govern discrimination and harassment. For example, federal statutes, regulations, and executive orders forbid discrimination based on race, color, sex, religion, national origin, age, or disability, and impose civil liability and potentially punitive damages for violations of these laws[3]. The number of discrimination and harassment actions has increased significantly over the past ten to fifteen years. This increase in employment law litigation is expected to be seen in the DOE Weapons Complex as well, given the nationwide effort to downsize the workforce. Other areas of regulation for a company doing business generally include antitrust, securities regulation, and labor law.

REGULATORY REQUIREMENTS AFFECTING GOVERNMENT CONTRACTORS

One area of compliance concern for government contractors is an area that is generally referred to as "defective pricing." Under the Truth in Negotiations Act (TINA), as recently modified by the Federal Acquisition Streamlining Act of 1994 (FASA), government contractors are required to submit "cost or pricing data" for all sole-source competitions and contract modifications that exceed $500,000 (by regulation, the threshold amount presently stands at $550,000). Under these provisions, government contractors are required to certify that to the best of the contractor's knowledge and belief the cost or pricing data is current, accurate, and complete. Failure to provide current, accurate, and complete data can result in a downward pricing action. Where the contractor deliberately fails to provide current, accurate, and complete data, the government can bring an action against the contractor under any number of anti-fraud provisions, described below.

Another area of compliance concern for government contractors generally is described under the rubric of "anti-fraud" provisions. The False Statements Act, 18 U.S.C. § 1001, prohibits knowingly or willfully making a false statement or representation, or concealing a material fact, or using a false writing or document in connection with a matter before a federal agency. The Major Fraud Act, 18 U.S.C. § 1031, proscribes knowingly executing or attempting a scheme to defraud the United States where the contract involved has a value of $1 million or more. The Forfeiture Act, 28 U.S.C. § 2514, provides that a claim against the government is forfeited in its entirety if fraud by the contractor occurs during contract performance or during the claim submission process. The act requires that the government prove by clear and convincing evidence that the claimant (1) knew the claim was false, and (2) intended to deceive the government by submitting the claim[4]. The anti-fraud provisions of the CDA provide that a contractor who is unable to support any part of a claim because of misrepresentation of fact or fraud shall be liable for the unsupported part of the claim as well as for the government's costs to review the claim[5].

The False Claims Act (FCA), 31 U.S.C. § 3729 *et seq.* imposes liability for seven enumerated acts, including knowingly presenting a false or fraudulent claim for payment or approval or making a false record or statement to get a false or fraudulent claim paid or approved by the government. A "knowing" submission may be shown by either (1)

actual knowledge of the false information, (2) a deliberate ignorance of the information, or (3) a reckless disregard of the false information. The government only need prove its fraud case by a preponderance of the evidence and can recover up to three times the amount of damage and additional civil penalties of $5,000 to $10,000 per fraudulent act. As amended in 1986, the FCA provides remedies for persons wrongfully discharged or otherwise discriminated against in their employment because "lawful acts done in furtherance of" an FCA action. 31 U.S.C. § 3730(h). Under the *qui tam* provisions of the FCA, if the government declines to intervene on the relator's behalf, the relator can "take on primary responsibility for prosecuting the action." 31 U.S.C. § 373(c)(1). Several high profile qui tam cases have been filed against contractors at a number of DOE Weapons Complex sites, including Savannah River[6], INEEL[7], Hanford[8], and Rocky Flats[9].

Underscoring the need to comply with the "anti-fraud" regulations affecting government contractors is the result in the recent case of *UMC Electronics Co. v. U.S.*[10]. In that case, the contractor filed a certified claim for $3.8 million with the Air Force on a contract to provide portable floodlights. In that submission, the contractor identified its claimed costs as actual costs. The contractor further represented that it had actual cost data to support its claim. Following denial of the claim and appeal of the claim to the Court of Federal Claims, the government filed counterclaims under the Forfeiture Act (28 U.S.C. § 2514), the False Claims Act (31 U.S.C. § 3729), and the anti-fraud provisions of the Contract Disputes Act (41 U.S.C. § 604). The government argued that the costs represented by the contractor as "actual" were really just purchase order amounts that included amounts that had not yet been incurred. In holding that the penalties under the Forfeiture Act, the FCA, and the CDA are cumulative, the court ruled that the contractor violated all three statutes. As a result, the contractor forfeited the entire $3.8 million claim under the Forfeiture Act, exposed itself to at least $5,000 in civil penalties for each fraudulent act under the FCA, and was liable to the government under the CDA in the amount of $223,500 corresponding with the amount of the unincurred material costs represented as "actual" by the contractor.

REGULATORY REQUIREMENTS HAVING ENVIRONMENTAL APPLICATION

While any number of environmental laws and regulations can affect DOE contractors, the two laws that have the most sweeping application at DOE Weapons Complex sites are The Comprehensive Environmental Response, Compensation, and Liability Act (CERCLA of Superfund), 42 U.S.C. § 9601 *et seq.*, and The Resource Conservation and Recovery Act (RCRA), 42 U.S.C. § 6901 *et seq.* As a general matter, CERCLA is retroactive in application, in that it covers conduct that occurred in the past as long as there is a present effect of that past activity. Under CERCLA, liability is imposed on a strict liability basis, with joint and several liability for all Potentially Responsible Parties (PRPs), including owners, operators, generators, and transporters. RCRA, on the other hand, primarily focuses on the ongoing activities of waste management treatment and disposal.

Virtually all the Weapons Complex sites are covered by CERCLA, inasmuch as the major sites are on Superfund's National Priorities List. Likewise, many of the pump-and-treat, vitrification, and other low-level and mixed waste processing activities are considered to be "treatment, storage, or disposal facilities," and are thus governed by RCRA. In this environment, remediation contractors have been held by the courts to be potentially liable under the environmental statutes[11]. Moreover, remediation contractors have not been afforded the protections of the "government contractor" defense[12]. Contractors found to be in violation of RCRA can be fined upwards of $25,000 per day for each day of non-compliance. Criminal violations of RCRA can draw jail time.

REGULATORY REQUIREMENTS HAVING NUCLEAR APPLICATION

Price Anderson Amendments Act of 1988

The Price Anderson Amendments Act of 1988 (PAAA), 42 U.S.C. §§ 2011-2282, extends public liability indemnity coverage to all DOE contractors and subcontractors in the event of a nuclear incident in exchange for the submission of the covered parties to a penalty provisions for failure to comply with nuclear safety-related rules. Although the organic act has been in effect for over twenty years, the Office of Enforcement and Inspection (E&I) of DOE's Environmental, Safety, and Health (ES&H) organization did not begin enforcement proceedings under the act until 1995. This is due almost entirely to the fact that DOE had not developed a cohesive set of implementing regulations until 1995. Those regulations include 10 CFR Part 820 (implements penalty provisions and prescribes procedural process, 10 CFR Part 830 (quality assurance), and 10 CFR Parts 834 and 835 (radiation protection). Since 1995, enforcement actions have proceeded at a pace of approximately one per month. These actions have included virtually all the major contractors at each of the major weapons complex sites. Enforcement targets also have included national laboratories and various subcontractors. Most recently[13], on August 24, 2000, DOE issued a PNOV to Lockheed Martin Energy Systems (LMES) in an amount of $1,045,000 concerning a number of quality assurance issues affecting nuclear safety at the Y-12 site at Oak Ridge. This Severity Level II PNOV included the largest civil penalty ever proposed under the PAAA enforcement regime.

Whistleblower Protection Provisions

The DOE whistleblower provisions are modeled after a parallel set of provisions applicable to Nuclear Regulatory Commission licensees, under Section 210 of the Energy Reorganization Act of 1974. The principal regulations applicable to DOE contractors are set out at 10 CFR Part 708. These regulations, which have been modified over the years, were first promulgated in 1992. They were promulgated in part because the Secretary of Labor had determined that the Department of Labor (DOL) lacked jurisdiction over contractor-operated DOE facilities and that Section 210 applied to NRC licensees only[14]. The DOE whistleblower provisions are incorporated by reference into all DOE contracts and subcontracts by the DOE supplements to the Federal Acquisition Regulations (DEARs). In particular, the DEAR clauses require that all M&O contractors and others performing work at sites that DOE owns or leases, including contractors performing work

directly related to activities at DOE sites, to comply with the employee whistleblower requirements set forth in 10 CFR Part 708[15].

Of note, the DOE whistleblower provisions are complementary to a family of other whistleblower provisions under various environmental statutes. These related statutes include: (1) Safe Drinking Water Act, 42 U.S.C. § 300j-9(i); (2) Water Pollution Control Act, 33 U.S.C. § 1367; (3) Toxic Substances Control Act, 15 U.S.C. § 2622; (4) Solid Waste Disposal Act, 42 U.S.C. § 6971; and (5) Clean Air Act, 42 U.S.C. § 7622. These statutes share the same legislative histories and are implemented by the same set of regulations. While these whistleblower statutes, as implemented, may be applicable to various DOE contractor employee activities in addition to the provisions set out at 10 CFR Part 708, the employee may elect to proceed only under one set of regulations[16].

Under the DOE whistleblower provision, activity protected from retaliation includes employee disclosures to any upper-tier contractor, the Department, or the Government: (1) a substantial violation of the law, rule, or regulation; (2) a substantial and specific danger to employees or to public health or safety; (3) fraud, gross mismanagement, gross waste of funds, or abuse of authority; or (4) refusal to participate in an activity the employee reasonably fears will cause bodily injury to himself or others[17]. If a contractor retaliates against an employee (*e.g.*, discharge or other adverse action), the employee must file within 90 days of the day he knew or should have known of the alleged retaliation two copies of a complaint with the cognizant DOE site manager[18]. The complaint, among other things, must include a description of the alleged retaliation taken against the employee along with a description of the disclosure, participation, or refusal the employee believes gave rise to the retaliation[19]. In the event that the parties are not able to resolve the matter at the pre-adjudicatory phase, the employee may refer the matter to DOE's Office of Hearings and Appeals (OHA). The OHA may conduct an investigation, following which, a Hearing Officer will be appointed and a hearing will be held[20].

Under a final rule promulgated on October 18, 2000, DOE's "Legal and other proceedings" cost principle is modified to make allowable certain defense, settlement, and award costs associated with employee whistleblower retaliation actions filed in various courts and administrative agencies. Under new regulation DEAR § 931.205-47(h), contracting officers are granted greater flexibility in allowing or disallowing retaliation-related costs. Under the previous application of the rule, which disallowed contractor costs if the employee prevailed in its whistleblower action, contractors were quick to settle so as to avoid any potential disallowance. Under the new rule, defense costs arising from the exercise of prudent business judgment would be allowed, while costs of defending against "unlawful or egregious" contractor actions would be disallowed.

WHY DEVELOP A COMPLIANCE PROGRAM?

Without more, achieving compliance with applicable laws and regulations is salutary in its own right. Such compliance avoids potential civil and/or criminal liability that might

otherwise attach to non-compliance and improves the safety and working conditions of workers and others. Recent court cases suggest, however, that the existence of a robust compliance program can insulate corporate officers and directors from liability for breach of duty in corporate governance and oversight. In one such case[21], the influential Delaware Chancery Court ruled that a corporation's directors avoided liability to disgruntled shareholders because they had taken active steps to ensure compliance.

In various other regulatory schemes, the existence of robust and effective compliance programs is looked upon favorably by the courts, and is often viewed as a mitigation factor in the applicable enforcement regimes. In the employment law setting, the United States Supreme Court has recognized as an affirmative defense against the imposition of vicarious liability in sexual harassment cases the existence of a compliance program addressing such issues[22]. Elsewhere, in accordance with the EPA's "Policy on Incentives for Self-Policing: Discovery, Disclosure, Correction, and Prevention of Violations"[23], the EPA sets forth guidelines for self-policing and voluntary disclosure of environmental violations. To achieve full mitigation under the EPA rule, the company must have discovered and immediately disclosed the environmental violation through its own self-assessment or audit procedure. By the end of the first full year of implementation, the EPA reported that 105 companies self-reported in accordance with the policy. Additionally, EPA often times expedites the issuance of permits for corporations whose compliance plans the agency trusts.

In the PAAA enforcement arena, the existence of a robust compliance program that results in early self-detection of potential nuclear safety non-conformances can mitigate the severity of a PNOV and any accompanying civil penalty. The existence of such a program can also help to demonstrate that the potential PAAA non-conformance is an isolated event instead of a programmatic breakdown involving weakness in administrative or management controls. This, too, is viewed as a mitigating factor in the PAAA enforcement regime[24].

Finally, regardless of the regulatory environment in which a company is operating, the existence of a robust and effective compliance program gives that company credibility with the regulators that it can self-assess and self-police without the need for the intrusiveness of regulatory intervention.

COMMON FEATURES OF A COMPLIANCE PROGRAM

Much of the recent interest in compliance planning derives not so much from a corporate groundswell to become better and more responsible actors; but rather, comes in response to the Sentencing Guidelines for Organizational Defendants, issued on November 1, 1991 (Sentencing Guidelines or USSG). The Sentencing Guidelines provided in no uncertain terms that corporate self-reporting of violations and the institution of an effective compliance program are mitigating factors in assessing criminal liability. Specifically, these guidelines provide that a company's "culpability score" be reduced by three points if the offense occurred despite an effective program to prevent and detect violations of law (*e.g.*, a compliance program). More recently, the influential Delaware Chancery

Court has ruled that corporate management has an affirmative duty to put in place an internal system to timely detect illegal activity[25]. Accordingly, corporations have nothing to lose and much to gain by implementing internal compliance planning.

Under the Sentencing Guidelines[26], a company should include the following elements in its compliance program for it to be considered effective:

- Establish compliance standards and procedures for its employees that are reasonably capable of reducing the prospect of non-compliant conduct;
- Assign specific senior manager(s) overall responsibility to oversee compliance;
- Use due care to not delegate substantial discretionary authority to individuals whom the company knows, or should know, are likely to be engaged in non-compliant activity;
- Communicate its standards and procedures effectively to all employees through training programs or practical written guides;
- Monitor compliance with its standards, both through audit-type procedures and by instituting and publicizing a reporting system (e.g., "hotline") through which employees can report misconduct without fear of retribution;
- Enforce the standards through appropriate disciplinary mechanisms; and
- Respond appropriately to any offense that is detected, and take steps to prevent recurrences.

The company's compliance program should take advantage of the legal protections afforded under the attorney-client privilege[27] and the attorney "work product" doctrine[28]. The compliance program should provide that all internal investigations be headed by legal counsel so as to protect from disclosure communications between the corporate client and counsel. This attorney-client privilege protects both discussions between counsel and employees as well as reports by counsel to corporate management. Likewise, all internal reports should emanate from counsel to gain maximum attorney work product protection. A few words of caution are in order. The attorney-client privilege may be destroyed by the presence of even one non-client participant. Similarly, a disclosure to the government, even if "voluntary", can destroy both the attorney-client privilege and the attorney work product. Such a waiver can also be effected simply by voluntarily disclosing documents to a government auditor[29]. Finally, at least as against private litigants, a company may seek the protections of the so-called "critical self-analysis" or "self-evaluative" privileges. In jurisdictions recognizing the privilege, the company could protect from disclosure not only investigative files but also the audit process as a whole[30]. The "self-evaluative" privilege has not been successful, however, in thwarting discovery efforts of the government[31].

A compliance program should also include a detailed outline of the specific steps that need to be taken at the outset of an outside investigation. This should include a company-wide announcement to preserve the integrity of documents and computer files. The compliance program should also provide that employees are to notify the investigation response coordinator immediately upon being approached by government investigators.

SPECIAL FEATURES OF A DOE CONTRACTOR'S COMPLIANCE PROGRAM

The general principles described above can provide the basic compliance framework that can then be tailored to the particular compliance setting. Following below are the additional compliance features that should be considered when tailoring a compliance program for the DOE contractor. Working from the more general to the specific, these additional features include compliance issues affecting government contractors, environmental remediation and processing, and DOE Weapons Complex contractors.

Government Contractor Compliance Issues

During the early 1980s, the defense industry came under significant scrutiny on issues concerning fraud, waste, and abuse. Senator Proxmire (R-Wisconsin) regularly bestowed his "golden fleece" award on government contracts projects yielding highly uneconomic results (*e.g.*, the $400 hammer). In response to these criticisms, top executives of major defense contractors drafted principles of business ethics to encourage self-compliance. These principles, issued in 1986, became known as the Defense Industry Initiative on Business Ethics and Conduct. The centerpiece of this initiative was the recommendation that companies put in place a written code of business ethics and conduct. Other recommendations include:

- Robust program for distribution of the Code of Conduct and for orientation of employees with the code;
- Establishment of business standards in the Code of Conduct;
- Appointment of an ombudsman, ethics officer, or corporate review board to afford employee communication outside of direct line supervision;
- Assignment of high-level individuals to the program;
- Inclusion of follow-up procedures to employee charges;
- Mechanism for employee reaffirmation of Code of Conduct; and
- Inclusion of mechanism for voluntary reporting of violations.

In addition to including in a compliance program the core recommendations of the Defense Industry Initiative outlined above, the government contractor of today ought to place special emphasis on avoiding exposure to liability under the family of "anti-fraud" regulations that apply to virtually all government contracts. As the first line of defense against running afoul of the Forfeiture Act, the FCA, and the anti-fraud provisions of the CDA, the contractor should always verify that any claimed cost was, in fact, incurred. In its compliance program, such a control could be implemented by ensuring that the project manager reviews all pricing submissions, with assistance, as necessary, by the senior cost accounting specialist. The second line of defense is to properly characterize the nature of the incurred cost (*e.g.*, if the incurred cost is based on information gleaned from daily reports, describe it as such). There is nothing to be gained by overplaying the hand as to the degree of pricing definiteness: the government auditors will sooner or later divine the truth.

Environmental Remediation and Processing

With respect to environmental issues, a DOE contractor's compliance plan ought to include policy and procedural features designed to limit the contractor's liability arising from environmental issues. Most of the environmental risks can be effectively managed during the contract formation and administration phases of the project. Some recommendations include:

- Carefully characterize initial conditions to ensure that the proposed process works and to establish a well-defined baseline against which changes can be measured;
- Understand fully the effluent conditions required by the contract and the means to be employed to assure attainment of such conditions;
- Seek to use negotiated procurement over sealed bidding for complex projects;
- Do not agree to perform to the "highest professional standards"; the professional negligence standard is high enough;
- Limit overall liability to a stipulated amount;
- Contractor should sign shipping manifests only as *agent* for owner;
- Risk of change in regulation concerning remediation levels should be allocated to owner.

Nuclear Compliance Issues

A DOE contractor's compliance program should include a number of features that are specific to PAAA compliance initiatives. First, the contractor should appoint a PAAA compliance officer to serve as the point of contact on all PAAA-related matters, whether

inside or outside the organization. Second, the compliance plan should provide for the conduct of compliance audits to ensure that the contractor's non-compliance self-assessments are proceeding on a vital and proactive basis. Third, the compliance plan should provide for the prompt reporting of potential non-compliances through the NTS system to DOE. Similarly, the compliance plan should include provision for the regular briefing of the respective DOE site representatives for PAAA compliance matters.

The compliance audit itself should be proactive rather than reactive, and should be treated as a function separate from the investigation of a non-compliance. The audits should be scheduled to take place at regular intervals, either on a system- or process-wide basis or on an integrated basis (*i.e.*, cutting an administrative "slice" through the project). The audit team generally should be composed of contractor specialists knowledgeable of the audit process and having independent expertise in quality assurance, radiation protection, and/or nuclear safety. The contractor's organization should be sensitized to accommodate and cooperate with the auditors, given that the benefits derived from the audit function inure to the project as a whole.

Also set out in the contractor's compliance program should be pre-determined response mechanism. As pointed out above, virtually all major contractors on DOE Weapons Complex sites have had to respond to PAAA investigations, whether arising from their own conduct or the conduct of subcontractors. As such, the prospects of a continued and increasingly aggressive PAAA investigation program are well justified[32]. The first step is to determine whether individuals within the company (*e.g.*, officers, directors, managers, etc.) are targets of the investigation and/or whether any parent company is implicated. This latter issue is especially important in the DOE contracting community because so many of the contractors set up site-specific subsidiaries and because the DOE now requires parental guarantee of such subsidiaries' performance. Once an investigation is underway, the initial point of contact could be the company's PAAA coordinator. At some point, however, the PAAA coordinator should share or cede that function to the company's PAAA legal counsel. All internal and external information flows regarding the investigation should now be routed through the PAAA point of contract. The compliance plan should also emphasize that the most important juncture in the enforcement continuum to influence DOE into adopting a reduced enforcement posture is at the Enforcement Conference, prior to the issuance of any PNOV. It is at this Enforcement Conference that the contractor should state (if applicable) that (1) the violation was an isolated occurrence and not symptomatic of a breakdown of management controls, (2) the non-conformance was timely discovered through self-assessment and reported to DOE, (3) a prompt corrective plan was initiated, and (4) root cause analyses were implemented, as appropriate. The DOE has significant enforcement discretion; contractors should attempt to channel enforcement to the lower ranges of that discretion.

In addressing employee whistleblower concerns, a DOE contractor's compliance plan should incorporate features that promote the free flow of nuclear safety information and internal reporting. For starters, the company should require as a condition of employment that each employee cooperate fully in any investigation and report freely and

openly to the company all nuclear and safety-related concerns. Another compliance plan feature to address this issue is the establishment of a corporate policy that favors disclosure of safety concerns, articulates expectations concerning reporting, and prohibits discrimination.

As far as implementation of these features, a company's procedures should include regular training of supervisors and employees alike of the requirement of the free flow of nuclear and safety-related information within the company. Another feature of a company's implementing procedure could be the establishment of outlet mechanisms for employee concerns, including: (1) screening allegations for safety significance; (2) establishing processes for identifying and investigating wrongdoing; (3) assurances of employee confidentiality in the pre-adjudicatory stage; and (4) provision of a feedback mechanism to employee. Finally, the DOE contractor's implementing procedure should include an audit feature and pre-determined response mechanism similar to that outlined in connection with PAAA investigations, discussed above.

BEYOND THE ROLLOUT: HOW TO MAINTAIN A ROBUST COMPLIANCE PROGRAM IN THE DIGITAL AGE

Being a DOE Weapons Complex contractor subjects the company to a highly regulated environment that is fraught with risk – both monetary and non-monetary – for regulatory non-compliance. Presented above are the considerations that should go into the preparation of a DOE contractor's compliance program. For each layer of regulation considered (*e.g.*, the increasingly specialized regulations affecting government contractors, environmental contractors, and DOE contractors), a key element to effective compliance is the dissemination of the compliance program beyond the initial rollout. Without a continual training, feedback, and audit function, the compliance program is largely ineffectual and stillborn.

In this digital era, in addition to preparing the initial compliance plan and implementing procedures, the DOE contractor should make compliance awareness part of the fabric of the day-to-day work environment. That can be done using intra-company e-mails, intra-nets, and web sites dedicated to providing relevant postings to the company's employees. The web site can also be utilized to provide answers to frequently asked questions and engage various groups of employees into discussions on compliance issues. The training can be targeted such that various departments and the different management levels within those departments can receive compliance training that is tailored to the targeted group. Additionally, employees can be awarded "compliance certifications" for correctly answering web-generated compliance questions targeted for the particular group.

CONCLUSION

It is important for DOE contractors to understand the full range of compliance issues applicable to their day-to-day contract performance. In addition to compliance with regulations that apply to U.S. companies generally, DOE contractors must comply with the regulatory schemes governing contractors that: (1) work on government contracts; (2)

perform environmental remediation; and (3) work in a nuclear environment. The implementation of robust compliance plans to address these regulatory schemes is good and salutary in its own right: such plans heighten levels of worker protection and minimize corporate missteps in these important regulatory areas. In addition, in virtually every application the fact that a contractor has implemented such plans is a mitigating factor in both the assessment of liability and the imposition of damages. In addition, the cost of preparing and implementing[33] compliance planning are allowable costs that are valid indirect costs that may be spread across the contractor's business and fully recovered under cost-type contracts.

In the final analysis, a corporation likely will get involved in compliance planning in one way or another. Under one approach – the approach advocated by this paper – the contractor can develop and implement a compliance program in a proactive manner. If the corporation, however, gets caught in a non-compliant mode without a robust compliance program in place, it most assuredly will be forced to implement one as a government-imposed condition to probation.

FOOTNOTES

1. The term "contractor" in this paper includes subcontractors at any tier, given that most, if not all, the legal and regulatory requirements apply to all contractors, regardless of contractual privity with DOE or its Management and Operations (M&O) contractors.
2. *See* 29 U.S.C. § 666, *et seq.*
3. *See, e.g.*, Title VII of the Civil Rights Act of 1964, 42 U.S.C § 2000e; Americans with Disabilities Act of 1990, 42 U.S.C. § 12101 *et seq.*
4. *See Young-Montenay, Inc. v. U.S.*, 15 F.3d 1040 (Fed. Cir. 1994).
5. *See* 41 U.S.C. § 604.
6. *See Harrison v. Westinghouse Savannah River Co.*, 176 F.3d 776 (4th Cir. 1999).
7. *U.S. ex rel. Mock v. Lockheed Martin Idaho Technologies Co.*, U.S.D.C. Cause No. CIV 96-0061-E-BLW.
8. *U.S. ex rel. Carbaugh v. Westinghouse Hanford, et al.*, E.D. Wa. No. SC-96-0171-WFN.
9. *U.S. ex rel. Stone v. Rockwell International Corp.*, 144 F.R.D. 396 (D. Colo. 1992).
10. 1999 WL 428039 (Fed. Cl. June 23, 1999).
11. *See, e.g., Kaiser Aluminum & Chemical Corp. v. Catellus Development Corp.*, 976 F.2d 1338 (9th Cir. 1992); *Ganton Technologies, Inc. v. Quadion Corp.*, 834 F.Supp. 1018 (N.D. Ill. 1993).
12. *See Amtreco, Inc. v. OH Materials, Inc.*, 802 F.Supp. 443 (M.D. Ga. 1992).
13. To date, DOE has initiated 55 enforcement actions against DOE contractors and laboratories. Records of these enforcement actions may be found at http://tis.eh.doe.gov/enforce.
14. *See Bricker v. Rockwell Hanford Operations*, No. CY-90-3090-AAM, 1991 U.S. LEXIS 18965 (E.D. Wash. Sept. 17, 1991) (Judge dismissed a case brought by a former employee of Westinghouse Hanford Co. who had blown the whistle on

safety violations at the Hanford Nuclear Reservation, finding that because Section 210 amended subchapter II of the Energy Authorization Act, dealing exclusively with the NRC, it was not intended to extend to the DOE, which was governed by subchapter I of the Act).

15. *See* DEAR § 970.2274-1; DEAR § 970.7101; DEAR § 913.507.
16. *See* 57 Fed. Reg. 7541 (Mar. 3, 1992).
17. 10 CFR Part 708.5.
18. *See* 10 CFR Part 708.14, 708.10.
19. 10 CFR Part 708.12.
20. *See* 10 CFR Part 708.22, 708.25.
21. *See In re Caremark International Inc. Derivative Litigation*, 698 A.2d 959, 970 (Del. Ch. 1996).
22. *See Faragher v. City of Boca Raton*, 118 S.Ct. 2275 (1998); *Burlington Industries v. Ellerth*, 118 S.Ct. 2365 (1998).
23. 60 Fed. Reg. 66706 (Effective Jan. 22, 1996).
24. *See* 10 CFR Part 820, Appendix A.
25. *See In re Caremark International, Inc. Derivative Litigation*, 698 A.2d 959 (Del. Ch. 1996).
26. USSG § 8A1.2 comment.
27. *See Upjohn Co. v. U.S.*, 449 U.S. 383 (1981).
28. *See Hickman v. Taylor*, 329 U.S. 495 (1947).
29. *See U.S. v. Massachusetts Institute of Technology*, 129 F.3d 681 (1st Cir. 1997).
30. *See* Note, "The Privilege of Self-Critical Analysis," 96 Harv.L.Rev. 1083 (1983).
31. *See U.S. v. Dexter Corp.*, 132 F.R.D. 8 (D. Conn. 1990).
32. Although the NRC takeover from DOE of the nuclear safety oversight function seemed imminent and certain only a few years ago, this regulatory transference appears to be on a far longer-term time horizon.
33. The cost of responding to investigations and/or defending against administrative or legal proceedings may or may not be recoverable, depending on the situation.