October 1, 1979

79-73 MEMORANDUM OPINION FOR THE GENERAL COUNSEL OFFICE OF PERSONNEL MANAGEMENT

Federal Computer Systems—Access by Contractor Employees—Authority to Screen for Security Purposes (31 U.S.C. § 18a; 5 U.S.C. §§ 301, 552a; 44 U.S.C. § 3102)—Due Process

You have asked for our views concerning the authority of executive branch agencies to implement Transmittal Memorandum No. 1 to Office of Management and Budget (OMB) Circular No. A-71, dated July 27, 1978. The Transmittal Memorandum, among other things, requires Federal agencies to establish personnel security policies for screening all individuals participating in the design, operation, or maintenance of Federal computer systems or having access to data in Federal computer systems. You have asked us to confine our opinion to the question of an agency's authority to investigate and screen non-Federal employees before granting them access to unclassified information in Federal computer systems.

We conclude that Federal agencies have the authority to implement the Transmittal Memorandum by screening contractor employees[1] in any reasonable manner, but that such implementation must be consistent with due process of law.

---

[1]Although your request referred to the authority to investigate non-Federal personnel, including employees of contractors and prospective contractors, we are unaware of any non-Federal employees who would come within the purview of the Transmittal Memorandum who would not be contractor personnel. For example, the Transmittal Memorandum says (at p. 3) that "[t]hese policies should be established for government and contractor personnel."

The Transmittal Memorandum was intended to promulgate policy and define the responsibilities of various executive branch agencies for computer security. This function appears to be within the broad authority of the Director of the Office of Management and Budget to "develop improved plans for the organization, coordination, and management of the executive branch of the Government with a view to efficient and economical service." 31 U.S.C. § 18a (1976).

The memorandum makes it the responsibility of the head of each executive agency to assure an adequate level of security for all agency computer data whether processed in-house or commercially. In the area of personnel security, it requires that each agency at a minimum—

> [E]stablish personnel security policies for screening all individuals participating in the design operation or maintenance of Federal computer systems or having access to data in Federal computer systems. The level of screening required by these policies should vary from minimal checks to full background investigations commensurate with the sensitivity of the data to be handled and the risk and magnitude of loss or harm that could be caused by the individual. These policies should be established for government and contractor personnel. Personnel security policies for Federal employees should be consistent with policies issued by the Civil Service Commission. [p. 3.]

It should be noted that the memorandum contemplates a range of screening procedures varying from minimal checks to full background investigations depending upon the risk of harm and the sensitivity of the data. It may be that adequate security can be assured in many cases without an actual investigation of contractor employees. For example, in some instances submission of information or certification by the employer may be sufficient. In other cases it may be advisable to obtain verification of an employee's arrest record, or lack thereof. There will, no doubt, also be instances where a full background investigation of a contractor is warranted. The memorandum directs the head of each agency to exercise discretion in choosing a screening method to fit the circumstances of particular data-processing contracts.

We have found three statutory sources of agency authority to take action to assure the security of agency records. The head of every executive or military department has the authority to "prescribe regulations for the government of his department, the conduct of its employees, the distribution and performance of its business, and the custody, use, and preservation of its records, papers and property." 5 U.S.C. § 301 (1977). Although that section specifically notes that it does not authorize the withholding of information from the public, it does appear to authorize regulations of the sort contemplated by OMB to assure the security of data-processing records and property.

The Privacy Act of 1974 gives Federal agencies a more specific mandate. That Act was passed in response to a congressional finding that

> [t]he increasing use of computers and sophisticated information technology, while essential to the efficient operations of the Government, has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use, or dissemination of personal information * * *. [Pub. L. 93-579, § 2(a)(2), quoted at 5 U.S.C. § 552a note.]

In order to prevent such harm to individual privacy, the Privacy Act requires that each agency establish (1) rules of conduct for persons involved in the design, operation, or maintenance of any system of records; and (2) appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records. 5 U.S.C. § 552a(e) (9) and (10). Although the Privacy Act applies only to systems of records that contain information about individuals,[2] 5 U.S.C. § 552a(a), the Act does provide that an agency, consistent with its authority, shall cause the requirements of the Act to be applied to government contractors who operate a system of records to accomplish an agency function. Moreover, the employees of a contractor are to be considered employees of the agency for purposes of criminal penalties under the Act. 5 U.S.C. § 552a(m).

The head of each Federal agency is also required by 44 U.S.C. § 3102 to provide for "effective controls over the creation and over the maintenance and use of records in the conduct of current business" and in cooperation with the Administrator of General Services to "promote the maintenance and security of records deemed appropriate for preservation."[3] To the extent that computer records are involved in the current conduct of agency business or deemed appropriate for preservation, this section would provide further authority for the imposition of controls on access to computer information.

Due Process

Although we conclude that the head of a Federal agency has authority to screen contractor employees before granting them access to Federal data-processing systems, there are legal and constitutional limits to the exercise of any authority. We will discuss the application of due process to this situation because we understand that some agencies have expressed concern about *Greene* v. *McElroy,* 360 U.S. 474 (1959). In that case the Supreme Court found that the authority of the Department of Defense to screen contractor employees for work on classified projects was not specific enough to permit action that would deprive a person of his or her ability to pursue his or her chosen profession without the safeguards of confrontation and cross-examination.

---

[2]The Act defines "individual" as "a citizen of the United States or an alien lawfully admitted for permanent residence." 5 U.S.C. § 552a(a)(2).

[3]The scope of the term "records" as used in this section can be found in 44 U.S.C. § 3101. That definition appears to be sufficiently broad to encompass data-processing materials.

The plaintiff in *Greene* was an aeronautical engineer and general manager of a corporation that had defense contracts that required it to exclude from its premises persons not having security clearances. Although the plaintiff had been granted security clearances on previous occasions, he was eventually deprived of his clearance on the basis of alleged Communist associations and sympathies. He was notified of specific written allegations and was permitted to present evidence to refute the allegations at several hearings concerning the revocation of his clearance. However, he was denied access to the source of much of the information against him and was not permitted to confront or cross-examine witnesses against him. As a result of the loss of his clearance, he resigned from his position and was effectively barred from the practice of his profession. Proceeding very cautiously, the Supreme Court held that in authorizing or acquiescing in Department of Defense procedures to restrict dissemination of classified information, neither the President nor Congress intended to dispense with safeguards of confrontation or cross-examination. Accordingly, it invalidated the Defense Department procedures as beyond the scope of the agency's authority.

In a subsequent case, *Cafeteria & Restaurant Workers Union* v. *McElroy,* 367 U.S. 886 (1961), the Supreme Court distinguished and limited its holding in *Greene. Cafeteria Workers* involved a cook who was barred from her job at a naval facility upon failure to meet security requirements. Noting that the due process issue had not been resolved in *Greene*, the Court held that the Due Process Clause will be involved if an agency's action in excluding certain contractor employees is likely to result in the foreclosure of other employment for them in the data-processing field. We would suggest that in any such case the agency general counsel be consulted for more particular guidance concerning the application of due process principles.[4]

LEON ULMAN
Deputy Assistant Attorney General
Office of Legal Counsel

[4]In this connection, *see, Doe* v. *United States Civil Service Commission,* 483 F. Supp. 539 (D.S.D. N.Y. 1980).