U.S. Department of Energy
Washington, DC

ORDER

DOE O 240.1

Approved: 4-9-2024

SUBJECT: REQUESTING ACCESS TO ELECTRONIC RECORDS, ELECTRONIC COMMUNICATIONS, AND ACCESS CONTROL RECORDS

1. PURPOSE. To provide the Department of Energy (DOE) elements, including the National Nuclear Security Administration (NNSA), with uniform policies and procedures for submitting, reviewing, and approving requests to access electronic records (e.g., information stored on Government Furnished Equipment (GFE) or in an online cloud service used by the Government, such as OneDrive), electronic communications (e.g., emails, documents, websites visited, downloaded files and computer forensic information), and access control records (e.g., facility access, computer log-in information). This Order is not intended to, and does not, establish any rights on the part of any current or former Federal employees or employees of Federal contractors or subcontractors. This Order seeks to prevent abuses, including but not limited to retaliation against whistleblowers, by establishing a process for the review of electronic records and communications and access control records.

2. CANCELLATION. This Order supersedes the Deputy Secretarial Memorandum titled, "Policy for Accessing Employee Computing Records and Access Control Records," dated September 6, 2013, and the subsequent extension Deputy Secretarial Memorandum dated March 11, 2015.

3. APPLICABILITY.

   a. General. Current and former Federal employees and employees of Federal contractors and subcontractors have no reasonable expectation of privacy regarding electronic records or communications or records that transit or are stored on GFE. At login to a DOE computer system, users must acknowledge the terms of a privacy use banner that notifies them of the system and information contained therein being the property of the United States Government, and that they have no explicit or implicit expectation of privacy over their activity while using the system.

   b. Departmental Applicability. This Order applies to all DOE Elements (unless identified in Paragraph 3.d., Equivalencies/Exemptions). The NNSA Administrator must ensure that NNSA employees comply with their responsibilities under this Order. Nothing in this Order will be construed to interfere with the NNSA Administrator's authority under section 3212(d) of Public Law (P.L.) 106-65 to establish Administration-specific policies, unless disapproved by the Secretary.

   c. DOE Contractors. This Order shall apply only to contractor employees as set forth in section 4.g., below.

d. Equivalencies/Exemptions.

(1) Equivalency. In accordance with the responsibilities and authorities assigned by Executive Order 12344, codified at 50 U.S.C. Sections 2406 and 2511, and to ensure consistency through the joint Navy/DOE Naval Nuclear Propulsion Program, the Deputy Administrator for Naval Reactors (Director) will implement and oversee requirements and practices pertaining to this Order for activities under the Director's cognizance, as deemed appropriate.

(2) Exemption. Nothing in this Order shall inhibit the Office of Inspector General's (OIG) access to such records that the OIG is legally authorized access pursuant to the OIG authorities, which are enumerated in the Inspector General Act of 1978, as amended.

(3) Exemption. Nothing in this Order shall inhibit DOE Office of Intelligence and Counterintelligence (IN) from exercising its counterintelligence authorities when a request is made pursuant to IN. IN is subject to the requirements in this Order when a request is for access to employee computing and access control records that are not part of IN's exercise of its specific counterintelligence authorities.

(4) Exemption. If an employee or former employee provides written consent to conduct a search of records, no additional approval or authorization is required. However, it is recommended that the search request and the employee's written consent be submitted to the appropriate General Counsel Office (see Section 6.d.) to ensure a sufficiency.

(5) Exemption. Nothing in this Order shall inhibit Departmental efforts to access, sanitize and remove classified information from an unclassified computer system.

4. REQUIREMENTS.

a. Requests for access to computing records must clearly describe what information is sought and the reason and rationale for requesting a search. The request should be limited to only the material needed and include the time period to be searched, proposed search terms, name of the Federal employee requesting the search, name of individual(s) whose account is to be searched, and proposed search locations (e.g., emails or files). See Attachment 1, Electronic Access Data Request Template, for information that is necessary when submitting requests.

b. Access to computing records may be permissible when used:

(1) In furtherance of a demonstrable legitimate government interest, not otherwise addressed in this section.

(2) In response to a request for disclosure pursuant to statute (e.g., Freedom of Information Act Request, Privacy Act Request), regulation, Executive Order, discovery, or court-ordered production.

(3) Under reasonable suspicion that an employee is engaging in behavior that is illegal, dangerous, or in violation of a DOE Order, regulation, directive, or policy.

(4) Following an employee's unplanned and extended absence, or departure from Federal service. Whenever possible, supervisors should discuss records management and access to employee records with staff, and ensure staff complete required separation clearance form, which accounts for the custody of Federal records, prior to their departure.

c. Access to current employee computing or access control records for assessing employee performance or time and attendance is disfavored and there is a presumption against accessing these records for those purposes. Access is not a substitute for responsible workforce management. Therefore, a request for access for these purposes must clearly articulate why traditional management techniques are inadequate or have previously been unsuccessful.

d. Access to computing records on DOE computer systems may not be used to suppress or discourage or chill an employee's right to engage in union activity, protected Equal Employment Opportunity (EEO) activity, or to exercise a legal right to disclose wrongdoing without fear of retaliation, such as disclosures to the Office of Special Counsel or DOE's Inspector General. This includes the disclosure of information that the employee reasonably believes evidences a violation of any law, rule, or regulation, or gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety. A request for access to employee computing records must be evaluated to ensure that management is not engaging in retaliatory behavior or suppressing or discouraging an employee's legal rights or ability to make confidential disclosures.

e. All personal information retrieved as part of the search must be safeguarded and only disclosed when such disclosure is in furtherance of a legitimate government interest. If any personally identifiable information (PII) is inadvertently disclosed as part of the search, the recipient of such information should report the disclosure as a loss of PII under DOE O 206.1, *DOE Privacy Program*, current version, and alert the appropriate personnel so that proper follow-up measures are taken.

f. Where requests should be submitted and who has approval authority:

(1) Requests for records of DOE HQ-located employees who report to HQ (other than those in NNSA or OIG), DOE employees in field locations who obtain their legal support directly from the HQ Office of the General Counsel, or Field Chief Counsel or Power Marketing Administration Counsel employees.

(a) Requests should be submitted to the Associate General Counsel for Finance and Information Law.

(b) Authority to approve access is limited to the General Counsel, Deputy General Counsel, Deputy General Counsel for General Law and the Associate General Counsel for Finance and Information Law. This authority cannot be redelegated except by the General Counsel.

(2) Requests for DOE field records (other than those in NNSA or OIG)

(a) Requests should be submitted to the Chief Counsel or Deputy Chief Counsel responsible for providing legal services for the applicable DOE field office.

(b) Authority to approve access is limited to the Chief Counsel and Deputy Chief Counsel and cannot be redelegated.

(3) Requests for NNSA Headquarters records, NNSA employees in locations that obtain their legal support directly from NNSA Office of General Counsel, or records for an employee of an NNSA Field Counsel office.

(a) Requests must be submitted to the NNSA General Counsel or the NNSA Deputy General Counsel for General Law and Litigation.

(b) Authority to approve access is limited to NNSA General Counsel and the Deputy General Counsel for General Law and Litigation and cannot be redelegated.

(4) Requests for NNSA field records, except for NNSA Field Counsel employee records.

(a) Requests must be submitted to the Office of the Field Counsel for the appropriate NNSA field office.

(b) Authority to approve access is limited to the Field Counsel for the field office and cannot be redelegated.

(5) Requests for Power Marketing Administration (PMA)

(a) Must be submitted to the General Counsel for the PMA or a single designated supervisory attorney responsible for providing legal services for the applicable PMA.

(b) Authority to approve access is limited to the General Counsel and one designee supervisory attorney and cannot be redelegated.

(6) Requests for OIG records, regardless of the location or network.

(a) Must be submitted to the OIG Office of Counsel or the OIG Office of Investigations.

(b) Access to OIG computing or access control records is not permissible without express written authorization of the Chief Counsel to the Inspector General or the Assistant Inspector General for Investigations and can be redelegated to a single designated attorney.

g. While this Order does not apply to contractor-owned records, it does apply to Federal records on a DOE-controlled system. Therefore, any records created or held by contractor employees that are located on a DOE-owned and controlled records system may be accessed pursuant to this Order.

5. RESPONSIBILITIES.

a. DOE Office of the General Counsel (DOE GC)/ NNSA Office of General Counsel (NA-GC)/ DOE Field Counsels/ NNSA Field Counsels/ PMA Designated Supervisory Attorney/ OIG Office of Counsel and OIG Office of Investigations. Review requests for access to computing and access control records. If approved, the requester submits the search request to the appropriate entity for search.

b. Designated Office that Provides IT Support for Records Being Searched. Provide access to computing records upon receipt of an approved request. Such access must be limited to the specific information included in the approved request and provided only to those specified in the approved request.

d. Facility Security Officers. Provide access to access control records upon receipt of an approved request. Such access must be limited to the specified time period included in the approved request and provided only to those specified in the approved request.

e. Requesters. Submit requests for access to computing and access control records to the following:

(1) DOE HQ: GCInformationRequests@hq.doe.gov.

(2) NNSA: Please contact the NNSA Office of the General Counsel.

(3) PMA: Please contact your General Counsel's Office.

(4) DOE Field Offices: Please contact your Field Counsel's Office.

(5) NNSA Field Offices: Please contact your Field Counsel's Office.

(6) OIG: Please contact the OIG's Office of Counsel or the OIG's Office of Investigations.

6. INVOKED STANDARDS. This Order does not invoke any DOE technical standards or industry standards as required methods. Note: DOE O 251.1, current version, provides a definition for "invoked technical standard."

7. DEFINITIONS.

a. Access Control Records refers to records created to track facility access and computer log-in information.

b. Computing Records refers to records that are generated by or stored in Government computer systems.

c. Government Furnished Equipment (GFE) refers to property owned by the Government and furnished to a contractor or employee for the performance of their duties.

d. Record includes all recorded information, regardless of form or characteristics, made or received by a Federal agency under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the United States Government or because of the informational value of data in them. For more information on records, please refer to DOE Order 243.1C, Records Management Program.

8. CONTACT. Questions concerning this Order should be addressed to the Office of the Deputy General Counsel for General Law (GC-20) at GCInformationRequests@hq.doe.gov.

BY ORDER OF THE SECRETARY OF ENERGY:

DAVID M. TURK
Deputy Secretary

APPENDIX A

ELECTRONIC DATA ACCESS REQUEST

A. Nature of Request
   1. Freedom of Information Act (attach copy of FOIA request)
   2. Privacy Act Request (attach copy of PA request)
   3. Other External Request (e.g., court order, litigation discovery, Congressional inquiry -- attach copy of request)
   4. Internal investigation (describe)
   5. Other Work-Related Purposes (describe)

B. Data Requested
   1. Full Name of Person Possessing Records at Issue
   2. Federal or Contractor
   3. Position Title
   4. Program Office/Company
   5. Organizational Code
   6. Separated/Transferred/Current
   7. DOE Email Address
   8. Date Needed

C. Data Scope
   1. Files/Systems Location
   2. Files/Systems Titles
   3. Inclusive Date Ranges
   4. Data Format Requested
   5. Search terms (if applicable)
   6. Program Office
   7. Organizational Code
   8. Justification

D. Federal Supervisory Manager
   1. Name
   2. Position Title
   3. Program Office
   4. Organizational Code
   5. Office Phone Number
   6. Alternate Phone Number (optional)