SYSTEM NAME AND NUMBER:

Office of the Inspector General (OIG) Investigative Records—NRC and Defense Nuclear Facilities Safety Board (DNFSB) – NRC 18.

SECURITY CLASSIFICATION:

Unclassified

SYSTEM LOCATION:

Office of the Inspector General, NRC, One White Flint North, 11555 Rockville Pike, Rockville, Maryland

SYSTEM MANAGER(S):

Assistant Inspector General for Investigations, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Inspector General Act of 1978, as amended, 5 U.S.C. 401-424; and the Consolidated Appropriations Act, 2014.

PURPOSE(S) OF THE SYSTEM:

NRC OIG uses records and information collected and maintained in this system to receive and adjudicate allegations/complaints of violations of criminal, civil, and administrative laws and regulations relating to NRC programs, operations, and employees, as well as contractors and other individuals and entities associated with NRC; monitor complaint and investigation assignments, status, disposition, and results; manage investigations and information provided during the course of such investigations; track and assess actions taken by NRC management regarding employee misconduct and other allegations; support and assess legal actions taken following referrals for criminal prosecution or litigation; provide information relating to any adverse action or other proceeding that may occur as a result of the findings of an investigation.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Individuals and entities referred to in complaints or actual investigative cases, reports, accompanying documents, and correspondence prepared by, compiled by, or referred to the OIG.

CATEGORIES OF RECORDS IN THE SYSTEM:

The system comprises five parts: (1) An automated Investigative Database Program containing reports of investigations, inquiries, and other reports closed since 1989; (2) paper files of all OIG and predecessor Office of Inspector and Auditor (OIA) reports, correspondence, cases, matters, memoranda, materials, legal papers, evidence, exhibits, data, and work papers pertaining to all closed and pending investigations, inquiries, and other reports; (3) an automated Investigative Management System that includes allegations referred to the OIG from 1985 forward, whether or not the allegation progressed to an investigation, inquiry or other report, and dates that an investigation, inquiry or other report was opened and closed and reports, correspondence, cases, matters, memoranda, materials, legal papers, evidence, exhibits, data and work papers pertaining to these cases.

RECORD SOURCE CATEGORIES:

The information is obtained from sources including, but not limited to, the individual record subject; NRC officials and employees; employees of Federal, State, local, and foreign agencies; and other persons.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

In addition to the other types of disclosures permitted under subsection (b) of the Privacy Act, OIG may disclose information contained in this system of records without the consent of the subject individual if the disclosure is compatible with the purpose for which the record was collected under the following routine uses:

a. To any Federal, State, local, tribal, or foreign agency, or other public authority responsible for enforcing, investigating, or prosecuting violations of administrative, civil, or

criminal law or regulation if that information is relevant to any enforcement, regulatory, investigative, or prosecutorial responsibility of the receiving entity when records from this system of records, either by themselves or in combination with any other information, indicate a violation or potential violation of law, whether administrative, civil, criminal, or regulatory in nature;

b. To public or private sources to the extent necessary to obtain information from those sources relevant to an OIG investigation, audit, inspection, or other inquiry;

c. To a court, adjudicative body before which NRC or DNFSB is authorized to appear, Federal agency, individual or entity designated by NRC or DNFSB or otherwise empowered to resolve disputes, counsel or other representative, or witness or potential witness when it is relevant and necessary to the litigation if any of the parties listed below is involved in the litigation or has an interest in the litigation:

1. NRC or DNFSB, or any component of NRC or DNFSB;

2. Any employee of NRC or DNFSB where the NRC or DNFSB or the Department of Justice has agreed to represent the employee; or

3. The United States, where NRC or DNFSB determines that the litigation is likely to affect the NRC or DNFSB or any of their components;

d. To a private firm or other entity with which OIG or NRC or DNFSB contemplates it will contract or has contracted for the purpose of performing any functions or analyses that facilitate or are relevant to an investigation, audit, inspection, inquiry, or other activity related to this system of records, to include to contractors or entities who have a need for such information or records to resolve or support payment to the agency. The contractor, private firm, or entity needing access to the records to perform the activity shall maintain Privacy Act safeguards with respect to information. A contractor, private firm, or entity operating a system of records under 5 U.S.C. 552a(m) shall comply with the Privacy Act;

e. To another agency to the extent necessary for obtaining its advice on any matter

relevant to an OIG investigation, audit, inspection, or other inquiry related to the responsibilities of the OIG;

f. To the National Archives and Records Administration or to the General Services Administration for records management inspections conducted under 44 U.S.C. 2904 and 2906;

g. A record from this system of records which indicates a violation of civil or criminal law, regulation or order may be referred as a routine use to a Federal, State, local or foreign agency that has authority to investigate, enforce, implement or prosecute such laws. Further, a record from this system of records may be disclosed for civil or criminal law or regulatory enforcement purposes to another agency in response to a written request from that agency's head or an official who has been delegated such authority;

h. A record from this system of records may be disclosed as a routine use to a Federal, State, local, or foreign agency to obtain information relevant to an NRC decision concerning hiring or retaining an employee, letting a contract, or issuing a security clearance, license, grant or other benefit;

i. A record from this system of records may be disclosed as a routine use to a Federal, State, local, or foreign agency requesting a record that is relevant and necessary to its decision on a matter of hiring or retaining an employee, issuing a security clearance, reporting an investigation of an employee, letting a contract, or issuing a license, grant, or other benefit;

j. A record from this system of records may be disclosed as a routine use in the course of discovery; in presenting evidence to a court, magistrate, administrative tribunal, or grand jury or pursuant to a qualifying order from any of those; in alternative dispute resolution proceedings, such as arbitration or mediation; or in the course of settlement negotiations;

k. A record from this system of records may be disclosed as a routine use to a Congressional office from the record of an individual in response to an inquiry from the Congressional office made at the request of that individual;

l. A record from this system of records may be disclosed as a routine use to NRC-

paid experts or consultants, and those under contract with the NRC on a "need-to-know" basis for a purpose within the scope of the pertinent NRC task. This access will be granted to an NRC contractor or employee of such contractor by a system manager only after satisfactory justification has been provided to the system manager;

m. A record from this system of records may be disclosed as a routine use to appropriate agencies, entities, and persons when (1) NRC suspects or has confirmed that there has been a breach of the system of records, (2) NRC has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, NRC (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with NRC efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm; and

n. A record from this system of records may be disclosed as a routine use to another Federal agency or Federal entity, when the NRC determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Information is maintained in paper files and on electronic media.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Information is retrieved from the Investigative Database Program by the name of an individual, by case number, or by subject matter. Information in the paper files backing up the Investigative Database Program and older cases closed by 1989 is retrieved by subject matter and/or case number, not by individual identifier. Information in both the Allegations Tracking

System and the Investigative Management System is retrieved by allegation number, case number, or name.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Records are retained according to the National Archives and Records Administration's approved schedule for the Office of the Inspector General, N1-431-10-002, item 2.b, Investigation Case Files. Cut off at close of fiscal year in which the case is closed. Transfer to the Federal Records Center (FRC) 3 years after cutoff. Transfer to National Archives and Records Administration 20 years after cutoff. Retain an electronic copy until no longer needed (Allegation records will be managed in the corresponding Investigation Case File).

Referred Allegations are retained under the National Archives and Records Administration's approved schedule, N1-431-10-002, item 2.a.ii. Cut off allegation file at the end of the fiscal year when the issue described in the Referral Letter is resolved. Hold allegation file in the OIG for a minimum of 2 years after cutoff. Destroy 10 years after cutoff.

Closed Allegations are retained under the National Archives and Records Administration's approved schedule, N1-431-10-002, item 2.a.iii. Cut off allegation files at the end if the fiscal year in which the allegation is closed. Destroy the allegation file 5 years after cutoff.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Access to the automated Investigative Database Program is password protected. Both the Allegations Tracking System and the Investigative Management System are accessible from terminals that are double-password-protected. Paper files backing up the automated systems and older case reports and work papers are maintained in approved security containers and locked filing cabinets in a locked room; associated indices, records, diskettes, tapes, etc., are stored in locked metal filing cabinets, safes, storage rooms, or similar secure facilities. All records in this system are available only to authorized personnel who have a need to know and whose duties require access to the information.

RECORD ACCESS PROCEDURES:

Same as "Notification procedures." Information classified under Executive Order 12958 will not be disclosed. Information received in confidence will be maintained under the Inspector General Act, 5 U.S.C. 401-424, and the Commission's Policy Statement on Confidentiality, Management Directive 8.8, "Management of Allegations."

CONTESTING RECORD PROCEDURES:

Same as "Notification procedures."

NOTIFICATION PROCEDURES:

Individuals seeking to determine whether this system of records contains information about them should write to the Freedom of Information Act or Privacy Act Officer, Office of the Chief Information Officer, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001, and comply with the procedures contained in NRC's Privacy Act regulations, 10 CFR part 9.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

Under 5 U.S.C. 552a(j)(2), the Commission has exempted this system of records from subsections (c)(3) and (4), (d)(1)-(4), (e)(1)-(3), (5), and (8), and (g) of the Act. This exemption applies to information in the system that relates to criminal law enforcement and meets the criteria of the (j)(2) exemption. Under 5 U.S.C. 552a(k)(1), (k)(2), (k)(5), and (k)(6), the Commission has exempted portions of this system of records from 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (H), and (I), and (f).

DISCLOSURE TO CONSUMER REPORTING AGENCIES:

Disclosure Pursuant to 5 U.S.C. 552a(b)(13):

Disclosure of information to a consumer reporting agency is not considered a routine use of records. Disclosures may be made from this system to "consumer reporting agencies" as defined in the Fair Credit Reporting Act (15 U.S.C. 1681a(f) (1970)) or the Federal Claims Collection Act of 1966, as amended (31 U.S.C. 3701(a)(3) (1996)).