
Once a participant has obtained a digital ID certificate and a docket has been created, the participant can then submit a request for hearing or petition for leave to intervene. Submissions should be in Portable Document Format (PDF) in accordance with NRC guidance available on the NRC public Web site at http://www.nrc.gov/site-help/e-submittals.html. A filing is considered complete at the time the documents are submitted through the NRC’s E-Filing system. To be timely, an electronic filing must be submitted to the E-Filing system no later than 11:59 p.m. Eastern Time on the due date. Upon receipt of a transmission, the E-Filing system time-stamps the document and sends the submitter an email notice confirming receipt of the document. The E-Filing system also distributes an email notice that provides access to the document to the NRC’s Office of the General Counsel and any others who have advised the Office of the Secretary that they wish to participate in the proceeding, so that the filer need not serve the documents on those participants separately. Therefore, applicants and other participants (or their counsel or representative) must apply for and receive a digital ID certificate before a hearing request/petition to intervene is filed so that they can obtain access to the document via the E-Filing system.

A person filing electronically using the agency’s adjudicatory E-Filing system may seek assistance by contacting the NRC’s Meta System Help Desk through the “Contact Us” link located on the NRC’s public Web site at http://www.nrc.gov/site-help/e-submittals.html, by email at MSHD.Resource@nrc.gov, or by a toll-free call at 1–866–672–7640. The NRC Meta System Help Desk is available between 8 a.m. and 8 p.m., Eastern Time, Monday through Friday, excluding government holidays. Participants who believe that they have a good cause for not submitting documents electronically must file an exemption request, in accordance with 10 CFR 2.302(g), with their initial paper filing requesting authorization to continue to submit documents in paper format. Such filings must be submitted by: (1) First class mail addressed to the Office of the Secretary of the Commission, U.S. Nuclear Regulatory Commission, Washington, DC 20555–0001, Attention: Rulemaking and Adjudications Staff; or (2) courier, express mail, or expedited delivery service to the Office of the Secretary,

Sixteenth Floor, One White Flint North, 11555 Rockville Pike, Rockville, Maryland, 20852, Attention: Rulemaking and Adjudications Staff. Participants filing a document in this manner are responsible for serving the document on all other participants. Filing is considered complete by first-class mail as of the time of deposit in the mail, or by courier, express mail, or expedited delivery service upon depositing the document with the provider of the service. A presiding officer, having granted an exemption request from using E-Filing, may require a participant or party to use E-Filing if the presiding officer subsequently determines that the reason for granting the exemption from use of E-Filing no longer exists.

Documents submitted in adjudicatory proceedings will appear in NRC’s electronic hearing docket which is available to the public at http://ehd1.nrc.gov/ehd/, unless excluded pursuant to an order of the Commission, or the presiding officer. Participants are requested not to include personal privacy information, such as social security numbers, home addresses, or home phone numbers in their filings, unless an NRC regulation or other law requires submission of such information. With respect to copyrighted works, except for limited excerpts that serve the purpose of the adjudicatory filings and would constitute a Fair Use application, participants are requested not to include copyrighted materials in their submission.

IV. Opportunity To Provide Written Comments

Within 30 days from the date of publication of this notice, persons may submit written comments regarding the CA transfer application, as provided for in 10 CFR 2.1305. The NRC will consider and, if appropriate, respond to these comments, but such comments will not otherwise constitute part of the decisional record. Comments should be submitted to the Secretary, U.S. Nuclear Regulatory Commission, Washington, DC 20555–0001, Attention: Rulemakings and Adjudications Staff, and should cite the publication date and page number of this Federal Register notice. Comments received after 30 days will be considered if practicable to do so, but only those comments received on or before the due date can be assured consideration.

For further details with respect to this CA transfer application, see the application dated August 30, 2012. Publicly-available records will be accessible electronically from the Agency Wide Documents Access and Management System’s (ADAMS) Public Electronic Reading Room on the Internet at the NRC Web site http://www.nrc.gov/reading-rm/adams.html. Persons who do not have access to ADAMS or who encounter problems in accessing the documents located in ADAMS should contact the NRC PDR Reference staff by telephone at 1–800–397–4209, or 301–415–4737 or by email to pdr.resource@nrc.gov.

Dated at Rockville, Maryland, this 17th day of October, 2012.

For the Nuclear Regulatory Commission.

David H. Tiktinsky,
Senior Project Manager, Mixed Oxide and Deconversion Branch, Division of Fuel Cycle Safety and Safeguards, Office of Nuclear Material Safety and Safeguards.

[FR Doc. 2012–26300 Filed 10–24–12; 8:45 am]

BILLING CODE 7590–01–P

NUCLEAR REGULATORY COMMISSION

[NRC–2012–0255; EA–12–148]

In the Matter of Licensee Identified in Attachment 1 and all Other Persons Who Seek or Obtain Access to Safeguards Information Described Herein; Order Imposing Fingerprinting and Criminal History Records Check Requirements for Access to Safeguards Information (Effective Immediately)

I

The Licensee identified in Attachment 1 to this Order, holds a license issued in accordance with the Atomic Energy Act (AEA) of 1954, as amended, by the U.S. Nuclear Regulatory Commission (NRC or the Commission), authorizing them to engage in an activity subject to regulation by the Commission or Agreement States. In accordance with Section 149 of the AEA, fingerprinting and a Federal Bureau of Investigation (FBI) identification and criminal history records check are required of any person who is to be permitted to have access to Safeguards Information (SGI).2 The AEA permits the Commission by rule to except certain categories of individuals from the fingerprinting requirement, which the Commission has done (see 10 CFR 73.59, 71 FR 33989; June 13, 2006). Individuals relieved from fingerprinting and criminal history records checks

1 Attachment 1 contains sensitive information and will not be released to the public.

2 Safeguards Information is a form of sensitive, unclassified, security-related information that the Commission has the authority to designate and protect under section 147 of the AEA.
under the relief rule include Federal, State, and local officials and law enforcement personnel; Agreement State inspectors who conduct security inspections on behalf of the NRC; members of Congress and certain employees of members of Congress or Congressional Committees, and representatives of the International Atomic Energy Agency (IAEA) or certain foreign government organizations. In addition, individuals who have a favorably-decided U.S. Government criminal history records check within the last five (5) years, or individuals who have active Federal security clearances (provided in either case that they make available the appropriate documentation), have satisfied the AEA fingerprinting requirement and need not be fingerprinted again. Therefore, in accordance with Section 149 of the AEA the Commission is imposing additional requirements for access to SGI, as set forth by this Order, so that affected licensees can obtain and grant access to SGI. This Order also imposes requirements for access to SGI by any person, from any person,\(^3\) whether or not a Licensee, Applicant, or Certificate Holder of the Commission or Agreement States.

II

The Commission has broad statutory authority to protect and prohibit the unauthorized disclosure of SGI. Section 147 of the AEA grants the Commission explicit authority to issue such Orders as necessary to prohibit the unauthorized disclosure of SGI. Furthermore, Section 149 of the AEA requires fingerprinting and an FBI identification and a criminal history records check of each individual who seeks access to SGI. In addition, no person may have access to SGI unless the person has an established need-to-know the information and satisfies the trustworthy and reliability requirements described in Attachment 3 to Order EA–12–147.

In order to provide assurance that the Licensee identified in Attachment 1 to this Order is implementing appropriate measures to comply with the

---

3 Person means (1) any individual, corporation, partnership, trust, estate, public or private institution, group, governmental agency or other than the Commission or the Department of Energy, except that the Department of Energy shall be considered a person with respect to those facilities of the Department of Energy specified in section 202 of the Energy Reorganization Act of 1974 (88 Stat. 1244), any State or any political subdivision of, or any political entity within a State, any foreign government or nation or any political subdivision of any such government or nation, or other entity; and (2) any legal successor, representative, agent, or agency of the foregoing.

---

2. The Licensee shall, within twenty (20) days of the date of this Order, submit the fingerprints of one (1) individual who a) the Licensee nominates as the “reviewing official” for determining access to SGI by other individuals, and b) has an established need-to-know the information and has been determined to be trustworthy and reliable in accordance with the requirements described in Attachment 3 to Order EA–12–147. The NRC will determine whether this individual (or any subsequent reviewing official) may have access to SGI and, therefore, will be permitted to serve as the Licensee’s reviewing official.\(^4\) The Licensee may, at the same time or later, submit the fingerprints of other individuals to whom the Licensee seeks to grant access to SGI or designate an additional reviewing official(s). Fingerprints shall be submitted and reviewed in accordance with the procedures described in Attachment 2 of this Order.

3. The Licensee shall, in writing, within twenty (20) days of the date of this Order, notify the Commission, (1) if it is unable to comply with any of the requirements described in this Order, including Attachment 2 to this Order, or (2) if compliance with any of the requirements is unnecessary in its specific circumstances. The notification shall provide the Licensee’s justification for seeking relief from or variation of any specific requirement.


The Director, Office of Federal and State Materials and Environmental Management Programs, may, in writing, relax or rescind any of the above conditions upon demonstration of good cause by the Licensee.

IV

In accordance with 10 CFR 2.202, the Licensee must, and any other person adversely affected by this Order may, submit an answer to this Order within twenty (20) days of the date of this Order. In addition, the Licensee and any other person adversely affected by this Order may request a hearing of this Order within twenty (20) days of the

4 The NRC’s determination of this individual’s access to SGI in accordance with the process described in Enclosure 5 to the transmittal letter of this Order is an administrative determination that is outside the scope of this Order.
date of the Order. Where good cause is shown, consideration will be given to extending the time to request a hearing. A request for extension of time must be made, in writing, to the Director, Office of Federal and State Materials and Environmental Management Programs, U.S. Nuclear Regulatory Commission, Washington, DC 20555–0001, and include a statement of good cause for the extension.

The answer may consent to this Order. If the answer includes a request for a hearing, it shall, under oath or affirmation, specifically set forth the matters of fact and law on which the Licensee relies and the reasons as to why the Order should not have been issued. If a person other than the Licensee requests a hearing, that person shall set forth with particularity the manner in which his interest is adversely affected by this Order and shall address the criteria set forth in 10 CFR 2.309(d).

All documents filed in the NRC adjudicatory proceedings, including a request for hearing, a petition for leave to intervene, any motion or other document filed in the proceeding prior to the submission of a request for hearing or petition to intervene, and documents filed by interested governmental entities participating under 10 CFR 2.315(c), must be filed in accordance with the NRC’s E-Filing rule (72 FR 49139; August 28, 2007). The E-Filing process requires participants to submit electronic documents through the Electronic Information Exchange System, users will be required to install a Web browser plug-in from the NRC’s Web site. Further information on the Web-based submission form, including the installation of the Web browser plug-in, is available on the NRC’s public Web site at http://www.nrc.gov/site-help/e-submittals.html.

Once a participant has obtained a digital ID certificate and a docket has been created, the participant can then submit a request for hearing or petition for leave to intervene. Submissions should be in Portable Document Format (PDF) in accordance with the NRC guidance available on the NRC’s Web site at http://www.nrc.gov/site-help/e-submittals.html. A filing is considered complete at the time the documents are submitted through the NRC’s E-Filing system. To be timely, an electronic filing must be submitted to the E-Submittal server no later than 11:59 p.m. Eastern Time, Monday through Friday, excluding government holidays.

Participants who believe that they have a good cause for not submitting documents electronically must file an exemption request, in accordance with 10 CFR 2.302(g), with their initial paper filing requesting authorization to continue to submit documents in paper format. Such filings must be submitted by: (1) First class mail addressed to the Office of the Secretary, U.S. Nuclear Regulatory Commission, Washington, DC 20555–0001, Attention: Rulemaking and Adjudications Staff; or (2) courier, express mail, or expedited delivery service to the Office of the Secretary, Sixteenth Floor, One White Flint North, 11555 Rockville Pike, Rockville, Maryland 20852, Attention: Rulemaking and Adjudications Staff. Participants filing a document in this manner are responsible for serving the document on all other participants. Filing is considered complete by first-class mail as of the time of deposit in the mail, or by courier, express mail, or expedited delivery service upon depositing the document with the provider of the service. A presiding officer, having granted an exemption request from using E-Filing, may require a participant or party to use E-Filing if the presiding officer subsequently determines that the reason for granting the exemption from use of E-Filing no longer exists.

Documents submitted in adjudicatory proceedings will appear in the NRC’s electronic hearing docket which is available to the public at http://ehd1.nrc.gov/ehd/, unless excluded pursuant to an order of the Commission, or the presiding officer. Participants are requested not to include personal privacy information, such as social security numbers, home addresses, or home phone numbers in their filings, unless an NRC regulation or other law requires submission of such information.

For copyrighted works, except for limited excerpts that serve the purpose of the
judicially filed filings and would constitute a Fair Use application, participants are requested not to include copyrighted materials in their submission.

If a hearing is requested by the Licensee or a person whose interest is adversely affected, the Commission will issue an Order designating the time and place of any hearing. If a hearing is held the issue to be considered at such hearing shall be whether this Order should be sustained.

Pursuant to 10 CFR 2.202(c)(2)(i), the Licensee may, in addition to requesting a hearing, at the time the answer is filed or sooner, move the presiding officer to set aside the immediate effectiveness of the Order on the ground that the Order, including the need for immediate effectiveness, is not based on adequate evidence but on mere suspicion, unfounded allegations, or error.

In the absence of any request for hearing, or written approval of an extension of time in which to request a hearing, the provisions specified in Section III above shall be final twenty (20) days from the date of this Order without further order or proceedings. If an extension of time for requesting a hearing has been approved, the provisions specified in Section III shall be final when the extension expires if a hearing request has not been received. AN ANSWER OR A REQUEST FOR HEARING SHALL NOT STAY THE IMMEDIATE EFFECTIVENESS OF THIS ORDER.

Dated at Rockville, Maryland, this 16th day of October, 2012.

For the Nuclear Regulatory Commission.

Mark A. Satorius,
Director, Office of Federal and State Materials and Environmental Management Programs.

Attachment 1: Applicable Materials
Licensees Redacted

Attachment 2: Requirements for Fingerprinting and Criminal History Records Checks of Individuals When Licensee’s Reviewing Official is Determining Access to Safeguards Information

General Requirements

Licensees shall comply with the requirements of this attachment.

1. Each Licensee subject to the provisions of this attachment shall fingerprint each individual who is seeking or permitted access to Safeguards Information (SGI). The Licensee shall review and use the information received from the Federal Bureau of Investigation (FBI) and ensure that the provisions contained in the subject Order and this attachment are satisfied.

2. The Licensee shall notify each affected individual that the fingerprints will be used to secure a review of his/her criminal history record and inform the individual of the procedures for revising the record or including an explanation in the record, as specified in the “Right to Correct and Complete Information” section of this attachment.

3. Fingerprints need not be taken if an employed individual (e.g., a Licensee employee, contractor, manufacturer, or supplier) is relieved from the fingerprinting requirement by 10 CFR 73.59, has a favorably-decided U.S. Government criminal history records check within the last five (5) years, or has an active Federal security clearance. Written certification from the Agency/employer which granted the Federal security clearance or reviewed the criminal history records check must be provided. The Licensee must retain this documentation for a period of three (3) years from the date the individual no longer requires access to SGI associated with the Licensee’s activities.

4. All fingerprints obtained by the Licensee pursuant to this Order must be submitted to the Commission for transmission to the FBI.

5. The Licensee shall review the information provided by the FBI and consider it, in conjunction with the trustworthy and reliability requirements included in Attachment 3 to NRC Order EA–08–161, in making a determination whether to grant access to SGI to individuals who have a need-to-know the SGI.

6. The Licensee shall use any information obtained as part of a criminal history records check solely for the purpose of determining an individual’s suitability for access to SGI.

7. The Licensee shall document the basis for its determination whether to grant access to SGI.

8. The Licensee shall notify the NRC of any desired change in reviewing officials. The NRC will determine whether the individual nominated as the new reviewing official may have access to SGI based on a previously-obtained or new criminal history check and, therefore, will be permitted to serve as the Licensee’s reviewing official.

Prohibitions

A Licensee shall not base a final determination to deny an individual access to SGI solely on the basis of information received from the FBI involving: An arrest more than one (1) year old for which there is no information of the disposition of the case, or an arrest that resulted in dismissal of the charge.

A Licensee shall not use information received from a criminal history check obtained pursuant to this Order in a manner that would infringe upon the rights of any individual under the First Amendment to the Constitution of the United States, nor shall the Licensee use the information in any way which would discriminate among individuals on the basis of race, religion, national origin, sex, or age.

Procedures for Processing Fingerprint Checks

For the purpose of complying with this Order, Licensees shall, using an appropriate method listed in 10 CFR 73.4, submit to the NRC’s Division of Facilities and Security, Mail Stop T–6E46, one completed, legible standard fingerprint card (form FD–258, OR113NRC00467Z) or, where practicable, other fingerprint records for each individual seeking access to Safeguards Information, to the Director of the Division of Facilities and Security, marked for the attention of the Division’s Criminal History Check Section. Copies of these forms may be obtained by writing the Office of Information Services, U.S. Nuclear Regulatory Commission, Washington, DC 20555–0001, by calling 301–415–7232, or by email to forms.resource@nrc.gov. Practicable alternative formats are set forth in 10 CFR 73.4. The Licensee shall establish procedures to ensure that the quality of the fingerprints taken results in minimizing the rejection rate of fingerprint cards due to illegible or incomplete cards.

The NRC will review submitted fingerprint cards for completeness. Any Form FD–258 fingerprint record containing emissions or evident errors will be returned to the Licensee for corrections. The fee for processing fingerprint checks includes one re-submission if the initial submission is returned by the FBI because the fingerprint impressions cannot be classified. The one free re-submission must have the FBI Transaction Control Number reflected on the re-submission. If additional submissions are necessary, they will be treated as initial submittals and will require a second payment of the processing fee.

Fees for processing fingerprint checks are due upon application. Licensees shall submit payment with the application for processing fingerprints by corporate check, certified check, cashier’s check, or money order, made payable to “U.S. NRC.” [For guidance on making electronic payments, contact the Facilities Security Branch, Division of Facilities and Security, at 301–415–7404.] Combined payment for multiple applications is acceptable. The application fee (currently $36) is the sum of the user fee charged by the FBI for each fingerprint card or other fingerprint record submitted by the NRC on behalf of a Licensee, and an NRC processing fee, which covers administrative costs associated with NRC handling of Licensee fingerprint submissions. The Commission will directly notify Licensees who are subject to this regulation of any fee changes. The Commission will forward to the submitting Licensee all data received from the FBI as a result of the Licensee’s application(s) for criminal history records checks, including the FBI fingerprint record.

Right To Correct and Complete Information

Prior to any final adverse determination, the Licensee shall make available to the individual the contents of any criminal records obtained from the FBI for the purpose of assuring correct and complete information. Written confirmation by the individual of receipt of this notification must be maintained by the Licensee for a period of one (1) year from the date of the notification. If, after reviewing the record, an individual believes that it is incorrect or incomplete in any respect and wishes to change, correct, or update the alleged deficiency, or to explain any matter in the record, the individual may initiate challenge procedures. These procedures include either direct application by the individual challenging the record to
the agency (i.e., law enforcement agency) that contributed the questioned information, or
direct challenge as to the accuracy or
completeness of any entry on the criminal
history record to the Assistant Director,
Federal Bureau of Investigation Identification
Division, Washington, DC 20537–9700 (as set
forth in 28 CFR 16.30 through 16.34). In the
latter case, the FBI forwards the challenge
to the agency that submitted the data and
requests that agency to verify or correct the
challenged entry. Upon receipt of an official
communication directly from the agency that
contributed the original information, the FBI
Identification Division makes any changes
necessary in accordance with the information
supplied by that agency. The Licensee must
provide at least ten (10) days for an
individual to initiate an action challenging
the results of an FBI criminal history records
check after the record is made available for
his/her review. The Licensee may make a
final SGI access determination based upon
the criminal history record only upon receipt
of the FBI’s ultimate confirmation or
correction of the record. Upon a final adverse
determination on access to SGI, the Licensee
shall provide the individual its documented
basis for denial. Access to SGI shall not be
granted to an individual during the review
process.

Protection of Information
1. Each Licensee who obtains a criminal
history record on an individual pursuant to
this Order shall establish and maintain a
system of files and procedures for protecting
the record and the personal information from
unauthorized disclosure.
2. The Licensee may not disclose the
record or personal information collected and
maintained to persons other than the subject
individual, his/her representative, or to those
who have a need to access the information in
performing assigned duties in the process of
determining access to Safeguards
Information. No individual authorized to
have access to the information may re-
disseminate the information to any other
individual who does not have a need-to-
know.
3. The personal information obtained on an
individual from a criminal history record
check may be transferred to another Licensee
if the Licensee holding the criminal history
record check receives the individual’s
written request to re-disseminate the
information contained in his/her file, and the
gaining Licensee verifies information such as
the individual’s name, date of birth, social
security number, sex, and other applicable
physical characteristics for identification
purposes.
4. The Licensee shall make criminal
history records, obtained under this section,
available for examination by an authorized
representative of the NRC to determine
compliance with the regulations and laws.
5. The Licensee shall retain all fingerprint
and criminal history records received from
the FBI, or a copy if the individual’s file has
been transferred, for three (3) years after
termination of employment or determination
of access to SGI (whether access was
approved or denied). After the required three
(3) year period, these documents shall be
destroyed by a method that will prevent
reconstruction of the information in whole or
in part.

Guidance for Licensee’s Evaluation of
Access to Safeguards Information With
the Inclusion of Criminal History Records
(Fingerprint) Checks
When a Licensee submits fingerprints to
the NRC pursuant to an NRC Order, it will
receive a criminal history summary of
information, provided in Federal records,
since the individual’s eighteenth birthday.
Individuals retain the right to correct and
complete information and to initiate
challenge procedures described in
Attachment 2 of Enclosure 1. The Licensee
will receive the information from the
criminal history records check of those
individuals requiring access to Safeguards
Information, and the reviewing official
should evaluate that information using the
guidance below. Furthermore, the
requirements of all Orders which apply to the
information and material to which access is
being granted must be met.

The Licensee’s reviewing official is
required to evaluate all pertinent and
available information in making a
determination of access to SGI, including the
criminal history information pertaining to the
individual as required by the NRC Order. The
criminal history records check is used in the
determination of whether the individual has
a record of criminal activity that indicates
that the individual should not have access to
SGI. Each determination of access to SGI,
which includes a review of criminal history
information, must be documented to include
the basis for the decision made.
(i) If negative information is discovered
that was not provided by the individual, or
which is different in any material respect
from the information provided by the
individual, this information should be
considered, and decisions made based on
these findings, must be documented.
(ii) Any record containing a pattern of
behaviors which indicates that the behaviors
could be expected to recur or continue, or
reoccurring behaviors which cast questions on
whether an individual should have access to
SGI, should be carefully evaluated prior to
any authorization of access to SGI.

It is necessary for a Licensee to resubmit
fingerprints only under two conditions:
(1) The FBI has determined that the
fingerprints cannot be classified due to poor
quality in the mechanics of taking the initial
impressions; or
(2) the initial submission has been lost.
If the FBI advises that six sets of
fingerprints are unclassifiable based on
conditions other than poor quality, the
licensee may submit a request to NRC for
alternatives. When those search results are
received from the FBI, no further search
is necessary.

Process To Challenge NRC Denials or
Revocations of Access to Safeguards
Information
1. Policy.
This policy establishes a process for
individuals whom NRC licensees nominate
as reviewing officials to challenge and appeal
NRC denials or revocations of access to
Safeguards Information (SGI). Any individual
nominated as a reviewing official
whom the NRC has determined may not have
access to SGI shall, to the extent provided
below, be afforded an opportunity to
challenge and appeal the NRC’s final
determination. This policy shall not be
construed to require the disclosure of SGI to
any person, nor shall it be construed to create
a liberty or property interest of any kind in
the access of any individual to SGI.
2. Applicability.
This policy applies solely to those
employees of licensees who are nominated as
a reviewing official, and who are thus to be
considered by the NRC for initial or
continued access to SGI in that position.
3. SGI Access Determination Criteria.
Determinations for granting a nominated
reviewing official access to SGI will be made
by the NRC staff. Access to SGI shall be
denied or revoked whenever it is determined
that an individual does not meet the
applicable standards. Access to SGI shall be
denied or revoked if an individual’s
eligibility for initial or continued access to
SGI shall be resolved in favor of the national
security and access will be
denied or revoked.

4. Procedures to Challenge the
Contents of Records Obtained from the FBI.
(a) Prior to a determination by the NRC
Facilities Security Branch Chief that an
individual nominated as a reviewing official
is denied or revoked access to SGI, the
individual shall:
(i) Be provided the contents of records
obtained from the FBI for the purpose of
assuring correct and complete information.
If, after reviewing the record, an individual
believes that it is incorrect or incomplete in
any respect and wishes to change, correct, or
update the alleged deficiency, or to explain
any matter in the record, the individual may
initiate challenge procedures. These
procedures include either direct application
by the individual challenging the record to
the agency (i.e., law enforcement agency) that
contributed the questioned information, or
direct challenge as to the accuracy or
completeness of any entry on the criminal
history record to the Assistant Director,
Federal Bureau of Investigation Identification
Division, Washington, DC 20537–9700 (as set
forth in 28 CFR 16.30 through 16.34). In the
latter case, the FBI forwards the challenge to
the agency that submitted the data and
requests that agency to verify or correct the
challenged entry. Upon receipt of an official
communication directly from the agency that
contributed the original information, the FBI
Identification Division makes any changes
necessary in accordance with the information
supplied by that agency.
(ii) Be afforded 10 days to initiate an action
challenging the results of an FBI criminal
history records check described in (i), above
after the record is made available for the
individual’s review. If such a challenge is
initiated, the NRC Facilities Security Branch
Chief may make a determination based upon
the criminal history record only upon receipt
of the FBI’s ultimate confirmation or
correction of the record.
5. Procedures to Provide Additional
Information.
a. Prior to a determination by the NRC Facilities Security Branch Chief that an individual nominated as a reviewing official is denied or revoked access to SGI, the individual shall:
   (i) Be afforded an opportunity to submit information relevant to the individual’s trustworthiness and reliability. The NRC Facilities Security Branch Chief shall, in writing, notify the individual of this opportunity, and any deadlines for submitting this information. The NRC Facilities Security Branch Chief may make a determination of access to SGI only upon receipt of the additional information submitted by the individual, or, if no such information is submitted, when the deadline to submit such information has passed.

6. Procedures to Notify an Individual of the NRC Facilities Security Branch Chief Determination to Deny or Revoke Access to SGI

a. Upon a determination by the NRC Facilities Security Branch Chief that an individual nominated as a reviewing official is denied or revoked access to SGI, the individual shall be provided a written explanation of the basis for this determination.

7. Procedures to Appeal an NRC Determination to Deny or Revoke Access to SGI

a. Upon a determination by the NRC Facilities Security Branch Chief that an individual nominated as a reviewing official is denied or revoked access to SGI, the individual shall be provided an opportunity to appeal this determination to the Director, Division of Facilities and Security. The determination must be appealed within 20 days of receipt of the written notice of the determination by the Facilities Security Branch Chief, and may either be in writing or in person. Any appeal made in person shall take place at the NRC’s headquarters, and shall be at the individual’s own expense. The determination by the Director, Division of Facilities and Security, shall be rendered within 60 days after receipt of the appeal.

8. Procedures to Notify an Individual of the Determination by the Director, Division of Facilities and Security, Upon an Appeal

a. A determination by the Director, Division of Facilities and Security, shall be provided to the individual in writing and include an explanation of the basis for this determination. A determination by the Director, Division of Facilities and Security, to affirm the Facilities Branch Chief’s determination to deny or revoke an individual’s access to SGI is final and not subject to further administrative appeals.

NUCLEAR REGULATORY COMMISSION
[NRC–2012–0254; EA–12–147]

In the Matter of Licensee Identified in Attachment 1 and all Other Persons Who Obtain Safeguards Information Described Herein; Order Imposing Requirements for the Protection of Certain Safeguards Information (Effective Immediately)

I

The Licensee, identified in Attachment 1 to this Order, holds a license issued in accordance with the Atomic Energy Act of 1954, as amended, (AEA) by the U.S. Nuclear Regulatory Commission (NRC or the Commission), authorizing it to possess, use, and transfer items containing radioactive material quantities of concern. The NRC intends to issue a security Order to this Licensee in the near future. The Order will require compliance with specific Additional Security Measures to enhance the security for certain radioactive material quantities of concern. The Commission has determined that these documents will contain Safeguards Information, will not be released to the public, and must be protected from unauthorized disclosure.

Therefore, the Commission is imposing the requirements, as set forth in Attachments 2 and 3 to this Order and in Order EA–12–148, so that the Licensee can receive these documents. This Order also imposes requirements for the protection of Safeguards Information in the hands of any person,2 whether or not a licensee of the Commission, who produces, receives, or acquires Safeguards Information.

II

The Commission has broad statutory authority to protect and prohibit the unauthorized disclosure of Safeguards Information. Section 147 of the AEA grants the Commission explicit authority to * * * issue such orders, as necessary to prohibit the unauthorized disclosure of safeguards

1 Attachment 1 contains sensitive information and will not be released to the public.
2 Person means (1) any individual, corporation, partnership, firm, association, trust, estate, public or private institution, group, government agency other than the Commission or the Department of Energy, except that the Department of Energy shall be considered a person with respect to those facilities of the Department of Energy specified in section 202 of the Energy Reorganization Act of 1974 (48 Stat. 1244), any State or any political subdivision of, or any political entity within a State, any foreign government or nation or any political subdivision of any such government or nation, or other entity; and (2) any legal successor, representative, agent, or agency of the foregoing. This authority extends to information concerning the security measures for the physical protection of special nuclear material, source material, and byproduct material. Licensees and all persons who produce, receive, or acquire Safeguards Information must ensure proper handling and protection of Safeguards Information to avoid unauthorized disclosure in accordance with the specific requirements for the protection of Safeguards Information contained in Attachments 2 and 3 to this Order. The Commission hereby provides notice that it intends to treat violations of the requirements contained in Attachments 2 and 3 to this Order, applicable to the handling and unauthorized disclosure of Safeguards Information, as serious breaches of adequate protection of the public health and safety and the common defense and security of the United States.

Access to Safeguards Information is limited to those persons who have established the need-to-know the information and are considered to be trustworthy and reliable, and meet the requirements of Order EA–12–148. A need-to-know means a determination by a person having responsibility for protecting Safeguards Information that a proposed recipient’s access to Safeguards Information is necessary in the performance of official, contractual, or licensee duties of employment.

The Licensee and all other persons who obtain Safeguards Information must ensure that they develop, maintain and implement strict policies and procedures for the proper handling of Safeguards Information to prevent unauthorized disclosure, in accordance with the requirements in Attachments 2 and 3 to this Order. The Licensee must ensure that all contractors whose employees may have access to Safeguards Information either adhere to the Licensee’s policies and procedures on Safeguards Information or develop, or maintain and implement their own acceptable policies and procedures. The Licensee remains responsible for the conduct of their contractors. The policies and procedures necessary to ensure compliance with applicable requirements contained in Attachments 2 and 3 to this Order must address, at a minimum, the following: the general performance requirement that each person who produces, receives, or acquires Safeguards Information shall ensure that Safeguards Information is protected against unauthorized disclosure; protection of Safeguards Information at fixed location, in storage, and while in transit; correspondence containing Safeguards

BILLING CODE 7590–01–P