disposition instructions to any recordkeeping medium.

6. Department of Transportation, Federal Highway Administration (N1–406–04–5, 5 items, 3 temporary items). Electronic copies of records created using electronic mail and word processing that are associated with planning, numbering, and designating interstate highways. Also included are duplicate copies of these records. Recordkeeping copies of these files are proposed for permanent retention.

7. National Archives and Records Administration, Government-wide (N1–GRS–04–4, 9 items, 9 temporary items). Addition to the General Records Schedules covering records accumulated by Chief Information Officers. Included are records relating to such matters as information technology program planning, enterprise architecture, IT capital investments, legal and regulatory compliance, the activities of committees, and schedules of daily activities. Also included are electronic copies of records created using electronic mail and word processing.

8. National Archives and Records Administration, Office of Human Resources and Information Services (N1–64–05–2, 4 items, 4 temporary items). Case files relating to information technology projects, including records documenting various stages of the project such as concept development, system testing, and approvals. Also included are electronic copies of records created using electronic mail and word processing. This schedule authorizes the agency to apply the proposed disposition instructions to any recordkeeping medium.

9. National Archives and Records Administration, Office of the **Federal Register** (N1–64–05–3, 4 items, 4 temporary items). Inquiries from researchers and the general public concerning publications, policies, and procedures of the **Federal Register** and other Government publications. Also included are electronic copies of records created using electronic mail and word processing.

10. Small Business Administration, Office of Capital Access (N1–309–04–1, 8 items, 8 temporary items). Inputs, outputs, master files, and documentation associated with an electronic system which contains information concerning the Small Business Investment Company interim funding process and the New Markets Venture Capital Program. Also included are electronic copies of documents created using word processing and electronic mail.

Dated: December 9, 2004.

Michael J. Kurtz,

Assistant Archivist for Records Services—Washington, DC.

[FR Doc. 04–27537 Filed 12–15–04; 8:45 am]

BILLING CODE 7515–01–P

NATIONAL CRIME PREVENTION AND PRIVACY COMPACT COUNCIL

Security and Management Control Outsourcing Standards

AGENCY: National Crime Prevention and Privacy Compact Council.

ACTION: Notice.

SUMMARY: Pursuant to the publication requirement in title 42, United States Code, 14616, Article VI(e), the Compact Council, established by the National Crime Prevention and Privacy Compact (Compact) Act of 1998, is providing public notice of the attached Security and Management Control Outsourcing Standards (Outsourcing Standards) established by the Compact Council.

DATES: All comments must be received on or before February 14, 2005.

ADDRESSES: Send all written comments concerning these Outsourcing Standards to the Compact Council Office, 1000 Custer Hollow Road, Module C3, Clarksburg, WV 26306; Attention: Todd C. Commodore. Comments may also be submitted by fax at (304) 625–5388 or via electronic mail at *tcommodore@leo.gov*. To ensure proper handling, please reference Noncriminal Justice Outsourcing Standards'' on your correspondence.

FOR FURTHER INFORMATION CONTACT: Todd C. Commodore, FBI CJIS Division, 1000 Custer Hollow Road, Module C3, Clarksburg, WV 26306; telephone (304) 625–2803; e-mail *tcommodo@leo.gov*; fax number (304) 625–5388.

SUPPLEMENTARY INFORMATION: The National Crime Prevention and Privacy Compact (Compact), 42 U.S.C. 14616, establishes uniform standards and processes for the interstate and Federal-State exchange of criminal history records for noncriminal justice purposes. The Compact was approved by the Congress on October 9, 1998 (Pub. L. 105–251), and became effective on April 28, 1999, when ratified by the second state. Article VI of the Compact provides for a Compact Council that has the authority to promulgate rules and procedures governing the use of the Interstate Identification Index (III) System for noncriminal justice purposes. The III is the system of Federal and State criminal history records maintained by the Federal Bureau of Investigation (FBI).

The Compact Council has adopted an interim final rule, ''Outsourcing of Noncriminal Justice Administrative Functions'' (Outsourcing Rule), published elsewhere in today's edition of the **Federal Register** and to be codified at 28 CFR part 906, to permit the outsourcing of noncriminal justice administrative functions involving access to criminal history record information (CHRI) from the III System. This interim rule will permit a third party to perform noncriminal justice administrative functions relating to the processing of CHRI maintained in the III System, subject to appropriate controls, when acting as an agent for a governmental agency or other authorized recipient of CHRI. Among other things, the interim rule provides that contracts or agreements providing for the outsourcing authorized by the rule ''shall incorporate by reference a security and management control outsourcing standard approved by the Compact Council after consultation with the United States Attorney General.'' *See* 28 CFR 906.2(c). The attached Security and Management Control Outsourcing Standards (Outsourcing Standards), are the standards referenced in the Outsourcing Rule. The Outsourcing Standards were developed by the Compact Council in coordination with the FBI's Criminal Justice Information Services (CJIS) Division and relevant subcommittees of the CJIS Advisory Policy Board (APB). The APB is an advisory committee with representatives of State, local, and Federal contributors and users of the FBI's National Crime Information Center information systems, including the III.

The Compact Council developed two Outsourcing Standards—one for Contractors having access to CHRI on behalf of an authorized recipient for noncriminal justice purposes and one for Contractors serving as channelers of noncriminal justice criminal history record check requests and results. The first Outsourcing Standard (''Security and Management Control Outsourcing Standard for Contractors Having Access to CHRI on Behalf of an Authorized Recipient for Noncriminal Justice Purposes'') will be used by Contractors authorized to perform noncriminal justice administrative functions requiring access to CHRI without a direct connection to the FBI's CJIS Wide Area Network (WAN). The second Outsourcing Standard (''Security and Management Control Outsourcing Standard for Channelers Only'') will be used by Contractors authorized access to CHRI through a direct connection to the

FBI's CJIS WAN. The two Outsourcing Standards are printed below. Hereafter, prior to utilizing the Outsourcing Standards, interested parties should request the most current version by contacting the Compact Council Office, 1000 Custer Hollow Road, Module C3, Clarksburg, WV 26306, Attention: FBI Compact Officer.

The Outsourcing Standards were discussed at public Compact Council meetings held in May and November of 2004 and the Outsourcing Standards were adopted by the Compact Council at its November 2004 meeting. The meetings were attended by many interested stakeholders, but in order to facilitate more broad-based public comment, written comments on the Outsourcing Standards are invited.

Dated: November 29, 2004.

Donna M. Uzzell,

Compact Council Chairman.

Attachment: Security and Management Control Outsourcing Standard for Contractors Having Access to Criminal History Record Information on Behalf of an Authorized Recipient for Noncriminal Justice Purposes

The goal of this document is to provide adequate security and integrity for criminal history record information (CHRI) while under the control or management of an outsourced third party, the Contractor. Adequate security is defined in Office of Management and Budget Circular A–130 as ''security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.''

The intent of this Security and Management Control Outsourcing Standard (Outsourcing Standard) is to require that the Contractor maintain a security program consistent with Federal and State laws, regulations, and standards (including the FBI Criminal Justice Information Services (CJIS) Security Policy) as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General.

This Outsourcing Standard identifies the duties and responsibilities with respect to adequate internal controls within the contractual relationship so that the security and integrity of the Interstate Identification Index (III) System and CHRI are not compromised. The standard security program shall include consideration of site security, dissemination restrictions, personnel security, system security, and data security.

The provisions of this Outsourcing Standard are established by the Compact Council pursuant to 28 CFR part 906 and are subject to the scope of that rule. They apply to all personnel, systems, networks, and facilities supporting and/or acting on behalf of the Authorized Recipient of CHRI.

1.0 Definitions

1.01 *Access to CHRI* means to use, exchange, retain/store, or view CHRI obtained from the III System but excludes direct access to the III System by computer terminal or other automated means by Contractors other than those that may be contracted by the FBI or state criminal history record repositories or as provided by title 42, United States Code, section 14614(b).

1.02 *Authorized Recipient* means (1) a nongovernmental entity authorized by Federal statute or Federal executive order to receive CHRI for noncriminal justice purposes, or (2) a government agency authorized by Federal statute, Federal executive order, or State statute which has been approved by the United States Attorney General to receive CHRI for noncriminal justice purposes.

1.03 *Chief Administrator,* as referred to in Article I(2)(B) of the Compact, means the primary administrator of a Nonparty State's criminal history record repository or a designee of such administrator who is a regular full-time employee of the repository.

1.04 *CHRI,* as referred to in Article I(4) of the Compact, means information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, or other formal criminal charges, and any disposition arising therefrom, including acquittal, sentencing, correctional supervision, or release; but does not include identification information such as fingerprint records if such information does not indicate involvement of the individual with the criminal justice system.

1.05 *Criminal History Record Check, for purposes of this Outsourcing Standard only,* means an authorized noncriminal justice fingerprint-based search of a state criminal history record repository and/or the FBI system.

1.06 *Compact Officer,* as provided in Article I(2) of the Compact, means (A) with respect to the Federal Government, an official [FBI Compact Officer] so designated by the Director of the FBI [to administer and enforce the compact among Federal agencies], or (B) with respect to a Party State, the chief administrator of the State's criminal history record repository or a designee of the chief administrator who is a regular full-time employee of the repository.

1.07 *Contractor* means a government agency, a private business, non-profit organization or individual, that is not itself an Authorized Recipient with respect to the particular noncriminal justice purpose, who has entered into a contract with an Authorized Recipient to perform noncriminal justice administrative functions requiring access to CHRI.

1.08 *Dissemination* means the disclosure of III CHRI by an Authorized Recipient to an authorized Contractor, or by the Contractor to another Authorized Recipient consistent with the Contractor's responsibilities and with limitations imposed by Federal and State laws, regulations, and standards as well as rules, procedures, and standards established by the Compact Council and the United States Attorney General.

1.09 *Noncriminal Justice Administrative Functions* means the routine noncriminal justice administrative functions relating to the processing of CHRI, to include but not limited to the following:

1. Making fitness determinations/ recommendations.
2. Obtaining missing dispositions.
3. Disseminating CHRI as authorized by Federal statute, Federal Executive Order, or State statute approved by the United States Attorney General.
4. Other authorized activities relating to the general handling, use, and storage of CHRI.

1.10 *Noncriminal Justice Purposes,* as provided in Article I(18) of the Compact, means uses of criminal history records for purposes authorized by Federal or State law other than purposes relating to criminal justice activities, including employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.

1.11 *Outsourcing Standard* means a document approved by the Compact Council after consultation with the United States Attorney General which is to be incorporated by reference into a contract between an Authorized Recipient and a Contractor. The Outsourcing Standard authorizes access to CHRI, limits the use of the information to the purposes for which it is provided, prohibits retention and/or dissemination except as specifically authorized, ensures the security and confidentiality of the information, provides for audits and sanctions, provides conditions for termination of the contract, and contains such other provisions as the Compact Council may require.

1.12 *Physically Secure Location* means a location where access to CHRI can be obtained, and adequate protection is provided to prevent any unauthorized access to CHRI.

1.13 *Positive Identification,* as provided in Article I(20) of the Compact, means a determination, based upon a comparison of fingerprints [1] or other equally reliable biometric identification techniques, that the subject of a record search is the same person as the subject of a criminal history record or records indexed in the III System. Identifications based solely upon a comparison of subjects' names or other nonunique identification characteristics or numbers, or combinations thereof, shall not constitute positive identification.

1.14 *Public Carrier Network* means a telecommunications infrastructure consisting of network components that are not owned, operated, and managed solely by the agency using that network, *i.e.*, any telecommunications infrastructure which supports public users other than those of the agency using that network. Examples of a public carrier network include but are not limited to the following: dial-up and Internet connections, network connections to Verizon, network connections to AT&T, ATM Frame Relay clouds, wireless networks, wireless links, and cellular telephones. A public carrier network provides network services to the public; not just to the single agency using that network.

[1] The Compact Council currently defines positive identification for noncriminal justice purposes as identification based upon a qualifying ten-rolled or qualifying ten-flat fingerprint submission. Further information concerning qualifying fingerprint submissions may be obtained from the FBI Compact Council office.

1.15 *Security Violation* means the failure to prevent or failure to institute safeguards to prevent access, use, retention, or dissemination of CHRI in violation of: (A) federal or state law, regulation, or Executive Order; or (B) a rule, procedure, or standard established by the Compact Council and the United States Attorney General.

2.0 Responsibilities of the Authorized Recipient

2.01 Prior to engaging in outsourcing any noncriminal justice functions, the Authorized Recipient shall request and receive written permission from (A) the State Compact Officer/Chief Administrator [2] or (B) the FBI Compact Officer.[3] The Authorized Recipient shall provide the Compact Officer/Chief Administrator copies of the specific authority for the outsourced work, criminal history record check requirements, and/or a copy of the contract as requested. The Authorized Recipient shall inquire whether a prospective Contractor has any security violations (See Section 8.04) and report those findings to the Compact Officer/Chief Administrator prior to outsourcing noncriminal justice administrative functions.

2.02 The Authorized Recipient shall execute a contract prior to providing a Contractor access to CHRI. The contract shall, at a minimum, incorporate by reference and have appended thereto this Outsourcing Standard.

2.03 The Authorized Recipient shall, in those instances when the Contractor is to perform duties requiring access to CHRI, specify the terms and conditions of such access; limit the use of such information to the purposes for which it is provided; limit retention of the information to a period of time not to exceed that period of time the Authorized Recipient is permitted to retain such information; prohibit dissemination of the information except as specifically authorized by federal and state laws, regulations, and standards as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General; ensure the security and confidentiality of the information to include confirmation that the intended recipient is authorized to receive CHRI; provide for audits and sanctions; provide conditions for termination of the contract; maintain up-to-date records of Contractor personnel who have access to CHRI; and ensure that Contractor personnel comply with this Outsourcing Standard.

a. The Authorized Recipient shall conduct criminal history record checks of Contractor personnel having access to CHRI if such checks are required of the Authorized Recipient's personnel having similar access.[4]

b. The Authorized Recipient shall ensure that the Contractor maintains site security.

c. The Authorized Recipient shall ensure that the most current version of both the Outsourcing Standard and the CJIS Security Policy are incorporated by reference at the time of contract and/or Option renewal.

2.04 The Authorized Recipient is responsible for the actions of the Contractor and shall monitor the Contractor's compliance to the terms and conditions of the Outsourcing Standard. The Authorized Recipient shall certify to the Compact Officer/Chief Administrator that a compliance review was conducted with the Contractor within 90 days of execution of the contract.

2.05 The Authorized Recipient shall provide written notice of any early voluntary termination of the contract to the Compact Officer/Chief Administrator or the FBI Compact Officer.

3.0 Responsibilities of the Contractor

3.01 The Contractor and its employees shall comply with all Federal and State laws, regulations, and standards (including the CJIS Security Policy) as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General.

3.02 The Contractor shall develop and document a security program to comply with the current Outsourcing Standard and any revised or successor Outsourcing Standard. The Security Program shall describe the implementation of the security requirements described in this Outsourcing Standard, the associated Security Training Program, and the reporting guidelines for documenting and communicating security violations and corrective actions to the Authorized Recipient. The Security Program shall be subject to the approval of the Authorized Recipient.

3.03 The Contractor shall be accountable for the management of the Security Program. The Contractor shall be responsible for reporting all security violations of this Outsourcing Standard to the Authorized Recipient.

3.04 Except when the training requirement is retained by the Authorized Recipient, the Contractor shall develop a Security Training Program for all Contractor personnel with access to CHRI prior to their appointment/assignment. Immediate training shall be provided upon receipt of notice on any changes to Federal and State laws, regulations, and standards as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General. Annual refresher training shall also be provided. The Contractor shall certify to the Authorized Recipient that the annual refresher training was completed for those Contractor personnel with access to CHRI. The Security Training Program shall be subject to the approval of the Authorized Recipient.

3.05 The Contractor shall make its facilities available for announced and unannounced security inspections performed by the Authorized Recipient, the State, or the FBI on behalf of the Compact Council. Such facilities are also subject to triennial audits by the State and the FBI on behalf of the Compact Council. An audit may also be conducted on a more frequent basis.

3.06 The Contractor's Security Program is subject to review by the Authorized Recipient, the Compact Officer/Chief Administrator, and the FBI CJIS Division. During this review, provision will be made to update the Security Program to address security violations and to ensure changes in policies and standards as well as changes in Federal and State law are incorporated.

3.07 The Contractor shall maintain CHRI only for the period of time necessary to fulfill their contractual obligations but not to exceed the period of time that the Authorized Recipient is authorized to maintain and does maintain the CHRI.

3.08 The Contractor shall maintain a log of any dissemination of CHRI.

4.0 Site Security

4.01 The Authorized Recipient shall ensure that the Contractor site is a physically secure location at all times to protect against any unauthorized access to CHRI.

5.0 Dissemination

5.01 The Contractor shall not disseminate CHRI without the consent of the Authorized Recipient, and as specifically authorized by Federal and State laws, regulations, and standards as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General.

5.02 An up-to-date log concerning dissemination of CHRI shall be maintained by the Contractor for a minimum one year retention period. This log must clearly identify: (A) the Authorized Recipient and the secondary recipient with unique identifiers, (B) the record disseminated, (C) the date of dissemination, (D) the statutory authority for dissemination, and (E) the means of dissemination.

6.0 Personnel Security

6.01 If a local, State, or Federal written standard requires a criminal history record check of the Authorized Recipient's personnel with access to CHRI, then a criminal history record check shall be required of the Contractor's employees having access to CHRI. The criminal history record check of Contractor employees at a minimum will be no less stringent than the criminal history record check that is performed on the Authorized Recipient's personnel performing similar functions. Criminal history record checks must be completed prior to performing work under the contract.

6.02 If a local, State, or Federal written standard requires a criminal history record

[2] The Compact Officer/Chief Administrator may not grant such permission unless he/she has implemented a combined state/federal audit program to triennially audit each Contractor and Authorized Recipient engaging in outsourcing with the first of such audits to be conducted within one year of the signing of the contract.

[3] State or local Authorized Recipients based on State or Federal Statutes shall contact the State Compact Officer/Chief Administrator. Federal or Regulatory Agency Authorized Recipients shall contact the FBI Compact Officer.

[4] If a national criminal history record check of government personnel having access to CHRI is mandated by a state statute approved by the Attorney General under Public Law 92–544, the State Compact Officer/Chief Administrator must ensure Contractor personnel having similar access are either covered by the existing law or that the existing law is amended to include such Contractor personnel prior to authorizing outsourcing initiatives.

check for support personnel, contractors, and custodial workers who work in a physically secure location, then a criminal history record check shall be required for these individuals, unless these individuals are escorted by authorized personnel at all times. The criminal history record check for these individuals at a minimum will be no less stringent than the criminal history record check that is performed on the Authorized Recipient's support personnel, contractors, and custodial workers performing similar functions. Criminal history record checks must be completed prior to performing work under the contract.

6.03 The Contractor shall ensure that each employee performing work under the contract is aware of the requirements of the Outsourcing Standard and the State and Federal laws governing the security and integrity of CHRI. The Contractor shall confirm that each employee understands the Outsourcing Standard requirements and laws that apply to his/her responsibilities.

6.04 If a criminal history record check is required, the Contractor shall maintain a list of personnel who successfully completed the criminal history record check.

7.0 System Security

7.01 The Contractor's security system shall comply with the CJIS Security Policy in effect at the time the Outsourcing Standard is incorporated into the contract and with successor versions of the CJIS Security Policy as they are made known to the Contractor by the Authorized Recipient.

a. If CHRI can be accessed by unauthorized personnel via Wide Area Network/Local Area Network or the Internet, then the Contractor shall protect the CHRI with firewall-type devices to prevent such unauthorized access. These devices shall implement a minimum firewall profile as specified by the CJIS Security Policy in order to provide a point of defense and a controlled and audited access to CHRI, both from inside and outside the networks.

b. Data encryption shall be required throughout the network, passing CHRI through a shared public carrier network.

7.02 The Contractor shall provide for the secure storage and disposal of all hard copy and media associated with the system to prevent access by unauthorized personnel.

a. CHRI shall be stored in a physically secure location.

b. The Authorized Recipient shall ensure that a procedure is in place for sanitizing all fixed storage media (*e.g.*, disks, drives, backup storage) at the completion of the contract and/or before it is returned for maintenance, disposal, or reuse. Sanitization procedures include overwriting the media and/or degaussing the media.

7.03 To prevent and/or detect unauthorized access to CHRI in transmission or storage, each Authorized Recipient must be identified by an Originating Agency Identifier (ORI) or state assigned identifier, and each Contractor or sub-Contractor must be uniquely identified.

8.0 Security Violations

8.01 *Duties of the Authorized Recipient and Contractor.* a. The Contractor shall develop and maintain a written policy for discipline of Contractor employees who violate the security provisions of the contract, which includes this Outsourcing Standard that is incorporated by reference.

b. Pending investigation, the Contractor shall immediately suspend any employee who commits a security violation from assignments in which he/she has access to CHRI under the contract.

c. The Contractor shall immediately notify the Authorized Recipient of any security violation or termination of the contract, to include unauthorized access to CHRI made available pursuant to the contract. Within five calendar days of such notification, the Contractor shall provide the Authorized Recipient a written report documenting such security violation, any corrective actions taken by the Contractor to resolve such violation, and the date, time, and summary of the prior notification.

d. The Authorized Recipient shall immediately notify the State Compact Officer/Chief Administrator and the FBI Compact Officer of any security violation or termination of the contract, to include unauthorized access to CHRI made available pursuant to the contract. The Authorized Recipient shall provide a written report of any security violation (to include unauthorized access to CHRI by the Contractor) to the State Compact Officer/ Chief Administrator, if applicable, and the FBI Compact Officer, within five calendar days of receipt of the written report from the Contractor. The written report must include any corrective actions taken by the Contractor and the Authorized Recipient to resolve such security violation.

8.02 *Termination of the contract by the Authorized Recipient for security violations.*

a. The contract is subject to termination by the Authorized Recipient for security violations involving CHRI obtained pursuant to the contract.

b. The contract is subject to termination by the Authorized Recipient for the Contractor's failure to notify the Authorized Recipient of any security violation or to provide a written report concerning such violation.

c. If the Contractor refuses to or is incapable of taking corrective actions to successfully resolve a security violation, the Authorized Recipient shall terminate the contract.

8.03 *Suspension or termination of the exchange of CHRI for security violations.* a. Notwithstanding the actions taken by the State Compact Officer, if the Authorized Recipient fails to provide a written report notifying the State Compact Officer/Chief Administrator or the FBI Compact Officer of a security violation, or refuses to or is incapable of taking corrective action to successfully resolve a security violation, the Compact Council or the United States Attorney General may suspend or terminate the exchange of CHRI with the Authorized Recipient pursuant to 28 CFR 906.2(d).

b. If the exchange of CHRI is suspended, it may be reinstated after satisfactory written assurances have been provided to the Compact Council Chairman or the United States Attorney General by the Compact Officer/Chief Administrator, the Authorized Recipient and the Contractor that the security violation has been resolved. If the exchange of CHRI is terminated, the Contractor's records (including media) containing CHRI shall be immediately deleted or returned as specified by the Authorized Recipient.

8.04 The Authorized Recipient shall provide written notice (through the State Compact Officer/Chief Administrator if applicable) to the FBI Compact Officer of the following:

a. The termination of a contract for security violations.

b. Security violations involving the unauthorized access to CHRI.

c. The Contractor's name and unique identification number, the nature of the security violation, whether the violation was intentional, and the number of times the violation occurred.

8.05 The Compact Officer/Chief Administrator, Compact Council and the United States Attorney General reserve the right to investigate or decline to investigate any report of unauthorized access to CHRI.

8.06 The Compact Officer/Chief Administrator, Compact Council, and the United States Attorney General reserve the right to audit the Authorized Recipient and the Contractor's operations and procedures at scheduled or unscheduled times. The Compact Council, the United States Attorney General, and the state are authorized to perform a final audit of the Contractor's systems after termination of the contract.

9.0 Miscellaneous Provisions

9.01 This Outsourcing Standard does not confer, grant, or authorize any rights, privileges, or obligations to any persons other than the Contractor, the Authorized Recipient, Compact Officer/Chief Administrator (where applicable), and the FBI.

9.02 The following document is incorporated by reference and made part of this Outsourcing Standard: (1) The CJIS Security Policy.

9.03 The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they provide a minimum basis for the security of the system and the CHRI accessed therefrom and it is understood that there may be terms and conditions of the appended contract which impose more stringent requirements upon the Contractor.[5]

9.04 The minimum security measures as outlined in this Outsourcing Standard may only be modified by the Compact Council. Conformance to such security measures may not be less stringent than stated in this Outsourcing Standard without the consent of the Compact Council in consultation with the United States Attorney General.

9.05 This Outsourcing Standard may only be modified by the Compact Council and may not be modified by the parties to the appended contract without the consent of the Compact Council.

9.06 Appropriate notices, assurances, and correspondence to the FBI Compact Officer, Compact Council, and the United States

[5] Such conditions could include additional audits, fees, or security requirements.

Attorney General required by Section 8.0 of this Outsourcing Standard shall be forwarded by First Class Mail to: FBI Compact Officer, 1000 Custer Hollow Road, Module C3, Clarksburg, WV 26306.

Security and Management Control Outsourcing Standard for Channelers Only

The goal of this document is to provide adequate security and integrity for criminal history record information (CHRI) while under the control or management of an outsourced third party, the Contractor. Adequate security is defined in Office of Management and Budget Circular A–130 as ''security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.''

The intent of this Security and Management Control Outsourcing Standard (Outsourcing Standard) is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the FBI Criminal Justice Information Services (CJIS) Security Policy) as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General.

This Outsourcing Standard identifies the duties and responsibilities with respect to adequate internal controls within the contractual relationship so that the security and integrity of the Interstate Identification Index (III) System and CHRI are not compromised. The standard security program shall include consideration of site security, dissemination restrictions, personnel security, system security, and data security.

The provisions of this Outsourcing Standard are established by the Compact Council pursuant to 28 CFR part 906 and are subject to the scope of that rule. They apply to all personnel, systems, networks, and facilities supporting and/or acting on behalf of the Authorized Recipient of CHRI.

1.0 Definitions

1.01 *Access to CHRI* means to use, exchange, retain/store, or view CHRI obtained from the III System but excludes direct access to the III System by computer terminal or other automated means by Contractors other than those that may be contracted by the FBI or State criminal history record repositories or as provided by title 42, United States Code, section 14614(b).

1.02 *Authorized Recipient* means (1) a nongovernmental entity authorized by Federal statute or Federal executive order to receive CHRI for noncriminal justice purposes, or (2) a government agency authorized by Federal statute, Federal executive order, or State statute which has been approved by the United States Attorney General to receive CHRI for noncriminal justice purposes.

1.03 *Authorized Recipient's Information Security Officer* means the individual who shall ensure technical compliance with all applicable elements of this Outsourcing Standard.

1.04 *Chief Administrator*, as referred to in Article I(2)(B) of the Compact, means the primary administrator of a Nonparty State's criminal history record repository or a designee of such administrator who is a regular full-time employee of the repository.

1.05 *CHRI*, as referred in Article I(4) of the Compact, means information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, or other formal criminal charges, and any disposition arising therefrom, including acquittal, sentencing, correctional supervision, or release; but does not include identification information such as fingerprint records if such information does not indicate involvement of the individual with the criminal justice system.

1.06 *Criminal History Record Check*, for purposes of this Outsourcing Standard only, means an authorized noncriminal justice fingerprint-based search of a State criminal history record repository and/or the FBI system.

1.07 *CJIS Systems Agency*, as provided in Section 1.4 of the FBI Criminal Justice Information Services (CJIS) Division's Advisory Policy Board Bylaws, means a criminal justice agency which has overall responsibility for the administration and usage of CJIS Division Programs within a State, district, territory, or foreign country. This includes any Federal agency that meets the definition and provides services to other Federal agencies and/or whose users reside in multiple states or territories.

1.08 *CJIS Systems Officer*, as provided in Section 1.5 of the CJIS Advisory Policy Board Bylaws, means the individual employed by the CJIS Systems Agency who is responsible for monitoring system use, enforcing system discipline and security, and assuring that CJIS operating procedures are followed by all users as well as other related duties outlined by the user agreements with the FBI's CJIS Division. (This title was formerly referred to as the Control Terminal Officer or the Federal Service Coordinator).

1.09 *Compact Officer,* as provided in Article I(2) of the Compact, means (A) with respect to the Federal Government, an official [FBI Compact Officer] so designated by the Director of the FBI [to administer and enforce the compact among Federal agencies], or (B) with respect to a Party State, the chief administrator of the State's criminal history record repository or a designee of the chief administrator who is a regular full-time employee of the repository.

1.10 *Contractor* means a government agency, a private business, non-profit organization or individual, that is not itself an Authorized Recipient with respect to the particular noncriminal justice purpose, who has entered into a contract with an Authorized Recipient to perform noncriminal justice administrative functions requiring access to CHRI. Under this Outsourcing Standard applicable to channelers, a Contractor includes one who has direct connectivity to the CJIS Wide Area Network (WAN) for the purpose of electronic submission of fingerprints to and the receipt of CHRI from the FBI on behalf of an Authorized Recipient.

1.11 *Contractor's Security Officer* means the individual accountable for the management of the Contractor's security program.

1.12 *Dissemination* means the disclosure of III CHRI by an Authorized Recipient to an authorized Contractor, or by the Contractor to another Authorized Recipient consistent with the Contractor's responsibilities and with limitations imposed by Federal and State laws, regulations, and standards as well as rules, procedures, and standards established by the Compact Council and the United States Attorney General.

1.13 *Noncriminal Justice Administrative Functions* means the routine noncriminal justice administrative functions relating to the processing of CHRI, to include but not limited to the following:

1. Making fitness determinations/ recommendations.
2. Obtaining missing dispositions.
3. Disseminating CHRI as authorized by Federal statute, Federal Executive Order, or State statute approved by the United States Attorney General.
4. Other authorized activities relating to the general handling, use, and storage of CHRI.

1.14 *Noncriminal Justice Purposes,* as provided in Article I(18) of the Compact, means uses of criminal history records for purposes authorized by Federal or State law other than purposes relating to criminal justice activities, including employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.

1.15 *Outsourcing Standard* means a document approved by the Compact Council after consultation with the United States Attorney General which is to be incorporated by reference into a contract between an Authorized Recipient and a Contractor. The Outsourcing Standard authorizes access to CHRI, limits the use of the information to the purposes for which it is provided, prohibits retention and/or dissemination except as specifically authorized, ensures the security and confidentiality of the information, provides for audits and sanctions, provides conditions for termination of the contract, and contains such other provisions as the Compact Council may require.

1.16 *Physically Secure Location* means a location where access to CHRI can be obtained, and adequate protection is provided to prevent any unauthorized access to CHRI.

1.17 *Positive Identification,* as provided in Article I(20) of the Compact, means a determination, based upon a comparison of fingerprints [6] or other equally reliable biometric identification techniques, that the subject of a record search is the same person as the subject of a criminal history record or records indexed in the III System. Identifications based solely upon a comparison of subjects' names or other nonunique identification characteristics or numbers, or combinations thereof, shall not constitute positive identification.

1.18 *Public Carrier Network* means a telecommunications infrastructure consisting

[6] The Compact Council currently defines positive identification for noncriminal justice purposes as identification based upon a qualifying ten-rolled or qualifying ten-flat fingerprint submission. Further information concerning qualifying fingerprint submissions may be obtained from the FBI Compact Council office.

of network components that are not owned, operated, and managed solely by the agency using that network, *i.e.*, any telecommunications infrastructure which supports public users other than those of the agency using that network. Examples of a public carrier network include but are not limited to the following: dial-up and Internet connections, network connections to Verizon, network connections to AT&T, ATM Frame Relay clouds, wireless networks, wireless links, and cellular telephones. A public carrier network provides network services to the public; not just to the single agency using that network.

1.19 *Security Violation* means the failure to prevent or failure to institute safeguards to prevent access, use, retention, or dissemination of CHRI in violation of: (A) Federal or State law, regulation, or Executive Order; or (B) a rule, procedure, or standard established by the Compact Council and the United States Attorney General.

2.0 Responsibilities of the Authorized Recipient

2.01 Prior to engaging in outsourcing any noncriminal justice functions, the Authorized Recipient shall request and receive written permission from (A) the State Compact Officer/Chief Administrator [7] or (B) the FBI Compact Officer.[8] The Authorized Recipient shall provide the Compact Officer/Chief Administrator copies of the specific authority for the outsourced work, criminal history record check requirements, and/or a copy of the contract as requested. The Authorized Recipient shall inquire whether a prospective Contractor has any security violations (see Section 8.04) and report those findings to the Compact Officer/Chief Administrator prior to outsourcing noncriminal justice administrative functions.

2.02 The Authorized Recipient shall execute a contract prior to providing a Contractor access to CHRI. The contract shall, at a minimum, incorporate by reference and have appended thereto this Outsourcing Standard.

2.03 The Authorized Recipient shall, in those instances when the Contractor is to perform duties requiring access to CHRI, specify the terms and conditions of such access; limit the use of such information to the purposes for which it is provided; limit retention of the information to a period of time not to exceed that period of time the Authorized Recipient is permitted to retain such information; prohibit dissemination of the information except as specifically authorized by Federal and State laws, regulations, and standards as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General; ensure the security and confidentiality of the information to include confirmation that the intended recipient is authorized to receive CHRI; provide for audits and sanctions; provide conditions for termination of the contract; maintain up-to-date records of Contractor personnel who have access to CHRI; and ensure that Contractor personnel comply with this Outsourcing Standard.

a. The Authorized Recipient shall conduct criminal history record checks of Contractor personnel having access to CHRI if such checks are required of the Authorized Recipient's personnel having similar access.[9]

b. The Authorized Recipient shall ensure that the Contractor maintains site security.

c. The Authorized Recipient shall ensure that the most current version of both the Outsourcing Standard and the CJIS Security Policy are incorporated by reference at the time of contract and/or Option renewal.

d. The Authorized Recipient shall ensure that the Contractor establishes and administers an Information Technology (IT) Security Program.

e. The Authorized Recipient shall allow the FBI to periodically test the ability to penetrate the FBI's network through the external network connection or system.

2.04 The Authorized Recipient shall understand the communications and record capabilities of the Contractor which has access to federal or state records through, or because of, its outsourcing relationship with the Authorized Recipient. The Authorized Recipient shall maintain an updated topological drawing which depicts the interconnectivity of the Contractor's network configuration.

2.05 The Authorized Recipient is responsible for the actions of the Contractor and shall monitor the Contractor's compliance to the terms and conditions of the Outsourcing Standard. The Authorized Recipient shall certify to the Compact Officer/Chief Administrator that a compliance review was conducted with the Contractor within 90 days of execution of the contract.

2.06 The Authorized Recipient shall provide written notice of any early voluntary termination of the contract to the Compact Officer/Chief Administrator or the FBI Compact Officer.

2.07 The Authorized Recipient shall appoint an Information Security Officer. The Authorized Recipient's Information Security Officer shall:

a. Serve as the security POC for the FBI CJIS Division Information Security Officer;

b. Document technical compliance with this Outsourcing Standard; and

c. Establish a security incident response and reporting procedure to discover, investigate, document, and report on major incidents that significantly endanger the security or integrity of the noncriminal justice agency systems to the CJIS Systems Officer and the FBI CJIS Division Information Security Officer.

3.0 Responsibilities of the Contractor

3.01 The Contractor and its employees shall comply with all federal and state laws, regulations, and standards (including the CJIS Security Policy) as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General.

3.02 The Contractor shall develop and maintain an IT security program. The Contractor is therefore responsible to set, maintain, and enforce the following:

a. Standards for the selection, supervision, and separation of personnel who have access to CHRI.

b. Policy governing the operation of computers, access devices, circuits, hubs, routers, firewalls, and other components that comprise and support a telecommunications network and related CJIS systems used to process, store, or transmit CHRI.

3.03 The Contractor shall develop and document a security program to comply with the current Outsourcing Standard and any revised or successor Outsourcing Standard. The Security Program shall describe the implementation of the security requirements described in this Outsourcing Standard, the associated Security Training Program, and the reporting guidelines for documenting and communicating security violations and corrective actions to the Authorized Recipient. The Security Program shall be subject to the approval of the Authorized Recipient.

3.04 The Contractor shall be accountable for the management of the Security Program. The Contractor shall be responsible for reporting all security violations of this Outsourcing Standard to the Authorized Recipient.

3.05 Except when the training requirement is retained by the Authorized Recipient, the Contractor shall develop a Security Training Program for all Contractor personnel with access to CHRI prior to their appointment/assignment. Immediate training shall be provided upon receipt of notice on any changes to Federal and State laws, regulations, and standards as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General. Annual refresher training shall also be provided. The Contractor shall certify to the Authorized Recipient that the annual refresher training was completed for those Contractor personnel with access to CHRI. The Security Training Program shall be subject to the approval of the Authorized Recipient.

3.06 The Contractor shall make its facilities available for announced and unannounced security inspections performed by the Authorized Recipient, the State, or the FBI on behalf of the Compact Council. Such facilities are also subject to triennial audits by the state and the FBI on behalf of the Compact Council. An audit may also be conducted on a more frequent basis.

3.07 The Contractor's Security Program is subject to review by the Authorized

[7] The Compact Officer/Chief Administrator may not grant such permission unless he/she has implemented a combined state/federal audit program to triennially audit each Contractor and Authorized Recipient engaging in outsourcing with the first of such audits to be conducted within one year of the signing of the contract.

[8] State or local Authorized Recipients based on State or Federal Statutes shall contact the State Compact Officer/Chief Administrator. Federal or Regulatory Agency Authorized Recipients shall contact the FBI Compact Officer.

[9] If a national criminal history record check of government personnel having access to CHRI is mandated by a state statute approved by the Attorney General under Public Law 92–544, the State Compact Officer/Chief Administrator must ensure Contractor personnel having similar access are either covered by the existing law or that the existing law is amended to include such Contractor personnel prior to authorizing outsourcing initiatives.

Recipient, the Compact Officer/Chief Administrator, and the FBI CJIS Division. During this review, provision will be made to update the Security Program to address security violations and to ensure changes in policies and standards as well as changes in Federal and State law are incorporated.

3.08 The Contractor shall maintain CHRI only for the period of time necessary to fulfill their contractual obligations but not to exceed the period of time that the Authorized Recipient is authorized to maintain and does maintain the CHRI.

3.09 The Contractor shall maintain a log of any dissemination of CHRI.

4.0 Site Security

4.01 The Authorized Recipient shall ensure that the Contractor site is a physically secure location at all times to protect against any unauthorized access to CHRI.

4.02 All visitors to computer centers and/or terminal areas shall be escorted by authorized personnel at all times.

5.0 Dissemination

5.01 Only employees of the Contractor, employees of the Authorized Recipient, and such other persons as may be granted authorization by the Authorized Recipient shall be permitted access to the system.

5.02 The Contractor shall maintain appropriate and reasonable quality assurance procedures.

5.03 Access to the system shall be available only for official purposes consistent with the appended contract. Any dissemination of CHRI data to authorized employees of the Contractor is to be for official purposes only.

5.04 Information contained in or about the system will not be provided to agencies other than the Authorized Recipient or another entity which is specifically designated in the contract.

5.05 The Contractor shall not disseminate CHRI without the consent of the Authorized Recipient, and as specifically authorized by federal and state laws, regulations, and standards as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General.

5.06 An up-to-date log concerning dissemination of CHRI shall be maintained by the Contractor for a minimum one year retention period. This log must clearly identify: (A) The Authorized Recipient and the secondary recipient with unique identifiers, (B) the record disseminated, (C) the date of dissemination, (D) the statutory authority for dissemination, and (E) the means of dissemination.

5.07 The Contractor shall protect against any unauthorized persons gaining access to the equipment, any of the data, or the operational documentation for the system. In no event shall copies of messages or CHRI be disseminated other than as contracted and governed by this Outsourcing Standard.

5.08 All access attempts are subject to recording and routine review for detection of inappropriate or illegal activity.

5.09 The Contractor's system shall be supported by a well-written contingency plan.

6.0 Personnel Security

6.01 If a local, State, or Federal written standard requires a criminal history record check of the Authorized Recipient's personnel with access to CHRI, then a criminal history record check shall be required of the Contractor's employees having access to CHRI. The criminal history record check of Contractor employees at a minimum will be no less stringent than the criminal history record check that is performed on the Authorized Recipient's personnel performing similar functions. Criminal history record checks must be completed prior to performing work under the contract.

6.02 If a local, State, or Federal written standard requires a criminal history record check for support personnel, contractors, and custodial workers who work in a physically secure location, then a criminal history record check shall be required for these individuals, unless these individuals are escorted by authorized personnel at all times. The criminal history record check for these individuals at a minimum will be no less stringent than the criminal history record check that is performed on the Authorized Recipient's support personnel, contractors, and custodial workers performing similar functions. Criminal history record checks must be completed prior to performing work under the contract.

6.03 The Contractor shall ensure that each employee performing work under the contract is aware of the requirements of the Outsourcing Standard and the State and Federal laws governing the security and integrity of CHRI. The Contractor shall confirm that each employee understands the Outsourcing Standard requirements and laws that apply to his/her responsibilities.

6.04 If a criminal history record check is required, the Contractor shall maintain a list of personnel who successfully completed the criminal history record check.

7.0 System Security

7.01 The Contractor's security system shall comply with the CJIS Security Policy in effect at the time the Outsourcing Standard is incorporated into the contract and with successor versions of the CJIS Security Policy as they are made known to the Contractor by the Authorized Recipient.

a. If CHRI can be accessed by unauthorized personnel via Wide Area Network/Local Area Network or the Internet, then the Contractor shall protect the CHRI with firewall-type devices to prevent such unauthorized access. These devices shall implement a minimum firewall profile as specified by the CJIS Security Policy in order to provide a point of defense and a controlled and audited access to CHRI, both from inside and outside the networks.

b. Data encryption shall be required throughout the network, passing CHRI through a shared public carrier network.

7.02 The Contractor shall provide for the secure storage and disposal of all hard copy and media associated with the system to prevent access by unauthorized personnel.

a. CHRI shall be stored in a physically secure location.

b. The Authorized Recipient shall ensure that a procedure is in place for sanitizing all fixed storage media (*e.g.*, disks, drives, backup storage) at the completion of the contract and/or before it is returned for maintenance, disposal, or reuse. Sanitization procedures include overwriting the media and/or degaussing the media.

7.03 To prevent and/or detect unauthorized access to CHRI in transmission or storage, each Authorized Recipient must be identified by an Originating Agency Identifier (ORI) or state assigned identifier, and each Contractor or sub-Contractor must be uniquely identified.

8.0 Security Violations

8.01 *Duties of the Authorized Recipient and Contractor.* a. The Contractor shall develop and maintain a written policy for discipline of Contractor employees who violate the security provisions of the contract, which includes this Outsourcing Standard that is incorporated by reference.

b. Pending investigation, the Contractor shall immediately suspend any employee who commits a security violation from assignments in which he/she has access to CHRI under the contract.

c. The Contractor shall immediately notify the Authorized Recipient of any security violation or termination of the contract, to include unauthorized access to CHRI made available pursuant to the contract. Within five calendar days of such notification, the Contractor shall provide the Authorized Recipient a written report documenting such security violation, any corrective actions taken by the Contractor to resolve such violation, and the date, time, and summary of the prior notification.

d. The Authorized Recipient shall immediately notify the State Compact Officer/Chief Administrator and the FBI Compact Officer of any security violation or termination of the contract, to include unauthorized access to CHRI made available pursuant to the contract. The Authorized Recipient shall provide a written report of any security violation (to include unauthorized access to CHRI by the Contractor) to the State Compact Officer/Chief Administrator, if applicable, and the FBI Compact Officer, within five calendar days of receipt of the written report from the Contractor. The written report must include any corrective actions taken by the Contractor and the Authorized Recipient to resolve such security violation.

8.02 *Termination of the contract by the Authorized Recipient for security violations.*

a. The contract is subject to termination by the Authorized Recipient for security violations involving CHRI obtained pursuant to the contract.

b. The contract is subject to termination by the Authorized Recipient for the Contractor's failure to notify the Authorized Recipient of any security violation or to provide a written report concerning such violation.

c. If the Contractor refuses to or is incapable of taking corrective actions to successfully resolve a security violation, the Authorized Recipient shall terminate the contract.

8.03 *Suspension or termination of the exchange of CHRI for security violations.* a. Notwithstanding the actions taken by the

State Compact Officer, if the Authorized Recipient fails to provide a written report notifying the State Compact Officer/Chief Administrator or the FBI Compact Officer of a security violation, or refuses to or is incapable of taking corrective action to successfully resolve a security violation, the Compact Council or the United States Attorney General may suspend or terminate the exchange of CHRI with the Authorized Recipient pursuant to 28 CFR 906.2(d).

b. If the exchange of CHRI is suspended, it may be reinstated after satisfactory written assurances have been provided to the Compact Council Chairman or the United States Attorney General by the Compact Officer/Chief Administrator, the Authorized Recipient and the Contractor that the security violation has been resolved. If the exchange of CHRI is terminated, the Contractor's records (including media) containing CHRI shall be immediately deleted or returned as specified by the Authorized Recipient.

8.04 The Authorized Recipient shall provide written notice (through the State Compact Officer/Chief Administrator if applicable) to the FBI Compact Officer of the following:

a. The termination of a contract for security violations.

b. Security violations involving the unauthorized access to CHRI.

c. The Contractor's name and unique identification number, the nature of the security violation, whether the violation was intentional, and the number of times the violation occurred.

8.05 The Compact Officer/Chief Administrator, Compact Council and the United States Attorney General reserve the right to investigate or decline to investigate any report of unauthorized access to CHRI.

8.06 The Compact Officer/Chief Administrator, Compact Council, and the United States Attorney General reserve the right to audit the Authorized Recipient and the Contractor's operations and procedures at scheduled or unscheduled times. The Compact Council, the United States Attorney General, and the state are authorized to perform a final audit of the Contractor's systems after termination of the contract.

9.0 Miscellaneous Provisions

9.01 This Outsourcing Standard does not confer, grant, or authorize any rights, privileges, or obligations to any persons other than the Contractor, the Authorized Recipient, Compact Officer/Chief Administrator (where applicable), CJIS Systems Agency, and the FBI.

9.02 The following document is incorporated by reference and made part of this Outsourcing Standard: (1) The CJIS Security Policy.

9.03 The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they provide a minimum basis for the security of the system and the CHRI accessed therefrom and it is understood that there may be terms and conditions of the appended contract which impose more stringent requirements upon the Contractor.[10]

[10] Such conditions could include additional audits, fees, or security requirements.

9.04 The minimum security measures as outlined in this Outsourcing Standard may only be modified by the Compact Council. Conformance to such security measures may not be less stringent than stated in this Outsourcing Standard without the consent of the Compact Council in consultation with the United States Attorney General.

9.05 This Outsourcing Standard may only be modified by the Compact Council and may not be modified by the parties to the appended contract without the consent of the Compact Council.

9.06 Appropriate notices, assurances, and correspondence to the FBI Compact Officer, Compact Council, and the United States Attorney General required by Section 8.0 of this Outsourcing Standard shall be forwarded by First Class Mail to: FBI Compact Officer, 1000 Custer Hollow Road, Module C 3, Clarksburg, WV 26306.

[FR Doc. 04–27489 Filed 12–15–04; 8:45 am]

BILLING CODE 4410–02–P

NATIONAL WOMEN'S BUSINESS COUNCIL

Sunshine Act; Notice of Public Meeting

In accordance with the Women's Business Ownership Act, Public Law 106–554 as amended, the National Women's Business Council (NWBC) would like to announce a forthcoming Council meeting. The meeting will introduce the National Women's Business Council's agenda and action items for fiscal year 2005, included and not limited to procurement, access to capital, access to training and technical assistance, access to markets and affordable health care.

DATE: Tuesday, January 18, 2005.

ADDRESS: The Small Business Administration, Eisenhower Conference Room, 409 3rd Street, SW., 2nd Floor, Washington, DC.

TIME: 9 a.m. to 1 p.m.

STATUS: Open to the public. Attendance by RSVP only.

CONTACT: National Women's Business Council, (202) 205–3850—Katherine Stanley.

Anyone wishing to attend or would like to make an oral presentation at the meeting must contact Katherine Stanley, at (202) 205–6695, no later than Monday, January 10, 2005.

Matthew K. Becker,

Committee Management Officer.

[FR Doc. 04–27616 Filed 12–14–04; 10:23 am]

BILLING CODE 8025–01–P

NUCLEAR REGULATORY COMMISSION

[Docket No. 40–9022]

Notice of Consideration of an Amendment Request Transferring the License for Hartley and Hartley Landfill Site, Kawkawlin Township, Michigan, From SCA Services to SC Holdings, Inc., and Opportunity to Provide Comments and Request a Hearing

AGENCY: Nuclear Regulatory Commission.

ACTION: Notice and opportunity to provide comments and request a hearing.

DATES: Comments must be provided by January 18, 2005. Requests for a hearing must be provided by January 5, 2005.

FOR FURTHER INFORMATION CONTACT: David Nelson, Project Manager, Materials Decommissioning Section, Decommissioning Directorate, Division of Waste Management and Environmental Protection, Office of Nuclear Material Safety and Safeguards, U.S. Nuclear Regulatory Commission, Washington, DC 20555. Telephone: (301) 415–3017; fax number: (301) 415–5397; e-mail: *jbh@nrc.gov.*

SUPPLEMENTARY INFORMATION:

I. Introduction

The Nuclear Regulatory Commission (NRC) is considering issuance of a license amendment to Material License No. SUC–1565 issued to SCA Services (the licensee), to authorize transfer of its license to SC Holdings, Inc. License No. SUC–1565 was issued on June 14, 1995, to SCA Services under Title 10 of the Code of Federal Regulations (10 CFR) part 40 and authorizes SCA Services to possess radioactive materials on site leading to decommissioning of the site.

Pursuant to 10 CFR 40.44, no license issued or granted under the regulations in part 40 shall be transferred, assigned, or in any manner disposed of, either voluntarily or involuntarily, directly or indirectly, through transfer of control of any license to any person unless the Commission shall, after securing full information that the transfer is in accordance with the provisions of the Atomic Energy Act of 1954, as amended (AEA), and shall give its consent in writing. Therefore, before the issuance of an amendment, the NRC will have made the findings required by the AEA, and NRC's regulations. These findings will be documented in a Safety Evaluation Report. An Environmental Assessment (EA) will not be performed because, pursuant to 10 CFR 51.22(c)(21), this action is categorically