SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL ITEMS
OFFEROR TO COMPLETE BLOCKS 12, 17, 23, 24, & 30

1. REQUISITION NO.	PAGE 1 OF
ADM-12-332	28

2. CONTRACT NO.	3. AWARD/EFFECTIVE DATE	4. ORDER NO.	5. SOLICITATION NUMBER	6. SOLICITATION ISSUE DATE
	10-14-2012	NRC-HQ-12-P-10-0151		

7. FOR SOLICITATION INFORMATION CALL:	a. NAME	b. TELEPHONE NO. (No Collect Calls)	8. OFFER DUE DATE/LOCAL TIME
	Jim Leedom	315-405-8102	

9. ISSUED BY CODE 3100

U.S. Nuclear Regulatory Commission
Div. of Contracts
Attn: James Leedom
Mail Stop: TWB-01-B10M
Washington, DC 20555

10. THIS ACQUISITION IS

- [ ] UNRESTRICTED OR [X] SET ASIDE: 100 % FOR:
- [X] SMALL BUSINESS
- [ ] WOMEN-OWNED SMALL BUSINESS (WOSB) ELIGIBLE UNDER THE WOMEN-OWNED SMALL BUSINESS PROGRAM
- [ ] HUBZONE SMALL BUSINESS
- [ ] EDWOSB
- [ ] SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS
- [ ] 8(A)

NAICS: 621112

SIZE STANDARD: $10 Million

11. DELIVERY FOR FOB DESTINATION UNLESS BLOCK IS MARKED	12. DISCOUNT TERMS	13a. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700)	13b. RATING	14. METHOD OF SOLICITATION
[ ] SEE SCHEDULE		[ ]	N/A	[ ] RFQ [ ] IFB [ ] RFP

15. DELIVER TO CODE

U.S. Nuclear Regulatory Commission
Attn: James Leedom
Mail Stop: TWB-01-B10M
11555 Rockville Pike
Rockville MD 20852

16. ADMINISTERED BY CODE 3100

U.S. Nuclear Regulatory Commission
Div. of Contracts
Mail Stop: TWB-01-B10M

Washington, DC 20555

17a. CONTRACTOR/OFFEROR CODE 805198173 FACILITY CODE

BURBACH, RODNEY V M.D., P.C.

5630 WISCONSIN APT 1004

CHEVY CHASE MD 208154456

TELEPHONE NO.

[ ] 17b. CHECK IF REMITTANCE IS DIFFERENT AND PUT SUCH ADDRESS IN OFFER

18a. PAYMENT WILL BE MADE BY CODE 3100

Department of Interior / NBC
NRCPayments@nbc.gov
Attn: Fiscal Services Branch - D2770
7301 W. Mansfield Avenue
Denver CO 80235-2230

PHONE: FAX:

[ ] 18b. SUBMIT INVOICES TO ADDRESS SHOWN IN BLOCK 18a UNLESS BLOCK BELOW IS CHECKED — [ ] SEE ADDENDUM

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES (See CONTINUATION Page)	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
	The purpose of this labor hour purchase order is to provide the Nuclear Regulatory Commission's (NRC) Division of Facilities and Security with mental health evaluations of employees, consultants, contractors and licensee personnel. All work shall be conducted in accordance with the Statement of Work (SOW) and following Federal Regulations: Title 10 Code of Federal Regulations Part 10, Executive Order 12968 and Adjudicative Guidelines for Determining Eligibility for Access to Classified Information.				

(Use Reverse and/or Attach Additional Sheets as Necessary)

25. ACCOUNTING AND APPROPRIATION DATA See CONTINUATION Page

2012-40-51-F-170 D2372 252A 31X0200 Obligate $5,000.00
DUNS# 805198173 FAIMIS# 122024
NAICS: 621112 PSC: Q519

26. TOTAL AWARD AMOUNT (For Govt. Use Only)

$5,000.00

- [ ] 27a. SOLICITATION INCORPORATES BY REFERENCE FAR 52.212-1, 52.212-4. FAR 52.212-3 AND 52.212-5 ARE ATTACHED. ADDENDA — [ ] ARE [ ] ARE NOT ATTACHED.
- [X] 27b. CONTRACT/PURCHASE ORDER INCORPORATES BY REFERENCE FAR 52.212-4. FAR 52.212-5 IS ATTACHED. ADDENDA — [ ] ARE [X] ARE NOT ATTACHED
- [X] 28. CONTRACTOR IS REQUIRED TO SIGN THIS DOCUMENT AND RETURN 1 COPIES TO ISSUING OFFICE. CONTRACTOR AGREES TO FURNISH AND DELIVER ALL ITEMS SET FORTH OR OTHERWISE IDENTIFIED ABOVE AND ON ANY ADDITIONAL SHEETS SUBJECT TO THE TERMS AND CONDITIONS SPECIFIED
- [X] 29. AWARD OF CONTRACT: REF. Dr. Rodney Burbach OFFER DATED 06-09-2012 YOUR OFFER ON SOLICITATION (BLOCK 5), INCLUDING ANY ADDITIONS OR CHANGES WHICH ARE SET FORTH HEREIN IS ACCEPTED AS TO ITEMS:

30a. SIGNATURE OF OFFEROR/CONTRACTOR

Rodney V. Burbach MD

31a. UNITED STATES OF AMERICA (SIGNATURE OF CONTRACTING OFFICER)

30b. NAME AND TITLE OF SIGNER (TYPE OR PRINT)	30c. DATE SIGNED	31b. NAME OF CONTRACTING OFFICER (TYPE OR PRINT)	31c. DATE SIGNED
Rodney V. Burbach, MD	07/05/12	Stephen Pool Contracting Officer	7/2/12

AUTHORIZED FOR LOCAL REPRODUCTION
PREVIOUS EDITION IS NOT USABLE

STANDARD FORM 1449 (REV. 2/2012)
Prescribed by GSA - FAR (48 CFR) 53.212

SUNSI REVIEW COMPLETE

JUL 10 2012

TEMPLATE - ADM001

ADM002

Table of Contents

CONTINUATION PAGE

A.2 PRICE/COST SCHEDULE

ITEM NO.	DESCRIPTION OF SUPPLIES/SVCS	QTY	UNIT	UNIT PRICE	AMOUNT
0001	Mental Health Review Officer - Base Period - October 14, 2012 - October 13, 2013 NAICS Code Description: Offices of Physicians, Mental Health Specialists FUNDING/REQ NO: 1: $5,000.00 ADM-12-332	85	hours	[redacted]	[redacted]
1001	Mental Health Review Officer - Option Period 1 - October 14, 2013 - October 13, 2014 NAICS Code Description: Offices of Physicians, Mental Health Specialists	85	hours	[redacted]	[redacted]
2001	Mental Health Review Officer - Option Period 2 - October 14, 2014 - October 13, 2015 NAICS Code Description: Offices of Physicians, Mental Health Specialists	85	hours	[redacted]	[redacted]
3001	Mental Health Review Officer - Option Period 3 - October 14, 2015 - October 13, 2016 NAICS Code Description: Offices of Physicians, Mental Health Specialists	85	hours	[redacted]	[redacted]
4001	Mental Health Review Officer - Option Period 4 - October 14, 2016 - October 13, 2017 NAICS Code Description: Offices of Physicians, Mental Health Specialists	85	hours	[redacted]	[redacted]
	GRAND TOTAL ---				[redacted]

ACCOUNTING AND APPROPRIATION DATA:

ACRN	APPROPRIATION	REQUISITION NUMBER	AMOUNT
1	2012-40-51-F-170-JCN-D2372-BOC-252A-APPNUMBER-31X0200	ADM-12-332 P	[redacted]

A.3 CONSIDERATION AND OBLIGATION-LABOR-HOUR CONTRACT (AUG 2011)

(a) The ceiling price to the Government for full performance under this contract is $66,725.00.

(b) The contract includes direct labor hours at specified fixed hourly rates, inclusive of wages, fringe, overhead, general and administrative expenses, and profit.

(c) It is estimated that the amount currently obligated will cover performance through 03-13-2013.

(d) This is an incrementally-funded contract and FAR 52.232-22 - "Limitation of Funds" applies.

A.4 PERIOD OF PERFORMANCE (AUG 2011) ALTERNATE III (AUG 2011)

This contract shall commence on 10-14-2012 and will expire on 10-13-2013. The term of this contract may be extended at the option of the Government for an additional four option periods, from 10-14-2013 to 10-13-2017. The term of this contract may be extended at the option of the Government for an additional four option periods.

Base Period: October 14, 2012 - October 13, 2013 Option Period(s): 4

ADDITIONAL SIMPLIFIED ACQUISITION TERMS AND CONDITIONS

A.5 NOTICE LISTING CLAUSES INCORPORATED BY REFERENCE

The following clauses are hereby incorporated by reference (by Citation Number, Title, and Date) in accordance with the clause at FAR "52.252-2 CLAUSES INCORPORATED BY REFERENCE" contained in this document. FAR 52.252-2 contains the internet address for electronic access to the full text of a clause.

NUMBER	TITLE	DATE
	FEDERAL ACQUISITION REGULATION (48 CFR Chapter 1)	
52.212-4	CONTRACT TERMS AND CONDITIONS--COMMERCIAL ITEMS	FEB 2012
52.224-1	PRIVACY ACT NOTIFICATION	APR 1984
52.224-2	PRIVACY ACT	APR 1984
52.232-18	AVAILABILITY OF FUNDS	APR 1984
52.232-22	LIMITATION OF FUNDS	APR 1984
52.245-1	GOVERNMENT PROPERTY	APR 2012

A.6 52.212-5 CONTRACT TERMS AND CONDITIONS REQUIRED TO IMPLEMENT STATUTES OR EXECUTIVE ORDERS--COMMERCIAL ITEMS (MAY 2012)

(a) The Contractor shall comply with the following Federal Acquisition Regulation (FAR) clauses, which are incorporated in this contract by reference, to implement provisions of law or Executive orders applicable to acquisitions of commercial items:

(1) 52.222-50, Combating Trafficking in Persons (FEB 2009) (22 U.S.C. 7104(g)).

Alternate I (AUG 2007) of 52.222-50 (22 U.S.C. 7104 (g)).

(2) 52.233-3, Protest After Award (Aug 1996) (31 U.S.C. 3553).

(3) 52.233-4, Applicable Law for Breach of Contract Claim (Oct 2004) (Pub. L. 108-77, 108-78)

(b) The Contractor shall comply with the FAR clauses in this paragraph (b) that the Contracting Officer has indicated as being incorporated in this contract by reference to implement provisions of law or Executive orders applicable to acquisitions of commercial items:

[] (1) 52.203-6, Restrictions on Subcontractor Sales to the Government (Sept 2006), with Alternate I (Oct 1995) (41 U.S.C. 253g and 10 U.S.C. 2402).

[] (2) 52.203-13, Contractor Code of Business Ethics and Conduct (APR 2010)(Pub. L. 110-252, Title VI, Chapter 1 (41 U.S.C. 251 note)).

[] (3) 52.203-15, Whistleblower Protections under the American Recovery and Reinvestment Act of 2009 (JUN 2010) (Section 1553 of Pub. L. 111-5). (Applies to contracts funded by the American Recovery and Reinvestment Act of 2009.)

[] (4) 52.204-10, Reporting Executive Compensation and First-Tier Subcontract Awards (FEB 2012) (Pub. L. 109-282) (31 U.S.C. 6101 note).

[] (5) 52.204-11, American Recovery and Reinvestment Act-Reporting Requirements (JUL 2010) (Pub. L. 111-5).

[x] (6) 52.209-6, Protecting the Government's Interest When Subcontracting with Contractors Debarred, Suspended, or Proposed for Debarment. (Dec 2010) (31 U.S.C. 6101 note).

[] (7) 52.209-9, Updates of Publicly Available Information Regarding Responsibility Matters (FEB 2012) (41 U.S.C. 2313).

[] (8) 52.209-10, Prohibition on Contracting with Inverted Domestic Corporations (MAY 2012) (section 738 of Division C of Pub. L. 112-74, section 740 of Division C of Pub. L. 111-117, section 743 of Division D of Pub. L. 111-8, and section 745 of Division D of Pub. L. 110-161).

[] (9) 52.219-3, Notice of HUBZone Set-Aside or Sole-Source Award (NOV 2011) (15 U.S.C. 657a).

[] (10) 52.219-4, Notice of Price Evaluation Preference for HUBZone Small Business Concerns (JAN 2011) (if the offeror elects to waive the preference, it shall so indicate in its offer) (15 U.S.C. 657a).

[] (11) [Reserved]

[X] (12)(i) 52.219-6, Notice of Total Small Business Set-Aside (NOV 2011) (15 U.S.C. 644).

[] (ii) Alternate I (NOV 2011).

[] (iii) Alternate II (NOV 2011).

[] (13)(i) 52.219-7, Notice of Partial Small Business Set-Aside (June 2003) (15 U.S.C. 644).

[] (ii) Alternate I (Oct 1995) of 52.219-7.

[] (iii) Alternate II (Mar 2004) of 52.219-7.

[] (14) 52.219-8, Utilization of Small Business Concerns (JAN 2011) (15 U.S.C. 637(d)(2) and (3)).

[] (15)(i) 52.219-9, Small Business Subcontracting Plan (JAN 2011) (15 U.S.C. 637(d)(4)).

[] (ii) Alternate I (Oct 2001) of 52.219-9.

[] (iii) Alternate II (Oct 2001) of 52.219-9.

[] (iv) Alternate III (JUL 2010) of 52.219-9.

[] (16) 52.219-13, Notice of Set-Aside of Orders (NOV 2011) (15 U.S.C. 644(r)).

[] (17) 52.219-14, Limitations on Subcontracting (NOV 2011) (15 U.S.C. 637(a)(14)).

[] (18) 52.219-16, Liquidated Damages--Subcontracting Plan (Jan 1999) (15 U.S.C. 637(d)(4)(F)(i)).

[] (19)(i) 52.219-23, Notice of Price Evaluation Adjustment for Small Disadvantaged Business Concerns (OCT 2008) (10 U.S.C. 2323) (if the offeror elects to waive the adjustment, it shall so indicate in its offer.)

[] (ii) Alternate I (June 2003) of 52.219-23.

[] (20) 52.219-25, Small Disadvantaged Business Participation Program–Disadvantaged Status and Reporting (DEC 2010) (Pub. L. 103-355, section 7102, and 10 U.S.C. 2323).

[] (21) 52.219-26, Small Disadvantaged Business Participation Program–Incentive Subcontracting (Oct 2000) (Pub. L. 103-355, section 7102, and 10 U.S.C. 2323).

[] (22) 52.219-27, Notice of Service-Disabled Veteran-Owned Small Business Set-Aside (NOV 2011) (15 U.S.C. 657f).

[x] (23) 52.219-28, Post Award Small Business Program Rerepresentation (APR 2012) (15 U.S.C 632(a)(2)).

[] (24) 52.219-29, Notice of Set-Aside for Economically Disadvantaged Women-Owned Small Business (EDWOSB) Concerns (APR 2012) (15 U.S.C. 637(m)).

[] (25) 52.219-30, Notice of Set-Aside for Women-Owned Small Business (WOSB) Concerns Eligible Under the WOSB Program (APR 2012) (15 U.S.C. 637(m)).

[X] (26) 52.222-3, Convict Labor (June 2003) (E.O. 11755).

[x] (27) 52.222-19, Child Labor–Cooperation with Authorities and Remedies (MAR 2012) (E.O. 13126).

[x] (28) 52.222-21, Prohibition of Segregated Facilities (Feb 1999).

[x] (29) 52.222-26, Equal Opportunity (Mar 2007) (E.O. 11246).

[x] (30) 52.222-35, Equal Opportunity for Veterans (SEP 2010) (38 U.S.C. 4212).

[x] (31) 52.222-36, Affirmative Action for Workers with Disabilities (Oct 2010) (29 U.S.C. 793).

[x] (32) 52.222-37, Employment Reports on Veterans (SEP 2010) (38 U.S.C. 4212).

[] (33) 52.222-40, Notification of Employee Rights Under the National Labor Relations Act (DEC 2010) (E.O. 13496).

[] (34) 52.222-54, Employment Eligibility Verification (Jan 2009). (Executive Order 12989). (Not applicable to the acquisition of commercially available off-the-shelf items or certain other types of commercial items as prescribed in 22.1803.)

[] (35)(i) 52.223-9, Estimate of Percentage of Recovered Material Content for EPA-Designated Items (May 2008) (42 U.S.C.6962(c)(3)(A)(ii)). (Not applicable to the acquisition of commercially available off-the-shelf items.)

[] (ii) Alternate I (MAY 2008) of 52.223-9 (42 U.S.C. 6962(i)(2)(C)). (Not applicable to the acquisition of commercially available off-the-shelf items.)

[] (36) 52.223-15, Energy Efficiency in Energy-Consuming Products (DEC 2007)(42 U.S.C. 8259b).

[] (37)(i) 52.223-16, IEEE 1680 Standard for the Environmental Assessment of Personal Computer Products (DEC 2007) (E.O. 13423).

[] (ii) Alternate I (DEC 2007) of 52.223-16.

[X] (38) 52.223-18, Encouraging Contractor Policies to Ban Text Messaging While Driving (AUG 2011)

[x] (39) 52.225-1, Buy American Act--Supplies (FEB 2009) (41 U.S.C. 10a-10d).

[] (40)(i) 52.225-3, Buy American Act--Free Trade Agreements-- Israeli Trade Act (MAY 2012) (41 U.S.C. chapter 83, 19 U.S.C. 3301 note, 19 U.S.C. 2112 note, 19 U.S.C. 3805 note, 19 U.S.C. 4001 note, Pub. L. 103-182, 108-77, 108-78, 108-286, 108-302, 109-53, 109-169, 109-283, 110-138, 112-41, and 112-42).

[] (ii) Alternate I (MAR 2012) of 52.225-3.

[] (iii) Alternate II (MAR 2012) of 52.225-3.

[] (iv) Alternate III (MAR 2012) of 52.225-3.

[] (41) 52.225-5, Trade Agreements (MAY 2012) (19 U.S.C. 2501, et seq., 19 U.S.C. 3301 note).

[X] (42) 52.225-13, Restrictions on Certain Foreign Purchases (JUN 2008) (E.O.'s, proclamations, and statutes administered by the Office of Foreign Assets Control of the Department of the Treasury).

[] (43) 52.226-4, Notice of Disaster or Emergency Area Set-Aside (Nov 2007) (42 U.S.C. 5150).

[] (44) 52.226-5, Restrictions on Subcontracting Outside Disaster or Emergency Area (Nov 2007) (42 U.S.C. 5150).

[] (45) 52.232-29, Terms for Financing of Purchases of Commercial Items (Feb 2002) (41 U.S.C. 255(f), 10 U.S.C. 2307(f)).

[] (46) 52.232-30, Installment Payments for Commercial Items (Oct 1995) (41 U.S.C. 255(f), 10 U.S.C. 2307(f)).

[X] (47) 52.232-33, Payment by Electronic Funds Transfer--Central Contractor Registration (Oct 2003) (31 U.S.C. 3332).

[] (48) 52.232-34, Payment by Electronic Funds Transfer--Other than Central Contractor Registration (May 1999) (31 U.S.C. 3332).

[] (49) 52.232-36, Payment by Third Party (FEB 2010) (31 U.S.C. 3332).

[] (50) 52.239-1, Privacy or Security Safeguards (Aug 1996) (5 U.S.C. 552a).

[] (51)(i) 52.247-64, Preference for Privately Owned U.S.-Flag Commercial Vessels (Feb 2006) (46 U.S.C. Appx. 1241(b) and 10 U.S.C. 2631).

[] (ii) Alternate I (Apr 2003) of 52.247-64.

(c) The Contractor shall comply with the FAR clauses in this paragraph (c), applicable to commercial services, that the Contracting Officer has indicated as being incorporated in this contract by reference to implement provisions of law or Executive orders applicable to acquisitions of commercial items:

[] (1) 52.222-41, Service Contract Act of 1965 (Nov 2007) (41 U.S.C. 351, et seq.).

[] (2) 52.222-42, Statement of Equivalent Rates for Federal Hires (May 1989) (29 U.S.C. 206 and 41 U.S.C. 351, et seq.).

Employee Class	Monetary Wage-Fringe Benefits

[] (3) 52.222-43, Fair Labor Standards Act and Service Contract Act--Price Adjustment (Multiple Year and Option Contracts) (Sep 2009) (29 U.S.C. 206 and 41 U.S.C. 351, et seq.).

[] (4) 52.222-44, Fair Labor Standards Act and Service Contract Act--Price Adjustment (Sep 2009) (29 U.S.C. 206 and 41 U.S.C. 351, et seq.).

[] (5) 52.222-51, Exemption from Application of the Service Contract Act to Contracts for Maintenance, Calibration, or Repair of Certain Equipment--Requirements (Nov 2007) (41 U.S.C. 351, et seq.).

[] (6) 52.222-53, Exemption from Application of the Service Contract Act to Contracts for Certain Services--Requirements (FEB 2009) (41 U.S.C. 351, et seq.).

[] (7) 52.226-6, Promoting Excess Food Donation to Nonprofit Organizations. (MAR 2009)(Pub. L. 110-247)

[] (8) 52.237-11, Accepting and Dispensing of $1 Coin (SEP 2008) (31 U.S.C. 5112(p)(1)).

(d) Comptroller General Examination of Record. The Contractor shall comply with the provisions of this paragraph (d) if this contract was awarded using other than sealed bid, is in excess of the simplified acquisition threshold, and does not contain the clause at 52.215-2, Audit and Records--Negotiation.

(1) The Comptroller General of the United States, or an authorized representative of the Comptroller General, shall have access to and right to examine any of the Contractor's directly pertinent records involving transactions related to this contract.

(2) The Contractor shall make available at its offices at all reasonable times the records, materials, and other evidence for examination, audit, or reproduction, until 3 years after final payment under this contract or for any shorter period specified in FAR Subpart 4.7, Contractor Records Retention, of the other clauses of this contract. If this contract is completely or partially terminated, the records relating to the work terminated shall be made available for 3 years after any resulting final termination settlement. Records relating to appeals under the disputes clause or to litigation or the settlement of claims arising under or relating to this contract shall be made available until such appeals, litigation, or claims are finally resolved.

(3) As used in this clause, records include books, documents, accounting procedures and practices, and other data, regardless of type and regardless of form. This does not require the Contractor to create or maintain any record that the Contractor does not maintain in the ordinary course of business or pursuant to a provision of law.

(e)(1) Notwithstanding the requirements of the clauses in paragraphs (a), (b), (c), and (d) of this clause, the Contractor is not required to flow down any FAR clause, other than those in this paragraph (e)(1) in a subcontract for commercial items. Unless otherwise indicated below, the extent of the flow down shall be as required by the clause--

(i) 52.203-13, Contractor Code of Business Ethics and Conduct (APR 2010) (Pub. L. 110-252, Title VI, Chapter 1 (41 U.S.C. 251 note)).

(ii) 52.219-8, Utilization of Small Business Concerns (DEC 2010) (15 U.S.C. 637(d)(2) and (3)), in all subcontracts that offer further subcontracting opportunities. If the subcontract (except subcontracts to small business concerns) exceeds $650,000 ($1.5 million for construction of any public facility), the subcontractor must include 52.219-8 in lower tier subcontracts that offer subcontracting opportunities.

(iii) [Reserved]

(iv) 52.222-26, Equal Opportunity (Mar 2007) (E.O. 11246).

(v) 52.222-35, Equal Opportunity for Veterans (SEP 2010) (38 U.S.C. 4212).

(vi) 52.222-36, Affirmative Action for Workers with Disabilities (Oct 2010) (29 U.S.C. 793).

(vii) 52.222-40, Notification of Employee Rights Under the National Labor Relations Act (DEC 2010) (E.O. 13496). Flow down required in accordance with paragraph (f) of FAR clause 52.222-40.

(viii) 52.222-41, Service Contract Act of 1965 (Nov 2007) (41 U.S.C. 351, et seq.).

(ix) 52.222-50, Combating Trafficking in Persons (FEB 2009) (22 U.S.C. 7104(g)).

Alternate I (AUG 2007) of 52.222-50 (22 U.S.C. 7104(g)).

(x) 52.222-51, Exemption from Application of the Service Contract Act to Contracts for Maintenance, Calibration, or Repair of Certain Equipment–Requirements "(Nov 2007)" (41 U.S.C. 351, et seq.).

(xi) 52.222-53, Exemption from Application of the Service Contract Act to Contracts for Certain Services-Requirements (FEB 2009)(41 U.S.C. 351, et seq.).

(xii) 52.222-54, Employee Eligibility Verification (JAN 2009)

(xiii) 52.226-6, Promoting Excess Food Donation to Nonprofit Organizations. (MAR 2009)(Pub. L. 110-247). Flow down required in accordance with paragraph (e) of FAR clause 52.226-6.

(xiv) 52.247-64, Preference for Privately Owned U.S.-Flag Commercial Vessels (Feb 2006) (46 U.S.C. Appx. 1241(b) and 10 U.S.C. 2631). Flow down required in accordance with paragraph (d) of FAR clause 52.247-64.

(2) While not required, the contractor may include in its subcontracts for commercial items a minimal number of additional clauses necessary to satisfy its contractual obligations.

A.7 52.217-8 OPTION TO EXTEND SERVICES (NOV 1999)

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed 6 months. The Contracting Officer may exercise the option by written notice to the Contractor within 15 days of contract expiration.

A.8 52.217-9 OPTION TO EXTEND THE TERM OF THE CONTRACT (MAR 2000)

(a) The Government may extend the term of this contract by written notice to the Contractor within 15 days of contract expiration; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 30 days before the contract expires. The preliminary notice does not commit the Government to an extension.

(b) If the Government exercises this option, the extended contract shall be considered to include this option clause.

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed five (5) years.

A.9 2052.215-71 CONTRACTING OFFICER REPRESENTATIVE (COR) AUTHORITY (NOVEMBER 2006)

(a) The contracting officer's authorized representative (hereinafter referred to as the COR) for this contract is:

Name: Janice Kelsh

Address: U.S. Nuclear Regulatory Commission
Mail Stop: TWB-05-B32M
11555 Rockville Pike
Rockville, MD 20852

Telephone Number: 301-492-3530

(b) Performance of the work under this contract is subject to the technical direction of the NRC COR. The term "technical direction" is defined to include the following:

(1) Technical direction to the contractor which shifts work emphasis between areas of work or tasks, authorizes travel which was unanticipated in the Schedule (i.e., travel not contemplated in the Statement of Work (SOW) or changes to specific travel identified in the SOW), fills in details, or otherwise serves to accomplish the contractual SOW.

(2) Provide advice and guidance to the contractor in the preparation of drawings, specifications, or technical portions of the work description.

(3) Review and, where required by the contract, approval of technical reports, drawings, specifications, and technical information to be delivered by the contractor to the Government under the contract.

(c) Technical direction must be within the general statement of work stated in the contract. The COR does not have the authority to and may not issue any technical direction which:

(1) Constitutes an assignment of work outside the general scope of the contract.

(2) Constitutes a change as defined in the "Changes" clause of this contract.

(3) In any way causes an increase or decrease in the total estimated contract cost, the fixed fee, if any, or the time required for contract performance.

(4) Changes any of the expressed terms, conditions, or specifications of the contract.

(5) Terminates the contract, settles any claim or dispute arising under the contract, or issues any unilateral directive whatever.

(d) All technical directions must be issued in writing by the COR or must be confirmed by the project officer in writing within ten (10) working days after verbal issuance. A copy of the written direction must be furnished to the contracting officer. A copy of NRC Form 445, Request for Approval of Official Foreign Travel, which has received final approval from the NRC must be furnished to the contracting officer.

(e) The contractor shall proceed promptly with the performance of technical directions duly issued by the project officer in the manner prescribed by this clause and within the project officer's authority under the provisions of this clause.

(f) If, in the opinion of the contractor, any instruction or direction issued by the COR is within one of the categories as defined in paragraph (c) of this section, the contractor may not proceed but shall notify the contracting officer in writing within five (5) working days after the receipt of any instruction or direction and shall request the contracting officer to modify the contract accordingly. Upon receiving the notification from the contractor, the contracting officer shall issue an appropriate contract modification or advise the contractor in writing that, in the contracting officer's opinion, the technical direction is within the scope of this article and does not constitute a change under the "Changes" clause.

(g) Any unauthorized commitment or direction issued by the COR may result in an unnecessary delay in the contractor's performance and may even result in the contractor expending funds for unallowable costs under the contract.

(h) A failure of the parties to agree upon the nature of the instruction or direction or upon the contract action to be taken with respect thereto is subject to 52.233-1 -Disputes.

(i) In addition to providing technical direction as defined in paragraph (b) of the section, the project officer shall:

(1) Monitor the contractor's technical progress, including surveillance and assessment of performance, and recommend to the contracting officer changes in requirements.

(2) Assist the contractor in the resolution of technical problems encountered during performance.

(3) Review all costs requested for reimbursement by the contractor and submit to the contracting officer recommendations for approval, disapproval, or suspension of payment for supplies and services required under this contract.

(4) Assist the contractor in obtaining the badges for the contractor personnel.

(5) Immediately notify the Security Branch, Division of Facilities and Security (SB/DFS) (via e-mail) when a contractor employee no longer requires access authorization and return of any NRC issued badge to SB/DFS within three days after their termination.

(6) Ensure that all contractor employees that require access to classified Restricted Data or National Security Information or matter, access to sensitive unclassified information (Safeguards, Official Use Only, and Proprietary information) access to sensitive IT systems or data, unescorted access to NRC controlled buildings/space, or unescorted access to protected and vital areas of nuclear power plants receive approval of SB/DFS prior to access in accordance with Management Directive and Handbook 12.3.

(7) For contracts for the design, development, maintenance or operation of Privacy Act Systems of Records, obtain from the contractor as part of closeout procedures, written certification that the contractor has returned to NRC, transferred to the successor contractor, or destroyed at the end of the contract in accordance with instructions provided by the NRC Systems Manager for Privacy Act Systems of Records, all records (electronic or paper) which were created, compiled, obtained or maintained under the contract.

A.10 2052.215-70 KEY PERSONNEL (JAN 1993)

(a) The following individuals are considered to be essential to the successful performance of the work hereunder:

Dr. Rodney Burbach	Mental Health Review Officer

The contractor agrees that personnel may not be removed from the contract work or replaced without compliance with paragraphs (b) and (c) of this section.

(b) If one or more of the key personnel, for whatever reason, becomes, or is expected to become, unavailable for work under this contract for a continuous period exceeding 30 work days, or is expected to devote substantially less effort to the work than indicated in the proposal or initially anticipated, the contractor shall immediately notify the contracting officer and shall, subject to the concurrence of the contracting officer, promptly replace the personnel with personnel of at least substantially equal ability and qualifications.

(c) Each request for approval of substitutions must be in writing and contain a detailed explanation of the circumstances necessitating the proposed substitutions. The request must also contain a complete resume for the proposed substitute and other information requested or needed by the contracting officer to evaluate the proposed substitution. The contracting officer and the project officer shall evaluate the contractor's request and the contracting officer shall promptly notify the contractor of his or her decision in writing.

(d) If the contracting officer determines that suitable and timely replacement of key personnel who have been reassigned, terminated, or have otherwise become unavailable for the contract work is not reasonably forthcoming, or that the resultant reduction of productive effort would be so substantial as to impair the successful completion of the contract or the service order, the contract may be terminated by the contracting officer for default or for the convenience of the Government, as appropriate. If the contracting officer finds the contractor at fault for the condition, the contract price or fixed fee may be equitably adjusted downward to compensate the Government for any resultant delay, loss, or damage.

A.11 2052.204.70 SECURITY (MAR 2004)

(a) Contract Security and/or Classification Requirements (NRC Form 187). The policies, procedures, and criteria of the NRC Security Program, NRC Management Directive (MD) 12 (including MD 12.1, "NRC Facility Security Program;" MD 12.2, "NRC Classified Information Security Program;" MD 12.3, "NRC Personnel Security Program;" MD 12.4, "NRC Telecommunications Systems Security Program;" MD 12.5, "NRC Automated Information Systems Security Program;" and MD 12.6, "NRC Sensitive Unclassified Information Security Program"), apply to performance of this contract, subcontract or other activity. This MD is incorporated into this contract by reference as though fully set forth herein. The attached NRC Form 187 (See List of Attachments) furnishes the basis for providing security and classification requirements to prime contractors, subcontractors, or others (e.g., bidders) who have or may have an NRC contractual relationship that requires access to classified Restricted Data or National Security Information or matter, access to sensitive unclassified information (e.g., Safeguards), access to sensitive Information Technology (IT) systems or data, unescorted access to NRC controlled buildings/space, or unescorted access to protected and vital areas of nuclear power plants.

(b) It is the contractor's duty to protect National Security Information, Restricted Data, and Formerly Restricted Data. The contractor shall, in accordance with the Commission's security regulations and requirements, be responsible for protecting National Security Information, Restricted Data, and Formerly Restricted Data, and for protecting against sabotage, espionage, loss, and theft, the classified documents and material in the contractor's possession in connection with the performance of work under this contract. Except as otherwise expressly provided in this contract, the contractor shall, upon completion or termination of this contract, transmit to the Commission any classified matter in the possession of the contractor or any person under the contractor's control in connection with performance of this contract. If retention by the contractor of any classified matter is required after the completion or termination of the contract and the retention is approved by the contracting officer, the contractor shall complete a certificate of possession to be furnished to the Commission specifying the classified matter to be retained. The certification must identify the items and types or categories of matter retained, the conditions governing the retention of the matter and their period of retention, if known. If the retention is approved by the contracting officer, the security provisions of the contract continue to be applicable to the matter retained.

(c) In connection with the performance of the work under this contract, the contractor may be furnished, or may develop or acquire, safeguards information, or confidential or privileged technical, business, or financial information, including Commission plans, policies, reports, financial plans, internal data protected by the Privacy Act of 1974 (Pub. L. 93.579), or other information which has not been released to the public or has been determined by the Commission to be otherwise exempt from disclosure to the public. The contractor shall ensure that information protected from public disclosure is maintained as required by NRC regulations and policies, as cited in this contract or as otherwise provided by the NRC. The contractor will not directly or indirectly duplicate, disseminate, or disclose the information in whole or in part to any other person or organization except as may be necessary to perform the work under this contract. The contractor agrees to return the information to the Commission or otherwise dispose of it at the direction of the contracting officer. Failure to comply with this clause is grounds for termination of this contract.

(d) Regulations. The contractor agrees to conform to all security regulations and requirements of the Commission which are subject to change as directed by the NRC Division of Facilities and Security (DFS) and the Contracting Officer. These changes will be under the authority of the FAR Changes clause referenced in this document.

The contractor agrees to comply with the security requirements set forth in NRC Management Directive 12.1, NRC Facility Security Program which is incorporated into this contract by reference as though fully set forth herein. Attention is directed specifically to the section titled "Infractions and Violations," including "Administrative Actions" and "Reporting Infractions."

(e) Definition of National Security Information. The term National Security Information, as used in this clause, means information that has been determined pursuant to Executive Order 12958 or any predecessor order to require protection against unauthorized disclosure and that is so designated.

(f) Definition of Restricted Data. The term Restricted Data, as used in this clause, means all data concerning design, manufacture, or utilization of atomic weapons; the production of special nuclear material; or the use of special nuclear material in the production of energy, but does not include data declassified or removed from the Restricted Data category pursuant to Section 142 of the Atomic Energy Act of 1954, as amended.

(g) Definition of Formerly Restricted Data. The term Formerly Restricted Data, as used in this clause, means all data removed from the Restricted Data category under Section 142-d of the Atomic Energy Act of 1954, as amended.

(h) Definition of Safeguards Information. Sensitive unclassified information that specifically identifies the detailed security measures of a licensee or an applicant for the physical protection of special nuclear material; or security measures for the physical protection and location of certain plant equipment vital to the safety of production of utilization facilities. Protection of this information is required pursuant to Section 147 of the Atomic Energy Act of 1954, as amended.

(i) Security Clearance. The contractor may not permit any individual to have access to Restricted Data, Formerly Restricted Data, or other classified information, except in accordance with the Atomic Energy Act of 1954, as amended, and the Commission's regulations or requirements applicable to the particular type or category of classified information to which access is required. The contractor shall also execute a Standard Form 312, Classified Information Nondisclosure Agreement, when access to classified information is required.

(j) Criminal Liabilities. It is understood that disclosure of National Security Information, Restricted Data, and Formerly Restricted Data relating to the work or services ordered hereunder to any person not entitled to receive it, or failure to safeguard any Restricted Data, Formerly Restricted Data, or any other classified matter that may come to the contractor or any person under the contractor's control in connection with work under this contract, may subject the contractor, its agents, employees, or subcontractors to criminal liability under the laws of the United States. (See the Atomic Energy Act of 1954, as amended, 42 U.S.C. 2011 et seq.; 18 U.S.C. 793 and 794; and Executive Order 12958.)

(k) Subcontracts and Purchase Orders. Except as otherwise authorized in writing by the contracting officer, the contractor shall insert provisions similar to the foregoing in all subcontracts and purchase orders under this contract.

(l) In performing the contract work, the contractor shall classify all documents, material, and equipment originated or generated by the contractor in accordance with guidance issued by the Commission. Every subcontract and purchase order issued hereunder involving the origination or generation of classified documents, material, and equipment must provide that the subcontractor or supplier assign classification to all documents, material, and equipment in accordance with guidance furnished by the contractor.

A.12 2052.204-71 BADGE REQUIREMENTS FOR UNESCORTED BUILDING ACCESS TO NRC FACILITIES (MAR 2006)

During the life of this contract, the rights of ingress and egress for contractor personnel must be made available, as required, provided that the individual has been approved for unescorted access after a favorable adjudication from the Security Branch, Division of Facilities and Security (SB/DFS).

In this regard, all contractor personnel whose duties under this contract require their presence on site shall be clearly identifiable by a distinctive badge furnished by the NRC. The Project Officer shall assist the contractor in obtaining badges for the contractor personnel. All contractor personnel must present two forms of Identity Source Documents (I-9). One of the documents must be a valid picture ID issued by a state or by the Federal Government. Original I-9 documents must be presented in person for certification. A list of acceptable documents can be found at http://www.usdoj.gov/crt/recruit_employ/i9form.pdf. It is the sole responsibility of the contractor to ensure that each employee has a proper NRC-issued identification/badge at all times. All photo-identification badges must be immediately (no later than three days) delivered to SB/DFS for cancellation or disposition upon the termination of employment of any contractor personnel. Contractor personnel must display any NRC issued badge in clear view at all times during on site performance under this contract. It is the contractor's duty to assure that contractor personnel enter only those work areas necessary for performance of contract work, and to assure the protection of any Government records or data that contractor personnel may come into contact with.

A.13 SECURITY REQUIREMENTS FOR BUILDING ACCESS APPROVAL (AUG 2011)

The Contractor shall ensure that all its employees, subcontractor employees or consultants who are assigned to perform the work herein for contract performance for periods of more than 30 calendar days at NRC facilities, are approved by the NRC for unescorted NRC building access.

The Contractor shall conduct a preliminary federal facilities security screening interview or review for each of its employees, subcontractor employees, and consultants and submit to the NRC only the names of candidates for contract performance that have a reasonable probability of obtaining approval necessary for access to NRC's federal facilities. The Contractor shall pre-screen its applicants for the following:

(a) felony arrest in the last seven (7) years; (b) alcohol related arrest within the last five (5) years; (c) record of any military courts-martial convictions in the past ten (10) years; (d) illegal use of narcotics or other controlled substances possession in the past year, or illegal purchase, production, transfer, or distribution of narcotics or other controlled substances in the last seven (7) years; and (e) delinquency on any federal debts or bankruptcy in the last seven (7) years.

The Contractor shall make a written record of its pre-screening interview or review (including any information to mitigate the responses to items listed in (a) - (e)), and have the applicant verify the pre-screening record or review, sign and date it. Two (2) copies of the pre-screening signed record or review shall be supplied to the Division of Facilities and Security, Personnel Security Branch (DFS/PSB) with the Contractor employee's completed building access application package.

The Contractor shall further ensure that its employees, any subcontractor employees and consultants complete all building access security applications required by this clause within fourteen (14) calendar days of notification by DFS/PSB of initiation of the application process. Timely receipt of properly completed records of the Contractor's signed pre-screening record or review and building access security applications (submitted for candidates that have a reasonable probability of obtaining the level of access authorization necessary for access to NRC's facilities) is a contract requirement. Failure of the Contractor to comply with this contract administration requirement may be a basis to cancel the award, or terminate the contract for default, or offset from the contract's invoiced cost or price the NRC's incurred costs or delays as a result of inadequate pre-screening by the Contractor. In the event of cancellation or termination, the NRC may select another firm for contract award.

A Contractor, subcontractor employee or consultant shall not have access to NRC facilities until he/she is approved by DFS/PSB. Temporary access may be approved based on a favorable NRC review and discretionary determination of their building access security forms. Final building access will be approved based on favorably adjudicated checks by the Government. However, temporary access approval will be revoked and the Contractor's employee may subsequently be denied access in the event the employee's investigation cannot be favorably determined by the NRC. Such employee will not be authorized to work under any NRC contract requiring building access without the approval of DFS/PSB. When an individual receives final access, the individual will be subject to a review or reinvestigation every five (5) or ten (10) years, depending on their job responsibilities at the NRC.

The Government shall have and exercise full and complete control and discretion over granting, denying, withholding, or terminating building access approvals for individuals performing work under this contract. Individuals performing work under this contract at NRC facilities for a period of more than 30 calendar days shall be required to complete and submit to the Contractor representative an acceptable OPM Standard Form 85 (Questionnaire for Non-Sensitive Positions), and two (2) FD 258 (Fingerprint Charts). Non-U.S. citizens must provide official documentation to the DFS/PSB, as proof of their legal residency. This documentation can be a Permanent Resident Card, Temporary Work Visa, Employment Authorization Card, or other official documentation issued by the U.S. Citizenship and Immigration Services. Any applicant with less than five (5) years residency in the U.S. will not be approved for building access. The Contractor shall submit the documents to the NRC Contracting Officer's Representative (COR) who will give them to DFS/PSB.

DFS/PSB may, among other things, grant or deny temporary unescorted building access approval to an individual based upon its review of the information contained in the OPM Standard Form 85 and the Contractor's pre-screening record. Also, in the exercise of its authority, the Government may, among other things, grant or deny permanent building access approval based on the results of its review or investigation. This submittal requirement also applies to the officers of the firm who, for any reason, may visit the NRC work sites for an extended period of time during the term of the contract. In the event that DFS/ PSB are unable to grant a temporary or permanent building access approval, to any individual performing work under this contract, the Contractor is responsible for assigning another individual to perform the necessary function without any delay in the contract's performance schedule, or without adverse impact to any other terms or conditions of the contract. The Contractor is responsible for informing those affected by this procedure of the required building access approval process (i.e., temporary and permanent determinations), and the possibility that individuals may be required to wait until permanent building access approvals are granted before beginning work in NRC's buildings.

CANCELLATION OR TERMINATION OF BUILDING ACCESS/ REQUEST

The Contractor shall immediately notify the PO when a Contractor or subcontractor employee or consultant's need for NRC building access approval is withdrawn or the need by the Contractor employee's for building access terminates. The PO will immediately notify DFS/PSB (via e-mail) when a Contractor employee no longer requires building access. The Contractor shall be required to return any NRC issued badges to the Contracting Officer's Representative (COR) for return to DFS/FSB (Facilities Security Branch) within three (3) days after their termination.

A.14 SECURITY REQUIREMENTS FOR INFORMATION TECHNOLOGY LEVEL I OR LEVEL II ACCESS APPROVAL (AUG 2011)

The contractor must identify all individuals selected to work under this contract. The NRC Contracting Officer's Representative (COR) shall make the final determination of the level, if any, of IT access approval required for all individuals working under this contract/order using the following guidance. The Government shall have full and complete control and discretion over granting, denying, withholding, or terminating IT access approvals for contractor personnel performing work under this contract/order.

The contractor shall conduct a preliminary security interview or review for each employee requiring IT level I or II access and submit to the Government only the names of candidates that have a reasonable probability of obtaining the level of IT access approval for which the employee has been proposed. The contractor shall pre-screen its applicants for the following:

(a) felony arrest in the last seven (7) years; (b) alcohol related arrest within the last five (5) years; (c) record of any military courts-martial convictions in the past ten (10) years; (d) illegal use of narcotics or other controlled substances possession in the past year, or illegal purchase, production, transfer, or distribution of narcotics or other controlled substances in the last seven (7) years; and (e) delinquency on any federal debts or bankruptcy in the last seven (7) years.

The contractor shall make a written record of its pre-screening interview or review (including any information to mitigate the responses to items listed in (a) - (e)), and have the employee verify the pre-screening record or review, sign and date it. The contractor shall supply two (2) copies of the signed contractor's pre-screening record or review to the NRC Contracting Officer's Representative (COR), who will then provide them to the NRC Office of Administration, Division of Facilities and Security, Personnel Security Branch with the employee's completed IT access application package.

The contractor shall further ensure that its personnel complete all IT access approval security applications required by this clause within fourteen (14) calendar days of notification by the NRC Contracting Officer's Representative (COR) of initiation of the application process. Timely receipt of properly completed records of the pre-screening record and IT access approval applications (submitted for candidates that have a reasonable probability of obtaining the level of security assurance necessary for access to NRC's IT systems/data) is a requirement of this contract/order. Failure of the contractor to comply with this requirement may be a basis to terminate the contract/order for cause, or offset from the contract's invoiced cost or price the NRC's incurred costs or delays as a result of inadequate pre-screening by the contractor.

SECURITY REQUIREMENTS FOR IT LEVEL I

Performance under this contract/order will involve contractor personnel who perform services requiring direct access to or operate agency sensitive information technology systems or data (IT Level I). The IT Level I involves responsibility for the planning, direction, and implementation of a computer security program; major responsibility for the direction, planning, and design of a computer system, including hardware and software; or the capability to access a computer system during its operation or maintenance in such a way that could cause or that has a relatively high risk of causing grave damage; or the capability to realize a significant personal gain from computer access.

Contractor personnel shall not have access to sensitive information technology systems or data until they are approved by DFS/PSB and they have been so informed in writing by the NRC Contracting Officer's Representative (COR). Temporary IT access may be approved by DFS/PSB based on a favorable review or adjudication of their security forms and checks. Final IT access may be approved by DFS/PSB based on a favorably review or adjudication of a completed background investigation. However, temporary access authorization approval will be revoked and the employee may subsequently be denied IT access in the event the employee's investigation cannot be favorably adjudicated. Such an employee will not be authorized to work under any NRC contract/order requiring IT access without the approval of DFS/PSB, as communicated in writing to the contractor by the NRC Contracting Officer's Representative (COR). Where temporary access authorization has been revoked or denied by DFS/PSB, the contractor shall assign another contractor employee to perform the necessary work under this contract/ order without delay to the contract/order performance schedule, or without adverse impact to any other terms or conditions of the

contract/order. When an individual receives final IT access approval from DFS/PSB, the individual will be subject to a reinvestigation every ten (10) years thereafter (assuming continuous performance under contract/order at NRC) or more frequently in the event of noncontinuous performance under contract/order at NRC.

The contractor shall submit a completed security forms packet, including the OPM Standard Form (SF) 86 (Questionnaire for National Security Positions), two (2) copies of the Contractor's signed pre-screening record and two (2) FD 258 fingerprint charts, to the NRC PO who will then provide them to DFS/PSB for review and adjudication, prior to the individual being authorized to perform work under this contract/order requiring access to sensitive information technology systems or data. Non-U.S. citizens must provide official documentation to the DFS/PSB, as proof of their legal residency. This documentation can be a Permanent Resident Card, Temporary Work Visa, Employment Authorization Card, or other official documentation issued by the U.S. Citizenship and Immigration Services. Any applicant with less than seven (7) years residency in the U.S. will not be approved for IT Level I access. The Contractor shall submit the documents to the NRC Contracting Officer's Representative (COR) who will give them to DFS/PSB. The contractor shall ensure that all forms are accurate, complete, and legible. Based on DFS/PSB review of the contractor employee's security forms and/or the receipt of adverse information by NRC, the contractor individual may be denied access to NRC facilities and sensitive information technology systems or data until a final determination is made by DFS/PSB and thereafter communicated to the contractor by the NRC Contracting Officer's Representative (COR) regarding the contractor person's eligibility.

In accordance with NRCAR 2052.204-70 "Security," IT Level I contractors shall be subject to the attached NRC Form 187 and SF-86 which furnishes the basis for providing security requirements to contractors that have or may have an NRC contractual relationship which requires access to or operation of agency sensitive information technology systems or remote development and/or analysis of sensitive information technology systems or data or other access to such systems and data; access on a continuing basis (in excess more than 30 calendar days) to NRC buildings; or otherwise requires issuance of an unescorted NRC badge.

SECURITY REQUIREMENTS FOR IT LEVEL II

Performance under this contract/order will involve contractor personnel that develop and/or analyze sensitive information technology systems or data or otherwise have access to such systems or data (IT Level II).

The IT Level II involves responsibility for the planning, design, operation, or maintenance of a computer system and all other computer or IT positions.

Contractor personnel shall not have access to sensitive information technology systems or data until they are approved by DFS/PSB and they have been so informed in writing by the NRC Contracting Officer's Representative (COR). Temporary access may be approved by DFS/PSB based on a favorable review of their security forms and checks. Final IT access may be approved by DFS/PSB based on a favorably adjudication. However, temporary access authorization approval will be revoked and the contractor employee may subsequently be denied IT access in the event the employee's investigation cannot be favorably adjudicated. Such an employee will not be authorized to work under any NRC contract/order requiring IT access without the approval of DFS/PSB, as communicated in writing to the contractor by the NRC Contracting Officer's Representative (COR). Where temporary access authorization has been revoked or denied by DFS/PSB, the contractor is responsible for assigning another contractor employee to perform the necessary work under this contract/order without delay to the contract/order performance schedule, or without adverse impact to any other terms or conditions of the contract/order. When a contractor employee receives final IT access approval from DFS/PSB, the individual will be subject to a review or reinvestigation every ten (10) years (assuming continuous performance under contract/order at NRC) or more frequently in the event of noncontinuous performance under contract/order at NRC.

The contractor shall submit a completed security forms packet, including the OPM Standard Form (SF) 86 (Questionnaire for National Security Positions), two (2) copies of the Contractor's signed pre-screening record and two (2) FD 258 fingerprint charts, through the NRC Contracting Officer's Representative (COR) to DFS/PSB for review and adjudication, prior to the contractor employee being authorized to perform work under this contract/order. Non-U.S. citizens must provide official documentation to the DFS/PSB, as proof of their legal residency. This documentation

can be a Permanent Resident Card, Temporary Work Visa, Employment Authorization Card, or other official documentation issued by the U.S. Citizenship and Immigration Services. Any applicant with less than seven (7) years residency in the U.S. will not be approved for IT Level II access. The Contractor shall submit the documents to the NRC Contracting Officer's Representative (COR) who will give them to DFS/PSB. The contractor shall ensure that all forms are accurate, complete, and legible. Based on DFS/ PSB review of the contractor employee's security forms and/or the receipt of adverse information by NRC, the contractor employee may be denied access to NRC facilities, sensitive information technology systems or data until a final determination is made by DFS/PSB regarding the contractor person's eligibility.

In accordance with NRCAR 2052.204-70 "Security," IT Level II contractors shall be subject to the attached NRC Form 187, SF-86, and contractor's record of the pre-screening which furnishes the basis for providing security requirements to contractors that have or may have an NRC contractual relationship which requires access to or operation of agency sensitive information technology systems or remote development and/or analysis of sensitive information technology systems or data or other access to such systems or data; access on a continuing basis (in excess of more than 30 calendar days) to NRC buildings; or otherwise requires issuance of an unescorted NRC badge.

CANCELLATION OR TERMINATION OF IT ACCESS/REQUEST

When a request for IT access is to be withdrawn or canceled, the contractor shall immediately notify the NRC Contracting Officer's Representative (COR) by telephone so that the access review may be promptly discontinued. The notification shall contain the full name of the contractor employee and the date of the request. Telephone notifications must be promptly confirmed by the contractor in writing to the NRC Contracting Officer's Representative (COR), who will forward the confirmation to DFS/PSB. Additionally, the contractor shall immediately notify the NRC Contracting Officer's Representative (COR) in writing, who will in turn notify DFS/PSB, when a contractor employee no longer requires access to NRC sensitive automated information technology systems or data, including the voluntary or involuntary separation of employment of a contractor employee who has been approved for or is being processed for IT access.

The contractor shall flow the requirements of this clause down into all subcontracts and agreements with consultants for work that requires them to access NRC IT resources.

A.15 SECURITY REQUIREMENTS FOR ACCESS TO CLASSIFIED MATTER OR INFORMATION (AUG 2011)

Performance under this contract will require access to classified matter or information (National Security Information or Restricted Data) in accordance with the attached NRC Form 187 (See List of Attachments). Prime Contractor personnel, subcontractors or others performing work under this contract shall require a "Q" security clearance (allows access to Top Secret, Secret, and Confidential National Security Information and Restricted Data) or an "L" security clearance (allows access to Secret and Confidential National Security Information and/or Confidential Restricted Data).

The Contractor must identify all individuals to work under this contract. The NRC sponsoring office shall make the final determination of the type of security clearance required for all individuals working under this contract.

The Contractor shall conduct a preliminary security interview or review for each of its employees, subcontractor employees and consultants, and submit to the Government only the names of candidates that have a reasonable probability of obtaining the level of security clearance for which the candidate has been proposed. The Contractor will pre-screen applicants for the following:

(a) pending criminal charges or proceedings; (b) felony arrest records including alcohol related arrest within the last seven (7) years; (c) record of any military courts-martial charges and proceedings in the last seven (7) years and

courts-martial convictions in the last ten (10) years; (d)any involvement in hate crimes; (e) involvement in any group or organization that espouses extra-legal violence as a legitimate means to an end; (f) dual or multiple citizenship including the issuance of a foreign passport in the last seven (7) years; (g) illegal use possession, or distribution of narcotics or other controlled substances within the last seven (7) years; (h) financial issues regarding delinquent debts, liens, garnishments, bankruptcy and civil court actions in the last seven (7) years.

The Contractor will make a written record of their pre-screening interview or review (including any information to mitigate the responses to items listed in (a) - (h)), and have the candidate verify the record, sign and date it. Two (2) copies of the signed interview record or review will be supplied to DFS/PSB with the applicant's completed security application package.

The Contractor will further ensure that all Contractor employees, subcontractor employees and consultants for classified information access approval complete all security applications required by this clause within fourteen (14) calendar days of notification by DFS/PSB of initiation of the application process. Timely receipt of properly completed security applications (submitted for candidates that have a reasonable probability of obtaining the level of security clearance for which the candidate has been proposed) is a contract requirement. Failure of the Contractor to comply with this condition may be a basis to cancel the award, or terminate the contract for default, or offset from the contract's invoiced cost or price the NRC's incurred costs or delays as a result of inadequate pre-screening by the Contractor. In the event of termination or cancellation, the Government may select another firm for contract award.

Such Contractor personnel shall be subject to the NRC Contractor personnel security requirements of NRC Management Directive (MD) 12.3, Part I and 10 CFR Part 10.11, which is hereby incorporated by reference and made a part of this contract as though fully set forth herein, and will require a favorably adjudicated Single Scope Background Investigation (SSBI) for "Q" clearances or a favorably adjudicated Access National Agency Check and Inquiries (ANACI), or higher level investigation depending on the position the individual will occupy, for "L" clearances.

A Contractor employee shall not have access to classified information until he/she is granted a security clearance by DFS/PSB, based on a favorably adjudicated investigation. In the event the Contractor employee's investigation cannot be favorably adjudicated, any interim access approval could possibly be revoked and the individual could be subsequently removed from performing under the contract. If interim approval access is revoked or denied, the Contractor is responsible for assigning another individual to perform the necessary work under this contract without delay to the contract's performance schedule, or without adverse impact to any other terms or conditions of the contract. The individual will be subject to a reinvestigation every five (5) years for "Q" clearances and every ten (10) years for "L" clearances.

The Contractor shall submit a completed security forms packet, including the SF-86, "Questionnaire for National Security Positions," and fingerprint charts, through the PO to DFS/PSB for review and submission to the Office of Personnel Management for investigation. The individual may start working under this contract before a final clearance is granted if a temporary access determination can be made by DFS/PSB after the review of the security package. If the individual is granted a temporary access authorization, the individual may not have access to classified information under this contract until DFS/PSB has granted them the appropriate security clearance, and the Contractor has read, understood, and signed the SF 312, "Classified Information Nondisclosure Agreement." The Contractor shall assure that all forms are accurate, complete, and legible (except for Part 2 of the questionnaire, which is required to be completed in private and submitted by the individual to the Contractor in a sealed envelope), as set forth in NRC MD 12.3. Based on DFS/PSB review of the applicant's investigation, the individual may be denied his/her security clearance in accordance with the due process procedures set forth in MD 12.3, E.O. 12968, and 10 CFR Part 10.11.

In accordance with NRCAR 2052.204-70 cleared Contractors shall be subject to the attached NRC Form 187 (See Section J for List of Attachments), MD 12.3, SF- 86 and Contractor's signed record or review of the pre-screening which furnishes the basis for providing security requirements to prime Contractors, subcontractors or others who have or may have an NRC contractual relationship which requires access to classified information.

CANCELLATION OR TERMINATION OF SECURITY CLEARANCE ACCESS/REQUEST

When a request for clearance investigation is to be withdrawn or canceled, the Contractor shall immediately notify the PO by telephone so that the investigation may be promptly discontinued. The notification shall contain the full name of the individual, and the date of the request. Telephone notifications must be promptly confirmed in writing by the Contractor to the PO who will forward the confirmation via email to DFS/PSB. Additionally, DFS/PSB must be immediately notified in writing when an individual no longer requires access to Government classified information, including the voluntary or involuntary separation of employment of an individual who has been approved for or is being processed for access under the NRC "Personnel Security Program."

A.16 DRUG FREE WORKPLACE TESTING: UNESCORTED ACCESS TO NUCLEAR FACILITIES, ACCESS TO CLASSIFIED INFORMATION OR SAFEGUARDS INFORMATION, OR PERFORMING IN SPECIALLY SENSITIVE POSITIONS (AUG 2011)

All contractor employees, subcontractor employees, and consultants proposed for performance or performing under this contract shall be subject to pre- assignment, random, reasonable suspicion, and post-accident drug testing applicable to: (1) individuals who require unescorted access to nuclear power plants, (2) individuals who have access to classified or safeguards information, (3) individuals who are required to carry firearms in performing security services for the NRC, (4) individuals who are required to operate government vehicles or transport passengers for the NRC, (5) individuals who are required to operate hazardous equipment at NRC facilities, or (6) individuals who admit to recent illegal drug use or those who are found through other means to be using drugs illegally. The Plan includes a contractor's employees and their subcontractors are subject to the procedures and terms of their employment agreements with their employer.

The NRC Drug Program Manager will schedule the drug testing for all contractor employees, subcontractor employees, and consultants who are subject to testing under this clause. Any NRC contractor found to be using, selling, or possessing illegal drugs, or any contractor with a verified positive drug test result under this program while in a duty status will immediately be removed from working under the NRC contract. The contractor's employer will be notified of the denial or revocation of the individual's authorization to have access to information and ability to perform under the contract. The individual may not work on any NRC contract for a period of not less than one year from the date of the failed drug test and will not be considered for reinstatement unless evidence of rehabilitation, as determined by the NRC "drug testing contractor's" Medical Review Officer, is provided.

Contractor drug testing records are protected under the NRC Privacy Act Systems of Records, System 35, "Drug Testing Program Records - NRC" found at: http://www.nrc.gov/reading-rm/foia/privacy-systems.html

A.17 PACKAGING AND MARKING (AUG 2011)

(a) The Contractor shall package material for shipment to the NRC in such a manner that will ensure acceptance by common carrier and safe delivery at destination. Containers and closures shall comply with the Surface Transportation Board, Uniform Freight Classification Rules, or regulations of other carriers as applicable to the mode of transportation.

(b) On the front of the package, the Contractor shall clearly identify the contract number under which the product is being provided.

(c) Additional packaging and/or marking requirements are as follows:

A.18 BRANDING (AUG 2011)

The Contractor is required to use the official NRC branding logo or seal on any publications, presentations, products, or materials funded under this contract, to the extent practical, in order to provide NRC recognition for its involvement

in and contribution to the project. If the work performed is funded entirely with NRC funds, then the contractor must acknowledge that information in its documentation/presentation.

Access the following websites for branding information and specifications:
http://www.internal.nrc.gov/ADM/branding/ and Management Directive and Handbook 3.13 -

(internal NRC website): http://www.internal.nrc.gov/policy/directives/toc/md3.13.htm

(external public website): http://pbadupws.nrc.gov/docs/ML1122/ML112280190.pdf

A.19 DENIAL OF FEDERAL BENEFITS TO INDIVIDUALS CONVICTED OF DRUG TRAFFICKING OR POSSESSION (AUG 2011)

In the event that an award is made to an individual, Section 5301 of the Anti-Drug Abuse Act of 1988 (P.L. 100-690), codified at 21 U.S.C. 862, authorizes denial of Federal benefits such as grants, contracts, purchase orders, financial aid, and business and professional licenses to individuals convicted of drug trafficking or possession.

A.20 ELECTRONIC PAYMENT (AUG 2011)

The Debt Collection Improvement Act of 1996 requires that all payments except IRS tax refunds be made by Electronic Funds Transfer. Payment shall be made in accordance with FAR 52.232-33, entitled "Payment by Electronic Funds- Central Contractor Registration".

To receive payment, the contractor shall prepare invoices in accordance with NRC's Billing Instructions. Claims shall be submitted on the payee's letterhead, invoice, or on the Government's Standard Form 1034, "Public Voucher for Purchases and Services Other than Personal," and Standard Form 1035, "Public Voucher for Purchases Other than Personal - Continuation Sheet." The preferred method of submitting invoices is electronically to the Department of the Interior at NRCPayments_NBCDenver@nbc.gov. If the contractor submits a hard copy of the invoice, it shall be submitted to the following address:

Department of the Interior
National Business Center
Attn: Fiscal Services Branch - D2770
7301 West Mansfield Avenue
Denver, CO 80235-2230

A.21 RECORDS MANAGEMENT (AUG 2011)

1. Definitions. As used in this clause-

"Alienation" means the unauthorized removal of Federal records from the care and control of the Government.

"Disposition" means actions taken regarding Federal records after they are no longer needed to conduct current Agency business; in other words, either the destruction or transfer of the records by the Contractor under the written direction of the Contracting Officer.

"Records" means books, papers, maps, photographs, machine readable materials, emails, web/portal documents, backup data used to create deliverables, or other documentary or electronic materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal Law in connection with a government contract and preserved or appropriate for preservation by that agency as evidence of the

organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of their informational value.

"Records management" means the planning, controlling, directing, organizing, training, and other managerial activities involved with respect to records creation, records maintenance and use, and records disposition in order to achieve adequate and proper documentation of all activities performed under the contract.

"Records management system" means a manual or automated system in which records are collected, organized, and categorized to facilitate preservation, retrieval, use, and disposition.

2. All records and data created or received while performing work on behalf of NRC are Federal records subject to the provisions of 44 U.S.C. Chapters 21, 29, 31, and 33, C.F.R. Parts 1222 and 1224, and must be managed and disposed of accordingly. Ownership of the records resides with the NRC, which will provide instructions regarding creation, management, and access to the records. These records are also subject to the requirements set forth in the Freedom of Information Act (5 U.S.C. 552) and Privacy Act (5 U.S.C. 552a). Records not covered by this clause are:

a. Employment-related records except for those records subject to the requirements of the Privacy Act (5 U.S.C. 552a);

b. Confidential contractor financial information; and

c. Legal records covered by the attorney-client and attorney work product privileges

3. Throughout the period of performance of the contract, the Contractor shall implement a records management system that collects, organizes, and categorizes Federal records to facilitate their preservation, retrieval, use and disposition.

4. Records created under this contract should be complete and accurate to the extent required to document the essential transactions and activities undertaken in the performance of the contract.

5. Upon request, the Contractor shall, as directed by the Contracting Officer, make records available to authorized individuals for inspection, copying, and audit.

6. Protection and Disposal of Records-

a. Records should be protected in accordance with applicable Federal laws, as appropriate. Inactive hardcopy records should be stored in designated storage area units in accordance with the standards specified in 36 CFR Part 1234;

b. Records are not to be alienated or destroyed except in accordance with all applicable Federal laws and regulations and will be subject to the penalties provided by law for the unlawful removal or destruction of records;

c. The Contractor shall preserve records generated in performance of work under a contract until disposal is authorized in writing by the NRC Contracting Officer, or they are delivered to NRC upon completion or termination of the contract.

d. The Contractor shall document the destruction of temporary records and any transfer of records to the NRC.

A.22 COMPLIANCE WITH U.S. IMMIGRATION LAWS AND REGULATIONS (AUG 2011)

NRC contractors are responsible to ensure that their alien personnel are not in violation of United States immigration laws and regulations, including employment authorization documents and visa requirements. Each alien employee of the Contractor must be lawfully admitted for permanent residence as evidenced by Permanent Resident Form I-551 (Green Card), or must present other evidence from the U.S. Department of Homeland Security/U.S. Citizenship and Immigration Services that employment will not affect his/her immigration status. The U.S. Citizenship and Immigration Services provides information to contractors to help them understand the employment eligibility verification process for non-US citizens. This information can be found on their website, http://www.uscis.gov/ portal/site/uscis.

The NRC reserves the right to deny or withdraw Contractor use or access to NRC facilities or its equipment/services, and/or take any number of contract administrative actions (e.g., disallow costs, terminate for cause) should the Contractor violate the Contractor's responsibility under this clause.

A.23 FOREIGN OWNERSHIP, CONTROL, OR INFLUENCE OVER CONTRACTOR (AUG 2011)

The National Industrial Security Program Operating Manual (NISPOM) implements the provisions of E.O. 12829, "National Industrial Security Program." A company is considered to be under FOCI whenever a foreign interest has the power, direct or indirect, whether or not exercised, and whether or not exercisable through the ownership of the U.S. company's securities, by contractual arrangements or otherwise, to direct or decide matters affecting the management or operations of that company in a manner that may result in unauthorized access to classified information or may adversely affect the performance of classified information contracts. (See NRC Management Directive 12.2 - "NRC Classified Information Security Program")

(a) For purposes of this clause, a foreign interest is defined as any of the following:

(1) A foreign government or foreign government agency;

(2) Any form of business enterprise organized under the laws of any country other than the United States or its possessions;

(3) Any form of business enterprise organized or incorporated under the laws of the U.S., or a State or other jurisdiction within the U.S., which is owned, controlled, or influenced by a foreign government, agency, firm, corporation or person; or

(4) Any person who is not a U.S. citizen.

(b) A U.S. company determined to be under FOCI is not eligible for facility clearance (FCL). If a company already has an FCL, the FCL shall be suspended or revoked unless security measures are taken to remove the possibility of unauthorized access to classified information.

(c) For purposes of this clause, subcontractor means any subcontractor at any tier and the term "contracting officer" shall mean NRC contracting officer. When this clause is included in a subcontract, the term "contractor" shall mean subcontractor and the term "contract" shall mean subcontract.

(d) The contractor shall complete and submit and SF-328, DD-441 and DD-441-1 forms, prior to contract award. The information contained in these forms may be used in making a determination as to whether a contractor is eligible to participate in the National Industrial Security Program and have a facility security clearance.

(e) The contractor shall immediately provide the contracting officer written notice of any changes in the extent and nature of FOCI over the contractor which would affect the answers to the questions presented in SF-328, "Certificate Pertaining to Foreign Interest". Further, notice of changes in ownership or control which are required to be reported to the Securities and Exchange Commission, the Federal Trade Commission, or the Department of Justice shall also be furnished concurrently to the contracting officer.

(f) In those cases where a contractor has changes involving FOCI, the NRC must determine whether the changes will pose an undue risk to the common defense and security. In making this determination, the contracting officer shall consider proposals made by the contractor to avoid or mitigate foreign influences.

(g) The contractor agrees to insert terms that conform substantially to the language of this clause including this paragraph (g) in all subcontracts under this contract that will require access to classified information and shall require such subcontractors to submit completed SF-328, DD-441 and DD-441-1 forms prior to award of a subcontract. Information to be provided by a subcontractor pursuant to this clause may be submitted directly to the contracting officer.

(h) Information submitted by the contractor or any affected subcontractor as required pursuant to this clause shall be treated by NRC to the extent permitted by law, as business or financial information submitted in confidence to be used solely for purposes of evaluating FOCI.

(i) The requirements of this clause are in addition to the requirement that a contractor obtain and retain the security clearances required by the contract. This clause shall not operate as a limitation on NRC's rights, including its rights to terminate this contract.

(j) The contracting officer may terminate this contract for default either if the contractor fails to meet obligations imposed by this clause, e.g., provide the information required by this clause, comply with the contracting officer's instructions about safeguarding classified information, or make this clause applicable to subcontractors, or if, in the contracting officer's judgment, the contractor creates a FOCI situation in order to avoid performance or a termination for default. The contracting officer may terminate this contract for convenience if the contractor becomes subject to FOCI and for reasons other than avoidance of performance of the contract, cannot, or chooses not to, avoid or mitigate the FOCI problem.

A.24 SECURITY REQUIREMENTS RELATING TO THE PRODUCTION OF REPORT(S) OR THE PUBLICATION OF RESULTS UNDER CONTRACTS, AGREEMENTS, AND GRANTS (AUG 2011)

Review and Approval of Reports

(a) Reporting Requirements. The contractor/grantee shall comply with the terms and conditions of the contract/grant regarding the contents of the draft and final report, summaries, data, and related documents, to include correcting, deleting, editing, revising, modifying, formatting, and supplementing any of the information contained therein, at no additional cost to the NRC. Performance under the contract/grant will not be deemed accepted or completed until it complies with the NRC's directions. The reports, summaries, data, and related documents will be considered draft until approved by the NRC. The contractor/ grantee agrees that the direction, determinations, and decisions on approval or disapproval of reports, summaries, data, and related documents created under this contract/grant remain solely within the discretion of the NRC.

(b) Publication of Results. Prior to any dissemination, display, publication, or release of articles, reports, summaries, data, or related documents developed under the contract/grant, the contractor/grantee shall submit them to the NRC for review and approval. The contractor/ grantee shall not release, disseminate, display or publish articles, reports, summaries, data, and related documents, or the contents therein, that have not been reviewed and approved by the NRC for release, display, dissemination or publication. The contractor/grantee agrees to conspicuously place any disclaimers, markings or notices, directed by the NRC, on any articles, reports, summaries, data, and related documents that the contractor/grantee intends to release, display, disseminate or publish to other persons, the public, or any other entities. The contractor/grantee agrees, and grants, a royalty-free, nonexclusive, irrevocable worldwide license to the government, to use, reproduce, modify, distribute, prepare derivative works, release, display or disclose the articles, reports, summaries, data, and related documents developed under the contract/grant, for any governmental purpose and to have or authorize others to do so.

(c) Identification/Marking of Sensitive Unclassified Non-Safeguards Information (SUNSI) and Safeguards Information (SGI). The decision, determination, or direction by the NRC that information possessed, formulated or produced by the contractor/grantee constitutes SUNSI or SGI is solely within the authority and discretion of the NRC. In performing the contract/grant, the contractor/grantee shall clearly mark SUNSI and SGI, to include for example, OUO-Allegation Information or OUO-Security Related Information on any reports, documents, designs, data, materials, and written information, as directed by the NRC. In addition to marking the information as directed by the NRC, the contractor shall use the applicable NRC cover sheet (e.g., NRC Form 461 Safeguards Information) in maintaining these records and documents. The contractor/grantee shall ensure that SUNSI and SGI is handled, maintained and protected from unauthorized disclosure, consistent with NRC policies and directions. The contractor/grantee shall comply with the requirements to mark, maintain, and protect all information, including documents, summaries, reports, data, designs, and materials in accordance with the provisions of Section 147 of the Atomic Energy Act of 1954 as amended, its implementing regulations (10 CFR 73.21), Sensitive Unclassified Non-Safeguards and Safeguards Information policies, and NRC Management Directives and Handbooks 12.5, 12.6 and 12.7.

(d) Remedies. In addition to any civil, criminal, and contractual remedies available under the applicable laws and regulations, failure to comply with the above provisions, and/or NRC directions, may result in suspension, withholding, or offsetting of any payments invoiced or claimed by the contractor/grantee.

(e) Flowdown. If the contractor/grantee intends to enter into any subcontracts or other agreements to perform this contract/grant, the contractor/grantee shall include all of the above provisions in any subcontracts or agreements.

A.25 WHISTLEBLOWER PROTECTION FOR NRC CONTRACTOR AND SUBCONTRACTOR EMPLOYEES (AUG 2011)

(a) The U.S. Nuclear Regulatory Commission (NRC) contractor and its subcontractor are subject to the Whistleblower Employee Protection public law provisions as codified at 42 U.S.C. 5851. NRC contractor(s) and subcontractor(s) shall comply with the requirements of this Whistleblower Employee Protection law, and the implementing regulations of the NRC and the Department of Labor (DOL). See, for example, DOL Procedures on Handling Complaints at 29 C.F.R. Part 24 concerning the employer obligations, prohibited acts, DOL procedures and the requirement for prominent posting of notice of Employee Rights at Appendix A to Part 24 entitled: "Your Rights Under the Energy Reorganization Act".

(b) Under this Whistleblower Employee Protection law, as implemented by regulations, NRC contractor and subcontractor employees are protected from discharge, reprisal, threats, intimidation, coercion, blacklisting or other employment discrimination practices with respect to compensation, terms, conditions or privileges of their employment because the contractor or subcontractor employee(s) has provided notice to the employer, refused to engage in unlawful practices, assisted in proceedings or testified on activities concerning alleged violations of the Atomic Energy Act of 1954 (as amended) and the Energy Reorganization Act of 1974 (as amended).

(c) The contractor shall insert this or the substance of this clause in any subcontracts involving work performed under this contract.

A.26 CONTRACTOR RESPONSIBILITY FOR PROTECTING PERSONALLY IDENTIFIABLE INFORMATION (PII) (AUG 2011)

In accordance with the Office of Management and Budget's guidance to Federal agencies and the Nuclear Regulatory Commission's (NRC) implementing policy and procedures, a contractor (including subcontractors and contractor employees), who performs work on behalf of the NRC, is responsible for protecting, from unauthorized

access or disclosure, personally identifiable information (PII) that may be provided, developed, maintained, collected, used, or disseminated, whether in paper, electronic, or other format, during performance of this contract.

A contractor who has access to NRC owned or controlled PII, whether provided to the contractor by the NRC or developed, maintained, collected, used, or disseminated by the contractor during the course of contract performance, must comply with the following requirements:

(1) General. In addition to implementing the specific requirements set forth in this clause, the contractor must adhere to all other applicable NRC guidance, policy and requirements for the handling and protection of NRC owned or controlled PII. The contractor is responsible for making sure that it has an adequate understanding of such guidance, policy and requirements.

(2) Use, Ownership, and Nondisclosure. A contractor may use NRC owned or controlled PII solely for purposes of this contract, and may not collect or use such PII for any purpose outside the contract without the prior written approval of the NRC Contracting Officer. The contractor must restrict access to such information to only those contractor employees who need the information to perform work under this contract, and must ensure that each such contractor employee (including subcontractors' employees) signs a nondisclosure agreement, in a form suitable to the NRC Contracting Officer, prior to being granted access to the information. The NRC retains sole ownership and rights to its PII. Unless the contract states otherwise, upon completion of the contract, the contractor must turn over all PII in its possession to the NRC, and must certify in writing that it has not retained any NRC owned or controlled PII except as otherwise authorized in writing by the NRC Contracting Officer.

(3) Security Plan. When applicable, and unless waived in writing by the NRC Contracting Officer, the contractor must work with the NRC to develop and implement a security plan setting forth adequate procedures for the protection of NRC owned or controlled PII as well as the procedures which the contractor must follow for notifying the NRC in the event of any security breach. The plan will be incorporated into the contract and must be implemented and followed by the contractor once it has been approved by the NRC Contracting Officer. If the contract does not include a security plan at the time of contract award, a plan must be submitted for the approval of the NRC Contracting Officer within 30 days after contract award.

(4) Breach Notification. The contractor must immediately notify the NRC Contracting Officer and the NRC Contracting Officer's Representative (COR) upon discovery of any suspected or confirmed breach in the security of NRC owned or controlled PII.

(5) Legal Demands for Information. If a legal demand is made for NRC owned or controlled PII (such as by subpoena), the contractor must immediately notify the NRC Contracting Officer and the NRC Contracting Officer's Representative (COR). After notification, the NRC will determine whether and to what extent to comply with the legal demand. The Contracting Officer will then notify the contractor in writing of the determination and such notice will indicate the extent of disclosure authorized, if any. The contractor may only release the information specifically demanded with the written permission of the NRC Contracting Officer.

(6) Audits. The NRC may audit the contractor's compliance with the requirements of this clause, including through the use of online compliance software.

(7) Flow-down. The prime contractor will flow this clause down to subcontractors that would be covered by any portion of this clause, as if they were the prime contractor.

(8) Remedies:

(a) The contractor is responsible for implementing and maintaining adequate security controls to prevent the loss of control or unauthorized disclosure of NRC owned or controlled PII in its possession. Furthermore, the contractor is responsible for reporting any known or suspected loss of control or unauthorized access to PII to the NRC in accordance with the provisions set forth in Article 4 above.

(b) Should the contractor fail to meet its responsibilities under this clause, the NRC reserves the right to take appropriate steps to mitigate the contractor's violation of this clause. This may include, at the sole discretion of the NRC, termination of the subject contract.

(9) Indemnification. Notwithstanding any other remedies available to the NRC, the contractor will indemnify the NRC against all liability (including costs and fees) for any damages arising out of violations of this clause.

A.27 GREEN PURCHASING (JUN 2011)

(a) In furtherance of the sustainable acquisition goals of Executive Order 13514, "Federal Leadership in Environmental, Energy, and Economic Performance" products and services provided under this contract/order shall be energy- efficient (Energy Star or Federal Energy Management Program (FEMP) designated), water-efficient, biobased, environmentally preferable (e.g., Electronic Product Environmental Assessment Tool (EPEAT) certified), non-ozone depleting, contain recycled content, or are non-toxic or less toxic alternatives, where such products and services meet agency performance requirements. http://www.fedcenter.gov/programs/eo13514/

(b) The contractor shall flow down this clause into all subcontracts and other agreements that relate to performance of this contract/order.

A.28 USE OF AUTOMATED CLEARING HOUSE (ACH) ELECTRONIC PAYMENT/REMITTANCE ADDRESS (AUG 2011)

The Debt Collection Improvement Act of 1996 requires that all Federal payments except IRS tax refunds be made by Electronic Funds Transfer. It is the policy of the Nuclear Regulatory Commission to pay government vendors by the Automated Clearing House (ACH) electronic funds transfer payment system. Item 15C of the Standard Form 33 may be disregarded.

ATTACHMENTS

ATTACHMENT NUMBER	TITLE	DATE	NO. PAGES
0001	Statement of Work		4
0002	10 CFR Part 10		15
0003	Adjudicative Guidelines		18
0004	Executive Order 12968		10
0005	Billing Instructions		7
0006	NRC-187		2

ATTACHMENT #1
U.S. NUCLEAR REGULATORY COMMISSION
DIVISION OF FACILITIES AND SECURITY
PERSONNEL SECURITY BRANCH

STATEMENT OF WORK

MENTAL HEALTH EVALUATION SERVICES

1.0 BACKGROUND

The Nuclear Regulatory Commission (NRC), Division of Facilities and Security (DFS), Personnel Security Branch (PSB) recognizes the importance of mental health evaluation services. The mental health evaluations must be conducted in accordance with Federal regulations in Title 10, Code of Federal Regulations, Part 10, "CRITERIA AND PROCEDURES FOR DETERMINING ELIGIBILITY FOR ACCESS TO RESTRICTED DATA OR NATIONAL SECURITY INFORMATION OR AN EMPLOYMENT CLEARANCE", hereafter referred to as "10 CFR Part 10" (Attachment 1); "EXECUTIVE ORDER 12968 (ACCESS TO CLASSIFIED INFORMATION)", hereafter referred to as "E.O. 12968" (Attachment 2); and Adjudicative Guidelines for Determining Eligibility for Access to Classified Information, hereafter referred to as "Guidelines" (Attachment 3). The Personnel Security Branch (PSB), requires, on an as-needed basis, mental health evaluations of employees, consultants, contractors, and licensee personnel to resolve security concerns in accordance with personnel security Adjudicative Guidelines and to include the diagnosis and treatment of mental, emotional, and personality disorders and the subspecialty of drug and alcohol abuse and addictions.

2.0 OBJECTIVES

The contractor shall conduct mental health evaluations, as-needed, of NRC employees, consultants, contractors and licensee personnel in accordance with 10 CFR Part 10, E.O. 12968, and Guidelines. Activities associated with these evaluations include coordinating the evaluation with the Personnel Security Branch Contracting Officer's Representative (PSB/COR), reviewing the individual's Personnel Security File (PSF), conducting the mental health evaluation, consulting with the individual's mental health care provider to verify current treatment, diagnosis, prognosis, medications, etc., and providing the PSB/COR with a written report, that includes the following:

1. Findings and recommendations of the individual's eligibility to maintain a security clearance, ability to properly safeguard classified national security information and the ability to be trustworthy and reliable.

The PSB/COR will request these evaluations to be conducted to determine and resolve security concerns involving drug and alcohol use, financial and criminal history, and emotional, mental and personality disorders, to include the diagnosis and treatment of mental, emotional, and personality disorders and the subspecialty of drug and alcohol abuse and addictions.

3.0 SCOPE OF WORK

The contractor shall conduct evaluations at the NRC facility in Rockville, MD, but there may be times when the contractor will be required to travel to a regional office. When an evaluation is required, the PSB/COR will contact the contractor by telephone or email correspondence to schedule the evaluation and to provide pertinent biographical data. The PSB/COR will subsequently forward to the contractor

for review, prior to the evaluation, a copy of the individual's PSF, which may include the background investigation, case analysis, and interview transcript and analysis, if applicable. The contractor may be asked to coordinate or assist PSB in coordinating appropriate medical releases to permit Agency access to a subject's medical records and/or treating physician(s).

In conducting the mental health evaluation, in addition to a review of the PSF, the contractor may be required to consult with a subject's mental health counselors to verify current treatment; diagnosis and prognosis; evaluate medication usage; verify counseling for drug, alcohol or other dependency/addiction; determine the necessity for an in-person mental health evaluation; determine if additional counseling or treatment would effectively mitigate the security concern(s); and provide expert witness testimony if applicable. While these activities are typical of those that will be required under the contract, this is not an exhaustive list and the contractor may be asked to perform other activities that might reasonably be expected to produce information pertinent to the determination of an individual's trustworthiness and reliability. This professional consultation is advisory in nature and does not obligate or restrict PSB in their independent adjudication of security issues.

After the contractor completes the mental health evaluation, they will provide PSB with a written report of the findings and a recommendation. Additionally, the contractor will provide a determination to reflect the individual's eligibility to maintain a security clearance, the ability to properly safeguard information, to handle classified national security information, and to be trustworthy and reliable with specific emphasis on the criteria set forth in 10 CFR Part 10 and the Guidelines. The contractor may be asked to provide or obtain additional information after PSB has reviewed the written report and may be requested to modify or amend the report after doing so.

The contractor will provide expert witness testimony, and participate in the CFR 10 Part 10 hearings and appeals process on an as-needed basis.

4.0 NRC-FURNISHED MATERIAL

Within 2 working days from the date of request for a mental health evaluation, the PSB/COR will provide the contractor with the individual's PSF for review prior to the scheduled evaluation. The contractor will confirm with the NRC that the furnished NRC documents are properly safeguarded while in their possession. The contractor will coordinate with the PSB/COR the return of NRC-furnished materials after the report is submitted.

5.0 SCHEDULE FOR DELIVERABLES

The contractor shall schedule evaluations to take place within 10 working days from the date of the PSB/COR's request.

The contractor shall provide the PSB/COR all written reports of findings and recommendations with respect to the individual's judgment, reliability, or ability to properly safeguard classified national security information within 10 working days from the date the mental the PSB/COR will determine whether to grant the extension.

The contractor shall provide written results of file reviews to the PSB/COR within 10 working days from the date the information was received. Extensions may be requested from the PSB/COR on a case by case basis.

The contractor shall notify the PSB/COR if an extension is needed to provide the written reports of findings and recommendations or the written results of file reviews. The PSB/COR may grant an extension of an additional 10 working days, if needed, upon request.

The contractor will respond to PSB within 10 working days with their availability to attend a hearing conducted in accordance with the CFR 10 Part 10 hearings and appeals process or to testify as an expert witness on an as-needed basis.

6.0 QUALIFICATIONS TO CONDUCT SECURITY RELATED MENTAL HEALTH EVALUATIONS

The NRC requires a credentialed mental health psychiatrist; i.e. Doctor of Medicine (MD) or Doctor of Osteopathy (DO), with familiarity and/or experience in conducting evaluations for personnel security organizations within the Federal government, to resolve security concerns including but not limited to the following Guidelines: Adjudicative Guideline D: Sexual Behavior; Guideline E: Personal Conduct; Guideline F: Financial Consideration; Guideline G: Alcohol Consumption; Guideline H: Drug Involvement; Guideline I: Psychological Conditions: Guideline J: Criminal Conduct; Guideline K: Handling Protected Information, to include the diagnosis and treatment of mental, emotional, and personality disorders and the subspecialty of drug and alcohol abuse and addictions.

When a mental, emotional or psychological condition, personality disorder, use of drugs or alcohol, or the side effects of medication adversely affects or could adversely affect a person's judgment, behavior, reliability and/or trustworthiness, a mental health evaluation may be required to determine if such conditions could impair an individual's ability to properly safeguard classified national security information. In these situations, the contractor, after evaluating all available information (see 2.0 Scope of Work, above), will make a recommendation to the security adjudicator regarding the issuance, suspension or revocation of a security clearance.

Contractor shall be utilized in evaluating potentially disqualifying and mitigating information fully and properly, and particularly for consultation with the individual's mental health care provider.

Only a qualified MD or DO can perform a comprehensive medical evaluation in order to render a medical opinion regarding a condition that could impair an individual's judgment, reliability or ability to properly safeguard classified national security information and the extent and duration of impairment or treatment. Only a qualified MD or DO can determine if prescribed medications are necessary or adequate for the treatment of mental and emotional conditions, personality disorders, and/or drug and alcohol abuse and addictions; that additional or different medications might be more effective for treatment of a condition; or that medications prescribed for other conditions impair an individual's judgment, reliability or ability to properly safeguard classified national security information.

The contractor shall be eligible to receive and maintain a national security clearance at the Secret level (L) or Top Secret (Q), and be available to conduct mental health evaluations on site at the NRC Headquarters facility in Rockville, MD.

7.0 TRAVEL

The NRC will not be responsible for any local travel costs to and from the NRC Headquarters for performance of these services. The NRC will reimburse travel costs should the contractor have to travel to one of the NRC's regional offices. All travel shall be conducted within the guidelines of the Federal Travel Regulation (FTR).

8.0 PERIOD OF PERFORMANCE

Duration of this contract is one year base period with four (4) option years.

Nuclear Regulatory Commission/ Personnel Security Branch/Contracting Officer Representative:

Primary = Janice E. Kelsh – 301-492-3530

upon whom the demand has been made shall respectfully decline to comply with the demand, citing these regulations and *United States ex rel. Touhy* v. *Ragen*, 340 U.S. 462 (1951).

PART 10—CRITERIA AND PROCEDURES FOR DETERMINING ELIGIBILITY FOR ACCESS TO RESTRICTED DATA OR NATIONAL SECURITY INFORMATION OR AN EMPLOYMENT CLEARANCE

Subpart A—General Provisions

Subpart B—Criteria for Determining Eligibility for Access to Restricted Data or National Security Information or an Employment Clearance

Subpart C—Procedures

Subpart D—Miscellaneous

AUTHORITY: Secs. 145, 161, 68 Stat. 942, 948, as amended (42 U.S.C. 2165, 2201); sec. 201, 88 Stat. 1242, as amended (42 U.S.C. 5841); E.O. 10450, 3 CFR parts 1949–1953 COMP., p. 936, as amended, E.O. 10865, 3 CFR 1959–1963 COMP., p. 398, as amended, 3 CFR Table 4.; E.O. 12968, 3 CFR 1995 COMP., p. 396

SOURCE: 47 FR 38676, Sept. 2, 1982, unless otherwise noted

EDITORIAL NOTE: Nomenclature changes to part 10 appear at 70 FR 30897, May 31, 2005

Subpart A—General Provisions

§ 10.1 Purpose.

(a) This part establishes the criteria, procedures, and methods for resolving questions concerning:

(1) The eligibility of individuals who are employed by or applicants for employment with NRC contractors, agents, and licensees of the NRC, individuals who are NRC employees or applicants for NRC employment, and other persons designated by the Deputy Executive Director for Information Services and Administration and Chief Information Officer of the NRC, for access to Restricted Data pursuant to the Atomic Energy Act of 1954, as amended, and the Energy Reorganization Act of 1974, or for access to national security information; and

(2) The eligibility of NRC employees, or the eligibility of applicants for employment with the NRC, for employment clearance.

(b) This part is published to implement the Atomic Energy Act of 1954, as amended, the Energy Reorganization Act of 1974, as amended, Executive Order 10865, 25 FR 1583 (February 24, 1960) Executive Order 10450, 18 FR 2489 (April 27, 1954), and Executive Order 12968, 60 FR 40245 (August 2, 1995)

[64 FR 15641, Apr. 1, 1999]

§ 10.2 Scope.

The criteria and procedures in this part shall be used in determining eligibility for NRC access authorization and/or employment clearance involving:

(a) Employees (including consultants) of contractors and agents of the Nuclear Regulatory Commission and applicants for employment;

(b) Licensees of the NRC and their employees (including consultants) and applicants for employment.

(c) NRC employees (including consultants) and applicants for employment; and

(d) Any other person designated by the Deputy Executive Director for Information Services and Administration and Chief Information Officer of the Nuclear Regulatory Commission.

[47 FR 38676, Sept. 2, 1982, as amended at 64 FR 1564], Apr. 1, 1999]

§ 10.3 [Reserved]

§ 10.4 Policy.

It is the policy of the Nuclear Regulatory Commission to carry out its responsibility for the security of the nuclear energy program in a manner consistent with traditional American concepts of justice. To this end, the Commission has established criteria for determining eligibility for access authorization and/or employment clearance and will afford those individuals described in § 10.2 the opportunity for administrative review of questions concerning their eligibility for access authorization and/or employment clearance.

§ 10.5 Definitions.

Access authorization means an administrative determination that an individual (including a consultant) who is employed by or an applicant for employment with the NRC, NRC contractors, agents, and licensees of the NRC, or other person designated by the Deputy Executive Director for Information Services and Administration and Chief Information Officer, is eligible for a security clearance for access to Restricted Data or National Security Information.

Commission means the Nuclear Regulatory Commission of five members or a quorum thereof sitting as a body, as provided by section 201 of the Energy Reorganization Act of 1974, or its designee.

Eligible or *Eligibility* means both initial eligibility and continued eligibility of an individual for access authorization and/or employment clearance.

Employment Clearance means an administrative determination that an individual (including a consultant) who is an NRC employee or applicant for NRC employment and other persons designated by the Deputy Executive Director for Information Services and Administration and Chief Information Officer of the NRC is eligible for employment or continued employment pursuant to subsection 145(b) of the Atomic Energy Act of 1954, as amended.

Hearing Counsel means an NRC attorney assigned by the General Counsel to prepare and administer hearings in accordance with this part.

Hearing Examiner means a qualified attorney appointed by the Director, Office of Administration, to conduct a hearing in accordance with this part.

National Security Information means information that has been determined pursuant to Executive Order 12958 or any predecessor order to require protection against unauthorized disclosure and that is so designated.

NRC Personnel Security Review Panel means an appeal panel appointed by the Deputy Executive Director for Information Services and Administration and Chief Information Officer and consisting of three members, two of whom shall be selected from outside the security field. One member of the Panel shall be designated as Chairman.

Personnel Security Review Examiners are persons designated by the Executive Director for Operations to conduct a review of the record in accordance with this part.

Restricted Data means all data concerning design, manufacture, or utilization of atomic weapons, the production of special nuclear material, or the use of special nuclear material in the production of energy, but shall not include data declassified or removed from the Restricted Data category pursuant to section 142 of the Atomic Energy Act of 1954, as amended.

[47 FR 38676, Sept. 2, 1982, as amended at 51 FR 35999, Oct. 8, 1986; 52 FR 31609, Aug. 21, 1987; 54 FR 53316, Dec. 28, 1989; 64 FR 1564], Apr. 1, 1999]

Subpart B—Criteria for Determining Eligibility for Access to Restricted Data or National Security Information or an Employment Clearance

§ 10.10 Application of the criteria.

(a) The decision as to access authorization and/or employment clearance is a comprehensive, common-sense judgment, made after consideration of all the information, favorable or unfavorable, relevant to whether the granting of access authorization and/or employment clearance would not endanger the common defense and security and would be clearly consistent with the national interest.

(b) The criteria in §10.11 set forth a number of the types of derogatory information used to assist in making determinations of eligibility for access authorization and/or employment clearance. These criteria are not exhaustive but contain the principal types of derogatory information which create a question as to the individual's eligibility for access authorization and/or employment clearance. While there must necessarily be adherence to such criteria, the NRC is not limited to them, nor precluded from exercising its judgment that information or facts in a case under its cognizance are derogatory although at variance with, or outside the scope of, the stated categories. These criteria are subject to continuing review and may be revised from time to time as experience and circumstances may make desirable.

(c) When the reports of investigation of an individual contain information reasonably tending to establish the truth of one or more of the items in the criteria, such information shall be regarded as derogatory and shall create a question as to the individual's eligibility for access authorization and/or employment clearance. A question concerning the eligibility of an individual for access authorization and/or employment clearance shall be resolved in accordance with the procedures set forth in § 10.20 *et seq.*

(d) In resolving a question concerning the eligibility or continued eligibility of an individual for access authorization and/or employment clearance, the following principles shall be applied by the Director, Division of Facilities and Security, Hearing Examiners, and the NRC Personnel Security Review Panel:

(1) Information reasonably tending to establish the truth of one or more of the items in the criteria shall be the basis for recommending denial or revocation of access authorization and/or employment clearance unless evidence to support faith in the individual's reliability and trust-worthiness is affirmatively shown.

(2) When deemed material to the deliberations, the extent of the activity, conduct, or condition, the period in which they occurred or existed, the length of time which has since elapsed, and the attitude and convictions of the individual shall be considered in determining whether the recommendation will be adverse or favorable.

[47 FR 38676, Sept. 2, 1982, as amended at 64 FR 15641, Apr. 1, 1999]

§ 10.11 Criteria.

(a) The criteria for determining eligibility for access authorization and/or employment clearance shall relate, but not be limited, to the following where an individual:

(1) Committed, attempted to commit, aided, or abetted another who committed or attempted to commit any act of sabotage, espionage, treason, sedition, or terrorism.

(2) Publicly or privately advocated actions that may be inimical to the interest of the United States, or publicly or privately advocated the use of force or violence to overthrow the Government of the United States or the alteration of the form of government of the United States by unconstitutional means.

(3) Knowingly established or continued a sympathetic association with a saboteur, spy, traitor, seditionist, anarchist, terrorist, or revolutionist, or with an espionage agent or other secret agent or representative of a foreign nation whose interests may be inimical to the interests of the United States, or with any person who advocates the use of force or violence to overthrow the Government of the United States or the alteration of the form of government of the United States by unconstitutional means.

(4) Joined or engaged in any activity knowingly in sympathy with or in support of any foreign or domestic organization, association, movement, group, or combination of persons which unlawfully advocates or practices the commission of acts of force or violence to prevent others from exercising their rights under the Constitution or laws of the United States or any State or any subdivisions thereof by unlawful means, or which advocate the use of force and violence to overthrow the Government of the United States or the alteration of the form of government of the United States by unconstitutional means. (Ordinarily, criteria (3) and (4) will not include chance or casual meetings or contacts limited to normal business or official relations.)

(5) Deliberately misrepresented, falsified or omitted relevant and material facts from or in a personnel security questionnaire, a personal qualifications statement, a personnel security interview, or any other information submitted pursuant this part.

(6) Willfully violated or disregarded security regulations or was grossly negligent with respect thereto to a degree which could endanger the common defense and security; or by intention or gross carelessness disclosed Restricted Data or national security information to any person not authorized to receive it.

(7) Has any illness or mental condition which in the opinion of competent medical authority may cause significant defect in the judgment or reliability of the individual.

(8) Has been convicted of crimes indicating habitual criminal tendencies.

(9) Has been convicted of a crime, or has a background, where the facts, circumstances, or conduct are of a nature indicating poor judgment, unreliability, or untrustworthiness.

(10) Is a user of alcohol habitually and to excess, or has been such without adequate evidence of rehabilitation.

(11) Has been, or is, a user of a drug or other substance listed in the schedules of Controlled Substances established pursuant to the Controlled Substances Act of 1970 (such as amphetamines, barbiturates, narcotics, etc.), except as prescribed or administered by a physician licensed to dispense drugs in the practice of medicine, without adequate evidence of rehabilitation.

(12) Refused, without satisfactory explanation, to answer questions before a congressional committee, Federal or state court, or Federal administrative body including the NRC regarding charges relevant to the individual's eligibility for access authorization and/or employment clearance.

(13) Engaged in any other conduct or is subject to any other circumstances which tend to show that the individual is not reliable or trustworthy, or which furnishes reason to believe that the individual may be subject to coercion, influence, or pressures which may cause the individual to act contrary to the national interest.

§ 10.12 Interview and other investigation.

(a) The Director, Division of Facilities and Security, Office of Administration, may authorize the granting of access authorization and/or employment clearance on the basis of the information in the possession of the NRC or may authorize an interview with the individual, if the individual consents to be interviewed, or other investigation as the Director deems appropriate. On the basis of this interview and/or an investigation, the Director may authorize the granting of access authorization and/or employment clearance.

(b) The individual may elect on constitutional or other grounds not to participate in an interview or other investigation; however, such refusal or failure to furnish or authorize the furnishing of relevant and material information is deemed to be derogatory information pursuant to § 10.11(a) (5) and (12).

(c) If the Director, Division of Facilities and Security, cannot make a favorable finding regarding the eligibility of an individual for access authorization and/or employment clearance, the question of the individual's eligibility must be resolved in accordance with the procedures set forth in § 10.20 *et seq.*

[47 FR 38676, Sept. 2, 1982, as amended at 52 FR 31609, Aug. 21, 1987; 54 FR 53316, Dec. 28, 1989; 64 FR 15642, Apr. 1, 1999]

Subpart C—Procedures

§ 10.20 Purpose of the procedures.

These procedures establish methods for the conduct of hearings and administrative review of questions concerning an individual's eligibility for an access authorization and/or an employment clearance pursuant to the Atomic Energy Act of 1954, as amended, and Executive Orders 10450, 10865, and 12968 when a resolution favorable to the individual cannot be made on the basis of the interview or other investigation.

[64 FR 15642, Apr. 1, 1999]

§ 10.21 Suspension of access authorization and/or employment clearance.

In those cases where information is received which raises a question concerning the continued eligibility of an individual for an access authorization and/or an employment clearance, the Director, Division of Facilities and Security, through the Director, Office of Administration, shall forward to the Deputy Executive Director for Information Services and Administration and Chief Information Officer or other Deputy Executive Director, his or her recommendation as to whether the individual's access authorization and/or employment clearance should be suspended pending the final determination resulting from the operation of the procedures provided in this part. In making this recommendation the Director, Division of Facilities and Security, shall consider factors such as the seriousness of the derogatory information developed, the degree of access of the individual to classified information, and the individual's opportunity by reason of his or her position to commit acts adversely affecting the national security. An individual's access authorization and/or employment clearance may not be suspended except by the direction of the Executive Director for Operations, Deputy Executive Director for Information Services and Administration and Chief Information Officer or other Deputy Executive Director.

[64 FR 15642, Apr. 1, 1999]

§ 10.22 Notice to individual.

A notification letter, prepared by the Division of Facilities and Security, approved by the Office of the General Counsel, and signed by the Director, Office of Administration, must be presented to each individual whose eligibility for an access authorization and/or an employment clearance is in question. Where practicable, the letter will be presented to the individual in person. The letter will be accompanied by a copy of this part and must state:

(a) That reliable information in the possession of the NRC has created a substantial doubt concerning the individual's eligibility for an access authorization and/or an employment clearance;

(b) The information that creates a substantial doubt regarding the individual's eligibility for an access authorization and/or an employment clearance, that must be as comprehensive and detailed as the national security interests and other applicable law permit;

(c) That the individual has the right to be represented by counsel or other representative at their own expense;

(d) That the individual may request within 20 days of the date of the notification letter, any documents, records and reports which form the basis for the question of their eligibility for an access authorization and/or an employment clearance. The individual will be provided within 30 days all such documents, records and reports to the extent they are unclassified and do not reveal a confidential source. The individual may also request the entire investigative file, which will be promptly provided, as permitted by the national security interests and other applicable law;

(e) That unless the individual files with the Director, Office of Administration, a written request for a hearing within 20 days of the individual's receipt of the notification letter or 20 days after receipt of the information provided in response to a request made under paragraph (d) of this section, whichever is later, the Director, Division of Facilities and Security, through the Director, Office of Administration, will submit a recommendation as to

the final action to the Deputy Executive Director for Information Services and Administration and Chief Information Officer on the basis of the information in the possession of the NRC;

(f) That if the individual files a written request for a hearing with the Director, Office of Administration, the individual shall file with that request a written answer under oath or affirmation that admits or denies specifically each allegation and each supporting fact contained in the notification letter. A general denial is not sufficient to controvert a specific allegation. If the individual is without knowledge, he or she shall so state and that statement will operate as a denial. The answer must also state any additional facts and information that the individual desires to have considered in explanation or mitigation of allegations in the notification letter. Failure to specifically deny or explain or deny knowledge of any allegation or supporting fact will be deemed an admission that the allegation or fact is true.

(g) That if the individual does not want to exercise his or her right to a hearing, but does want to submit an answer to the allegations in the notification letter, the individual may do so by filing with the Director, Office of Administration, within 20 days of receipt of the notification letter or 20 days after receipt of the information provided in response to a request made under paragraph (d) of this section, whichever is later, a written answer in accordance with the requirements of paragraph (f) of this section;

(h) That the procedures in § 10.24 *et seq.* will apply to any hearing and review.

[64 FR 15642, Apr. 1, 1999]

§ 10.23 Failure of individual to request a hearing.

(a) In the event the individual fails to file a timely written request for a hearing pursuant to § 10.22, a recommendation as to the final action to be taken will be made by the Director, Division of Facilities and Security, through the Director, Office of Administration, to the Deputy Executive Director for Information Services and Administration and Chief Information Officer on the basis of the information in the possession of the NRC, including any answer filed by the individual.

(b) The Director, Office of Administration, may for good cause shown, at the request of the individual, extend the time for filing a written request for a hearing or for filing a written answer to the matters contained in the notification letter.

[47 FR 38676, Sept. 2, 1982, as amended at 52 FR 31609, Aug. 21, 1987; 54 FR 53316, Dec. 28, 1989; 64 FR 15642, Apr. 1, 1999]

§ 10.24 Procedures for hearing and review.

(a) Upon receipt of a timely filed request for a hearing and answer complying with the requirements set forth in § 10.22, the Director, Office of Administration, shall forthwith appoint a Hearing Examiner, and the General Counsel shall forthwith assign an NRC attorney to act as Hearing Counsel. The Director, Office of Administration, shall promptly notify the individual of the identity of the Hearing Examiner and proposed hearing date, which shall be selected with due regard for the convenience of the parties and their representatives.

(b) Within 72 hours of being notified of the identity of the Hearing Examiner, the individual may request that the Hearing Examiner be disqualified for cause by filing with the Director, Office of Administration, a written statement of the individual's reasons for seeking disqualification. The time for filing the request may be extended by the Director, Office of Administration, for good cause shown. If the Director, Office of Administration, grants the request the procedures of paragraph (a) of this section and this paragraph shall be followed just as though there had been no prior appointment.

(c) The individual shall have the right to appear at the hearing before the Hearing Examiner, to be represented by counsel or other representative, to introduce documentary or other evidence, and to call, examine, and cross-examine witnesses, subject to the provisions and limitations set forth in this part.

[47 FR 38676, Sept. 2, 1982, as amended at 51 FR 35999, Oct. 8, 1986; 52 FR 31609, Aug. 21, 1987; 54 FR 53316, Dec. 28, 1989]

§ 10.25 NRC Hearing Counsel.

(a) Hearing Counsel assigned pursuant to § 10.24 will, before the scheduling of the hearing, review the information in the case and will request the presence of witnesses and the production of documents and other physical evidence relied upon by the Director, Division of Facilities and Security, in making a finding that a question exists regarding the eligibility of the individual for an NRC access authorization and/or an employment clearance in accordance with the provisions of this part. When the presence of a witness and the production of documents and other physical evidence is deemed by the Hearing Counsel to be necessary or desirable for a determination of the issues, the Director, Division of Facilities and Security, will make arrangements for the production of evidence and for witnesses to appear at the hearing by subpoena or otherwise.

(b) Hearing Counsel is authorized to consult directly with individual's counsel or representative or the individual, if the individual is not so represented, for purposes of reaching mutual agreement upon arrangements for expeditious hearing of the case. Such arrangements may include clarification of issues and stipulations with respect to testimony and contents of documents and other physical evidence. Such stipulations when entered into shall be binding upon the individual and the NRC for the purposes of this part. Prior to any consultation with the individual, the Hearing Counsel shall advise the individual of his or her rights under this part, of his or her right to counsel or other representation, and of the possibility that any statement made by the individual to the Hearing Counsel may be used in subsequent proceedings.

(c) The individual is responsible for producing witnesses in his or her own behalf and/or presenting other evidence before the Hearing Examiner to support the individual's answer and defense to the allegations contained in the notification letter. When requested by the individual, however, the Hearing Counsel may assist the individual to the extent practicable and necessary. The Hearing Counsel may at his or her discretion request the Director, Division of Facilities and Security, to arrange for the issuance of subpoenas for witnesses to attend the hearing in the individual's behalf, or for the production of specific documents or other physical evidence, provided a showing of the necessity for assistance has been made.

[47 FR 38676, Sept. 2, 1982, as amended at 64 FR 15643, Apr. 1, 1999]

§ 10.26 Appointment of Hearing Examiner.

The appointment of a Hearing Examiner, pursuant to § 10.24 of this part, shall be from a list of qualified attorneys possessing the highest degree of integrity, ability, and good judgment. To qualify, an attorney shall have an NRC "Q" access authorization and may be an employee of the NRC, its contractors, agents or licensees. However, no employee or consultant of the NRC shall serve as Hearing Examiner hearing the case of an employee (including a consultant) or applicant for employment with the NRC, nor shall any employee or consultant of an NRC contractor, agent or licensee serve as Hearing Examiner hearing the case of an employee (including a consultant) or an applicant for employment of that contractor, agent, or licensee. No Hearing Examiner shall be selected who has knowledge of the case or of any information relevant to the disposition of it, or who for any reason would be unable to issue a fair and unbiased recommendation.

§ 10.27 Prehearing proceedings.

(a) After the appointment of the Hearing Examiner, he or she shall be furnished the record in the case, which shall consist of the letter of notification, the request for hearing and its supporting answer, and the notice of hearing, if it has been issued, and any stipulations agreed to by the individual and the Hearing Counsel.

(b) The Hearing Examiner may on his or her own motion, or on that of either party, convene a prehearing conference with the Hearing Counsel and the individual and his or her counsel or representative, if any, for the purpose of clarifying the issues, identifying witnesses who may be called, identifying documents and other physical evidence

that may be offered into evidence, and entering into stipulations of fact.

(c) The parties will be notified by the Hearing Examiner at least ten days in advance of the hearing of the time and place of the hearing. For good cause shown, the Hearing Examiner may order postponements or continuances from time to time. If, after due notice, the individual fails to appear at the hearing, or appears but is not prepared to proceed, the Hearing Examiner shall, unless good cause is shown, return the case to the Director, Division of Facilities and Security, who shall make a recommendation on final action to be taken, through the Director, Office of Administration, to the Deputy Executive Director for Information Services and Administration and Chief Information Officer on the basis of the information in the possession of the NRC.

[47 FR 38676, Sept. 2, 1982, as amended at 52 FR 31609, Aug. 21, 1987; 54 FR 53016, Dec. 28, 1989; 64 FR 15643, Apr. 1, 1999]

§ 10.28 Conduct of hearing.

(a) The Hearing Examiner shall conduct the hearing in an orderly, impartial and decorous manner. Technical rules of evidence may be relaxed so that a full evidentiary record may be made based on all material and relevant facts. Hearsay evidence may for good cause shown be received at the discretion of the Hearing Examiner and accorded such weight as the circumstances warrant.

(b) The proceedings shall be open only to duly authorized representatives of the staff of the NRC, the individual, his or her counsel or representative, and such persons as may be officially authorized by the Hearing Examiner. Witnesses shall not testify in the presence of other witnesses except that the Hearing Examiner may, at his or her discretion, allow for expert witnesses to be present during testimony relevant to their own testimony.

(c) Witnesses, including the individual, shall be examined under oath or affirmation by the party who called them and may be cross-examined by the other. The Hearing Examiner shall rule on all evidentiary matters, may further examine any witness, and may call for additional witnesses or the production of documentary or other physical evidence if, in the exercise of his or her discretion, such additional evidence is deemed necessary to the resolution of an issue.

(d) If it appears during the hearing that Restricted Data or national security information may be disclosed, the Hearing Examiner shall assure that disclosure is made only to persons authorized to receive it.

(e) The Hearing Examiner may, at any time during the hearing, permit the Hearing Counsel to amend the notification letter to add or modify allegations to be considered. In the event of such an amendment to the notification letter, the individual shall be given an opportunity to answer the amended allegations. If the changes are of such a substantial nature that the individual cannot answer the amended allegations without additional time, the Hearing Examiner shall grant such additional time as he or she deems necessary.

(f) The Hearing Examiner may receive and consider evidence in the form of depositions or responses to interrogatories upon a showing that the witness is not available for good reason such as death, serious illness or similar cause, or in the form of depositions, interrogatories, affidavits or statements with agreement of the parties. The Hearing Examiner may take official notice at any stage of the proceeding, where appropriate, of any fact not subject to reasonable dispute in that it is either (1) generally known within the United States or (2) capable of accurate and ready determination by resort to sources whose accuracy cannot reasonably be questioned. A party is entitled upon timely request to an opportunity to be heard as to the propriety of taking such official notice. In the absence of prior notification the request may be made after notice is taken.

(g) Hearing Counsel shall examine and cross-examine witnesses and otherwise assist the Hearing Examiner in such a manner as to bring out a full and true disclosure of all facts, both favorable and unfavorable, having a bearing on the issues before the Hearing Examiner. In performing these duties, the Hearing Counsel shall avoid the attitude of a prosecutor and shall always

bear in mind that the proceeding is an administrative hearing and not a trial.

(h) Hearing Counsel shall not participate in the deliberations of the Hearing Examiner, and shall express no opinion to the Hearing Examiner concerning the merits of the case. Hearing Counsel shall also, during the course of the hearing, advise the individual of his or her rights under these procedures when the individual is not represented by counsel or other representative.

(i) The individual shall be afforded an opportunity to cross-examine persons who have made oral or written statements adverse to the individual relating to a controverted issue except that any such statement may be received and considered by the Hearing Examiner without affording such opportunity in either of the following circumstances:

(1) The head of the department or agency supplying the statement certifies that the person who furnished the information is a confidential informant who has been engaged in obtaining intelligence information for the Government and that disclosure of the informant's identity would substantially harm the national interest or would endanger the well-being of the informant.

(2) The Commission has determined, after considering the information furnished by the investigative agency concerning the reliability of the person who furnished the information and the accuracy of the statement concerned, that the statement appears to be reliable and material, and that failure of the Hearing Examiner to receive and consider such statement would, in view of the fact that access authorization and/or employment clearance is being sought, be substantially harmful to the national security and that the person who furnished the information cannot appear to testify due to death, serious illness, or similar cause.

(j)(1) Whenever the procedure under paragraph (i)(1) of this section is used, the individual shall be given a summary of the information which shall be as comprehensive and detailed as the national security permits.

(2) Whenever the procedure under paragraph (i)(2) is used, the individual shall be provided the identity of the person and the information to be considered.

(3) In both paragraph (i) (1) and (2) procedures, appropriate consideration shall be accorded to the fact that the individual did not have an opportunity to cross-examine such informant or person.

(k) Records provided by investigative agencies that were compiled as a regular or routine procedure by the business or agency from which obtained, or other physical evidence other than investigative reports, may be received and considered subject to rebuttal without authenticating witnesses, provided that the investigative agency furnished such information to the NRC pursuant to its responsibilities in connection with assisting the NRC in determining the individual's eligibility for access authorization and/or employment clearance.

(l) Records compiled in the regular course of business, or other physical evidence other than investigative reports, relating to a controverted issue which, because they are classified, may not be inspected by the individual, may be received and considered provided that:

(1) The Commission has made a determination that such records or other physical evidence appears to be material;

(2) The Commission has made a determination that failure to receive and consider such records or other physical evidence would, in view of the fact that access authorization and/or employment clearance is being sought, be substantially harmful to the national security; and

(3) To the extent that national security permits, a summary or description of such records or other physical evidence is made available to the individual. In every such case, information as to the authenticity and accuracy of such physical evidence furnished by the investigative agency shall be considered.

(m) If the Hearing Examiner determines that additional investigation of any material information is required, he or she shall request in writing that the Director, Office of Administration, arrange for the investigation and shall specify those issues upon which more

evidence is requested and identify, where possible, any persons or sources that might provide the evidence sought.

(n) A written transcript of the entire proceeding must be made by a person possessing appropriate NRC access authorization and/or employment clearance and, except for portions containing Restricted Data or National Security Information, or other lawfully withholdable information, a copy of the transcript will be furnished the individual without cost. The transcript or recording will be made part of the applicant's or employee's personnel security file.

[47 FR 38676, Sept. 2, 1982, as amended at 52 FR 31609, Aug. 21, 1987; 54 FR 53316, Dec. 28, 1989; 64 FR 15643, Apr. 1, 1999]

§ 10.29 Recommendation of the Hearing Examiner.

(a) The Hearing Examiner's findings and recommendation shall be based upon the entire record consisting of the transcript of the hearing, the documentary and other evidence adduced therein, and the letter of notification and answer. The Hearing Examiner shall also consider the circumstances of the receipt of evidence pursuant to § 10.28, the individual's record of past employment, and the nature and sensitivity of the job the individual is or may be expected to perform.

(b) The Hearing Examiner shall make specific findings on each allegation in the notification letter including the reasons for his or her findings, and shall make a recommendation as to the action which should be taken in the case.

(c) The Hearing Examiner's recommendation shall be predicated upon his or her findings. If, after considering all the factors in light of the criteria in this part, the Hearing Examiner is of the opinion that granting or continuing access authorization and/or employment clearance to the individual will not endanger the common defense and security and will be clearly consistent with the national interest, a favorable recommendation shall be made; otherwise, an adverse recommendation shall be made.

(d) The Hearing Examiner shall submit his or her findings and recommendation in a signed report together with the record of the case to the Director, Office Administration, with the least practical delay.

(e) The Hearing Examiner shall not consider the possible impact of the loss of the individual's services upon the NRC program.

[47 FR 38676, Sept. 2, 1982, as amended at 52 FR 31609, Aug. 21, 1987; 54 FR 53316, Dec. 28, 1989]

§ 10.30 New evidence.

After the close of the hearing, in the event the individual discovers new evidence not previously available or known to him or her, the individual may petition the Hearing Examiner if the Hearing Examiner's recommendation has not yet been issued, or thereafter, the Director, Office of Administration, to reopen the record to receive that evidence. If the Hearing Examiner or the Director, respectively, deem it material and appropriate, the record may be reopened to accept the evidence either by stipulation, with the agreement of the Hearing Counsel, or in a reconvened hearing.

[47 FR 38676, Sept. 2, 1982, as amended at 52 FR 31610, Aug. 21, 1987; 54 FR 53316, Dec. 28, 1989]

§ 10.31 Actions on the recommendations.

(a) Upon receipt of the findings and recommendation from the Hearing Examiner, and the record, the Director, Office of Administration, shall forthwith transmit it to the Deputy Executive Director for Information Services and Administration and Chief Information Officer who has the discretion to return the record to the Director, Office of Administration, for further proceedings by the Hearing Examiner with respect to specific matters designated by the Deputy Executive Director for Information Services and Administration and Chief Information Officer.

(b)(1) In the event of a recommendation by the Hearing Examiner that an individual's access authorization and/or employment clearance be denied or

revoked, the Deputy Executive Director for Information Services and Administration and Chief Information Officer shall immediately notify the individual in writing of the Hearing Examiner's findings with respect to each allegation contained in the notification letter, and that the individual has a right to request a review of his or her case by the NRC Personnel Security Review Panel and of the right to submit a brief in support of his or her contentions. The request for a review must be submitted to the Deputy Executive Director for Information Services and Administration and Chief Information Officer within five days after the receipt of the notice. The brief will be forwarded to the Deputy Executive Director for Information Services and Administration and Chief Information Officer, for transmission to the NRC Personnel Security Review Panel not later than 10 days after receipt of the notice.

(2) In the event the individual fails to request a review by the NRC Personnel Security Review Panel of an adverse recommendation within the prescribed time, the Deputy Executive Director for Information Services and Administration and Chief Information Officer may at his or her discretion request a review of the record of the case by the NRC Personnel Security Review Panel. The request will set forth those matters at issue in the hearing on which the Deputy Executive Director for Information Services and Administration and Chief Information Officer desires a review by the NRC Personnel Security Review Panel.

(c) Where the Hearing Examiner has made a recommendation favorable to the individual, the Deputy Executive Director for Information Services and Administration and Chief Information Officer may at his or her discretion request a review of the record of the case by the NRC Personnel Security Review Panel. If this request is made, the Deputy Executive Director for Information Services and Administration and Chief Information Officer shall immediately cause the individual to be notified of that fact and of those matters at issue in the hearing on which the Deputy Executive Director for Information Services and Administration and Chief Information Officer desires a review by the NRC Personnel Security Review Panel. The Deputy Executive Director for Information Services and Administration and Chief Information Officer will further inform the individual that within 10 days of receipt of this notice, the individual may submit a brief concerning those matters at issue for the consideration of the NRC Personnel Security Review Panel. The brief must be forwarded to the Deputy Executive Director for Information Services and Administration and Chief Information Officer for transmission to the NRC Personnel Security Review Panel.

(d) In the event of a request for a review pursuant to paragraphs (b) and (c) of this section, the Hearing Counsel may file a brief within 10 days of being notified by the Deputy Executive Director for Information Services and Administration and Chief Information Officer that a review has been requested. The brief will be forwarded to the Deputy Executive Director for Information Services and Administration and Chief Information Officer for transmission to the NRC Personnel Security Review Panel.

(e) The Hearing Counsel may also request a review of the case by the NRC Personnel Security Review Panel. The request for review, which will set forth those matters at issue in the hearing on which the Hearing Counsel desires a review, will be submitted to the Deputy Director Executive for Management Services within five days after receipt of the Hearing Examiner's findings and recommendation. Within 10 days of the request for review, the Hearing Counsel may file a brief which will be forwarded to the Deputy Executive Director for Information Services and Administration and Chief Information Officer for transmission to the NRC Personnel Security Review Panel. A copy of the request for review, and a copy of any brief filed, will be immediately sent to the individual. If the Hearing Counsel's request is for a review of a recommendation favorable to the individual, the individual may, within 10 days of receipt of a copy of the request for review, submit a brief concerning those matters at issue for consideration of the NRC Personnel Security Review Panel. The brief will be

forwarded to the Deputy Executive Director for Information Services and Administration and Chief Information Officer for transmission to the NRC Personnel Security Review Panel and Hearing Counsel. A copy of the brief will be made a part of the applicant's personnel security file.

(f) The time limits imposed by this section for requesting reviews and the filing of briefs may be extended by the Deputy Executive Director for Information Services and Administration and Chief Information Officer for good cause shown.

(g) In the event a request is made for a review of the record by the NRC Personnel Security Review Panel, the Deputy Executive Director for Information Services and Administration and Chief Information Officer shall send the record, with all findings and recommendations and any briefs filed by the individual and the Hearing Counsel, to the NRC Personnel Security Review Panel. If neither the individual, the Deputy Executive Director for Information Services and Administration and Chief Information Officer, nor the Hearing Counsel requests a review, the final determination will be made by the Deputy Executive Director for Information Services and Administration and Chief Information Officer on the basis of the record with all findings and recommendations.

[64 FR 15643, Apr. 1, 1999]

§ 10.32 Recommendation of the NRC Personnel Security Review Panel.

(a) The Deputy Executive Director for Information Services and Administration and Chief Information Officer shall designate an NRC Personnel Security Review Panel to conduct a review of the record of the case. The NRC Personnel Security Review Panel shall be comprised of three members, two of whom shall be selected from outside the security field. To qualify as an NRC Personnel Security Review Panel member, the person designated shall have an NRC "Q" access authorization and may be an employee of the NRC, its contractors, agents, or licensees. However, no employee or consultant of the NRC shall serve as an NRC Personnel Security Review Panel member reviewing the case of an employee (including a consultant) or applicant for employment with the NRC; nor shall any employee or consultant of an NRC contractor, agent or licensee serve as an NRC Personnel Security Review Panel member reviewing the case of an employee (including a consultant) or an applicant for employment of that contractor, agent, or licensee. No NRC Personnel Security Review Panel member shall be selected who has knowledge of the case or of any information relevant to the disposition of it, or who for any reason would be unable to issue a fair and unbiased recommendation.

(b) The NRC Personnel Security Review Panel shall consider the matter under review based upon the record supplemented by any brief submitted by the individual or the Hearing Counsel. The NRC Personnel Security Review Panel may request additional briefs as the Panel deems appropriate. When the NRC Personnel Security Review Panel determines that additional evidence or further proceedings are necessary, the record may be returned to the Deputy Executive Director for Information Services and Administration and Chief Information Officer with a recommendation that the case be returned to the Director, Office of Administration, for appropriate action, which may include returning the case to the Hearing Examiner and reconvening the hearing to obtain additional testimony. When additional testimony is taken by the Hearing Examiner, a written transcript of the testimony will be made a part of the record and will be taken by a person possessing an appropriate NRC access authorization and/or employment clearance and, except for portions containing Restricted Data or National Security Information, or other lawfully withholdable information, a copy of the transcript will be furnished the individual without cost.

(c) In conducting the review, the NRC Personnel Security Review Panel shall make its findings and recommendations as to the eligibility or continued eligibility of an individual for an access authorization and/or an employment clearance on the record supplemented by additional testimony or briefs, as has been previously determined by the NRC Personnel Security Review Panel as appropriate.

(d) The NRC Personnel Security Review Panel shall not consider the possible impact of the loss of the individual's services upon the NRC program.

(e) If, after considering all the factors in light of the criteria set forth in this part, the NRC Personnel Security Review Panel is of the opinion that granting or continuing an access authorization and/or an employment clearance to the individual will not endanger the common defense and security and will be clearly consistent with the national interest, the NRC Personnel Security Review Panel shall make a favorable recommendation; otherwise, the NRC Personnel Security Review Panel shall make an adverse recommendation. The NRC Personnel Security Review Panel shall prepare a report of its findings and recommendations and submit the report in writing to the Deputy Executive Director for Information Services and Administration and Chief Information Officer, who shall furnish a copy to the individual. The findings and recommendations must be fully supported by stated reasons.

[64 FR 15644, Apr. 1, 1999]

§ 10.33 Action by the Deputy Executive Director for Information Services and Administration and Chief Information Officer.

(a) The Deputy Executive Director for Information Services and Administration and Chief Information Officer, on the basis of the record accompanied by all findings and recommendations, shall make a final determination whether access authorization and/or employment clearance shall be granted, denied, or revoked, except when the provisions of § 10.28 (i), (j), or (l) have been used and the Deputy Executive Director for Information Services and Administration and Chief Information Officer determination is adverse, the Commission shall make the final agency determination.

(b) In making the determination as to whether an access authorization and/or an employment clearance shall be granted, denied, or revoked, the Deputy Executive Director for Information Services and Administration and Chief Information Officer or the Commission shall give due recognition to the favorable as well as the unfavorable information concerning the individual and shall take into account the value of the individual's services to the NRC's program and the consequences of denying or revoking access authorization and/or employment clearance.

(c) In the event of an adverse determination, the Deputy Executive Director for Information Services and Administration and Chief Information Officer shall promptly notify the individual through the Director, Office of Administration, of his or her decision that an access authorization and/or an employment clearance is being denied or revoked and of his or her findings with respect to each allegation contained in the notification letter for transmittal to the individual.

(d) In the event of a favorable determination, the Deputy Executive Director for Information Services and Administration and Chief Information Officer shall promptly notify the individual through the Director, Office of Administration.

[64 FR 15644, Apr. 1, 1999]

§ 10.34 Action by the Commission.

(a) Whenever, under the provisions of § 10.28(i), (j), or (l) an individual has not been afforded an opportunity to confront and cross-examine witnesses who have furnished information adverse to the individual and an adverse recommendation has been made by the Deputy Executive Director for Information Services and Administration and Chief Information Officer, the Commission shall review the record and determine whether an access authorization and/or an employment clearance should be granted, denied, or revoked, based upon the record.

(b) When the Commission determines to deny or revoke access authorization and/or employment clearance, the individual shall promptly be notified through the Director, Office of Administration, of its decision that access authorization and/or employment clearance is being denied or revoked and of its findings and conclusions with respect to each allegation contained in the notification letter for transmittal to the individual.

(c) Nothing contained in these procedures shall be deemed to limit or affect the responsibility and powers of the

Commission to deny or revoke access to Restricted Data or national security information if the security of the nation so requires. Such authority may not be delegated and may be exercised when the Commission determines that invocation of the procedures prescribed in this part is inconsistent with the national security. Such determination shall be conclusive.

[47 FR 38676, Sept. 2, 1982, as amended at 52 FR 31610, Aug. 21, 1987, 54 FR 53316, Dec. 28, 1989, 64 FR 15645, Apr. 1, 1999]

§ 10.35 Reconsideration of cases.

(a) Where, pursuant to the procedures set forth in §§ 10.20 through 10.34, the Deputy Executive Director for Information Services and Administration and Chief Information Officer or the Commission has made a determination granting an access authorization and/or an employment clearance to an individual, the individual's eligibility for an access authorization and/or an employment clearance will be reconsidered only when subsequent to the time of that determination, new derogatory information has been received or the scope or sensitivity of the Restricted Data or National Security Information to which the individual has or will have access has significantly increased. All new derogatory information, whether resulting from the NRC's reinvestigation program or other sources, will be evaluated relative to an individual's continued eligibility in accordance with the procedures of this part.

(b) Where, pursuant to these procedures, the Commission or Deputy Executive Director for Information Services and Administration and Chief Information Officer has made a determination denying or revoking an access authorization and/or an employment clearance to an individual, the individual's eligibility for an access authorization and/or an employment clearance may be reconsidered when there is a bona fide offer of employment and/or a bona fide need for access to Restricted Data or National Security Information and either material and relevant new evidence is presented, which the individual and his or her representatives are without fault in failing to present before, or there is convincing evidence of reformation or rehabilitation. Requests for reconsideration must be submitted in writing to the Deputy Executive Director for Information Services and Administration and Chief Information Officer through the Director, Office of Administration. Requests must be accompanied by an affidavit setting forth in detail the information referred to above. The Deputy Executive Director for Information Services and Administration and Chief Information Officer shall cause the individual to be notified as to whether his or her eligibility for an access authorization and/or an employment clearance will be reconsidered and if so, the method by which a reconsideration will be accomplished.

(c) Where an access authorization and/or an employment clearance has been granted to an individual by the Director, Division of Facilities and Security, without recourse to the procedures set forth in §§ 10.20 through 10.34, the individual's eligibility for an access authorization and/or an employment clearance will be reconsidered only in a case where, subsequent to the granting of the access authorization and/or employment clearance, new derogatory information has been received or the scope or sensitivity of the Restricted Data or National Security Information to which the individual has or will have access has significantly increased. All new derogatory information, whether resulting from the NRC's reinvestigation program or other sources, will be evaluated relative to an individual's continued eligibility in accordance with the procedures of this part.

[64 FR 15645, Apr. 1, 1999]

Subpart D—Miscellaneous

§ 10.36 Terminations.

In the event the individual is no longer an applicant for access authorization and/or employment clearance or no longer requires such, the procedures of this part shall be terminated without a final determination as to the individual's eligibility for access authorization and/or employment clearance

§ 10.37 Attorney representation.

In the event the individual is represented by an attorney or other representative, the individual shall file with the Director, Office of Administration, a document designating such attorney or representative and authorizing such attorney or representative to receive all correspondence, transcripts, and other documents pertaining to the proceeding under this part.

[47 FR 38676, Sept. 2, 1982, as amended at 52 FR 31610, Aug. 21, 1987; 54 FR 53316, Dec. 28, 1989]

§ 10.38 Certifications.

Whenever information is made a part of the record under the exceptions authorized by §10.28 (i), (j), or (l), the record shall contain certificates evidencing that the required determinations have been made.

PART 11—CRITERIA AND PROCEDURES FOR DETERMINING ELIGIBILITY FOR ACCESS TO OR CONTROL OVER SPECIAL NUCLEAR MATERIAL

GENERAL PROVISIONS

REQUIREMENTS FOR SPECIAL NUCLEAR MATERIAL ACCESS AUTHORIZATION

CRITERIA FOR DETERMINING ELIGIBILITY FOR ACCESS TO, OR CONTROL OVER, SPECIAL NUCLEAR MATERIAL

VIOLATIONS

AUTHORITY: Sec. 161, 68 Stat. 948, as amended (42 U.S.C. 2201); sec. 201, 88 Stat. 1242, as amended (42 U.S.C. 5841); sec. 1701, 112 Stat. 2750 (44 U.S.C. 3504 note)

Section 11.15(e) also issued under sec. 501, 85 Stat. 290 (31 U.S.C. 483a).

SOURCE: 45 FR 76970, Nov. 21, 1980, unless otherwise noted.

GENERAL PROVISIONS

§ 11.1 Purpose.

This part establishes the requirements for special nuclear material access authorization, and the criteria and procedures for resolving questions concerning the eligibility of individuals to receive special nuclear material access authorization for conduct of certain activities, licensed or otherwise, which involve access to or control over special nuclear material.

§ 11.3 Scope.

(a) The requirements, criteria, and procedures of this part apply to the establishment of and eligibility for special nuclear material access authorization for employees, contractors, consultants of, and applicants for employment with licensees or contractors of the Nuclear Regulatory Commission. This employment, contract, service, or consultation may involve any duties or assignments within the criteria of §11.11 or §11.13 requiring access to, or control over, formula quantities of special nuclear material (as defined in part 73 of this chapter).

(b) The requirements, criteria, and procedures of this part are in addition to and not in lieu of any requirements, criteria, or procedures for access to or control over classified special nuclear material.

[45 FR 76970, Nov. 21, 1980, as amended at 64 FR 15645, Apr. 1, 1999]

§ 11.5 Policy.

It is the policy of the Nuclear Regulatory Commission to carry out its authority to establish and administer, in a manner consistent with traditional American concepts of justice, a personnel security program in the interests of the common defense and security for the purpose of safeguarding

THE WHITE HOUSE

WASHINGTON

December 29, 2005

MEMORANDUM FOR WILLIAM LEONARD
Director
Information Security Oversight Office

SUBJECT: Adjudicative Guidelines

The President has approved the attached revision of the Adjudicative Guidelines for Determining Eligibility for Access to Classified Information as recommended unanimously by the NSC's PCC on Records Access and Information Security. Please circulate the revised guidelines to all affected agencies for immediate implementation. It is important to emphasize that all agencies must honor clearances granted under these guidelines, consistent with Executive Order 12968 and the December 12, 2005 memorandum to agencies from OMB Deputy Director for Management Clay Johnson.

Stephen J. Hadley
Assistant to the President
for National Security Affairs

Attachment
Tab A Revised Adjudicative Guidelines for Determining Eligibility for Access to Classified Information

Adjudicative Guidelines for Determining Eligibility For Access to Classified Information

1. *Introduction.* The following adjudicative guidelines are established for all U.S. government civilian and military personnel, consultants, contractors, employees of contractors, licensees, certificate holders or grantees and their employees, and other individuals who require access to classified information. They apply to persons being considered for initial or continued eligibility for access to classified information, to include sensitive compartmented information and special access programs, and are to be used by government departments and agencies in all final clearance determinations. Government departments and agencies may also choose to apply these guidelines to analogous situations regarding persons being considered for access to other types of protected information.

Decisions regarding eligibility for access to classified information take into account factors that could cause a conflict of interest and place a person in the position of having to choose between his or her commitments to the United States, including the commitment to protect classified information, and any other compelling loyalty. Access decisions also take into account a person's reliability, trustworthiness and ability to protect classified information. No coercive policing could replace the self-discipline and integrity of the person entrusted with the nation's secrets as the most effective means of protecting them. When a person's life history shows evidence of unreliability or untrustworthiness, questions arise whether the person can be relied on and trusted to exercise the responsibility necessary for working in a secure environment where protecting classified information is paramount.

2. *The Adjudicative Process.*

(a) The adjudicative process is an examination of a sufficient period of a person's life to make an affirmative determination that the person is an acceptable security risk. Eligibility for access to classified information is predicated upon the individual meeting these personnel security guidelines. The adjudication process is the careful weighing of a number of variables known as the whole-person concept. Available, reliable information about the person, past and present, favorable and unfavorable, should be considered in reaching a determination. In evaluating the relevance of an individual's conduct, the adjudicator should consider the following factors:

(1) the nature, extent, and seriousness of the conduct;

(2) the circumstances surrounding the conduct, to include knowledgeable participation;

(3) the frequency and recency of the conduct;

(4) the individual's age and maturity at the time of the conduct;

(5) the extent to which participation is voluntary;

(6) the presence or absence of rehabilitation and other permanent behavioral changes;

(7) the motivation for the conduct;

(8) the potential for pressure, coercion, exploitation, or duress; and

(9) the likelihood of continuation or recurrence;

(b) Each case must be judged on its own merits, and final determination remains the responsibility of the specific department or agency. Any doubt concerning personnel being considered for access to classified information will be resolved in favor of the national security.

(c) The ability to develop specific thresholds for action under these guidelines is limited by the nature and complexity of human behavior. The ultimate determination of whether the granting or continuing of eligibility for a security clearance is clearly consistent with the interests of national security must be an overall common sense judgment based upon careful consideration of the following guidelines, each of which is to be evaluated in the context of the whole person.

(1) GUIDELINE A: Allegiance to the United States;

(2) GUIDELINE B: Foreign Influence

(3) GUIDELINE C: Foreign Preference;

(4) GUIDELINE D: Sexual Behavior;

(5) GUIDELINE E: Personal Conduct;

(6) GUIDELINE F: Financial Considerations;

(7) GUIDELINE G: Alcohol Consumption;

(8) GUIDELINE H: Drug Involvement;

(9) GUIDELINE I: Psychological Conditions;

(10) GUIDELINE J: Criminal Conduct;

(11) GUIDELINE K: Handling Protected Information;

(12) GUIDELINE L: Outside Activities;

(13) GUIDELINE M: Use of Information Technology Systems

(d) Although adverse information concerning a single criterion may not be sufficient for an unfavorable determination, the individual may be disqualified if available information reflects a recent or recurring pattern of questionable judgment, irresponsibility, or emotionally unstable behavior. Notwithstanding the whole-person concept, pursuit of further investigation may be terminated by an appropriate adjudicative agency in the face of reliable, significant, disqualifying, adverse information.

(e) When information of security concern becomes known about an individual who is currently eligible for access to classified information, the adjudicator should consider whether the person:

(1) voluntarily reported the information;

(2) was truthful and complete in responding to questions;

(3) sought assistance and followed professional guidance, where appropriate;

(4) resolved or appears likely to favorably resolve the security concern;

(5) has demonstrated positive changes in behavior and employment;

(6) should have his or her access temporarily suspended pending final adjudication of the information.

(f) If after evaluating information of security concern, the adjudicator decides that the information is not serious enough to warrant a recommendation of disapproval or revocation of the security clearance, it may be appropriate to recommend approval with a warning that future incidents of a similar nature may result in revocation of access.

GUIDELINE A: ALLEGIANCE TO THE UNITED STATES

3. *The Concern.* An individual must be of unquestioned allegiance to the United States. The willingness to safeguard classified information is in doubt if there is any reason to suspect an individual's allegiance to the United States.

4. *Conditions that could raise a security concern and may be disqualifying include:*

(a) involvement in, support of, training to commit, or advocacy of any act of sabotage, espionage, treason, terrorism, or sedition against the United States of America;

(b) association or sympathy with persons who are attempting to commit, or who are committing, any of the above acts;

(c) association or sympathy with persons or organizations that advocate, threaten, or use force or violence, or use any other illegal or unconstitutional means, in an effort to:

(1) overthrow or influence the government of the United States or any state or local government;

(2) prevent Federal, state, or local government personnel from performing their official duties;

(3) gain retribution for perceived wrongs caused by the Federal, state, or local government;

(4) prevent others from exercising their rights under the Constitution or laws of the United States or of any state.

5. *Conditions that could mitigate security concerns include:*

(a) the individual was unaware of the unlawful aims of the individual or organization and severed ties upon learning of these;

(b) the individual's involvement was only with the lawful or humanitarian aspects of such an organization;

(c) involvement in the above activities occurred for only a short period of time and was attributable to curiosity or academic interest;

(d) the involvement or association with such activities occurred under such unusual circumstances, or so much time has elapsed, that it is unlikely to recur and does not cast doubt on the individual's current reliability, trustworthiness, or loyalty.

GUIDELINE B: FOREIGN INFLUENCE

6. *The Concern.* Foreign contacts and interests may be a security concern if the individual has divided loyalties or foreign financial interests, may be manipulated or induced to help a foreign person, group, organization, or government in a way that is not in U.S. interests, or is vulnerable to pressure or coercion by any foreign interest. Adjudication under this Guideline can and should consider the identity of the foreign country in which the foreign contact or financial interest is located, including, but not limited to, such considerations as whether the foreign country is known to target United States citizens to obtain protected information and/or is associated with a risk of terrorism.

7. *Conditions that could raise a security concern and may be disqualifying include:*

(a) contact with a foreign family member, business or professional associate, friend, or other person who is a citizen of or resident in a foreign country if that contact creates a heightened risk of foreign exploitation, inducement, manipulation, pressure, or coercion;

(b) connections to a foreign person, group, government, or country that create a potential conflict of interest between the individual's obligation to protect sensitive information or technology and the individual's desire to help a foreign person, group, or country by providing that information;

(c) counterintelligence information, that may be classified, indicates that the individual's access to protected information may involve unacceptable risk to national security;

(d) sharing living quarters with a person or persons, regardless of citizenship status, if that relationship creates a heightened risk of foreign inducement, manipulation, pressure, or coercion;

(e) a substantial business, financial, or property interest in a foreign country, or in any foreign-owned or foreign-operated business, which could subject the individual to heightened risk of foreign influence or exploitation;

(f) failure to report, when required, association with a foreign national;

(g) unauthorized association with a suspected or known agent, associate, or employee of a foreign intelligence service;

(h) indications that representatives or nationals from a foreign country are acting to increase the vulnerability of the individual to possible future exploitation, inducement, manipulation, pressure, or coercion;

(i) conduct, especially while traveling outside the U.S., which may make the individual vulnerable to exploitation, pressure, or coercion by a foreign person, group, government, or country.

8. *Conditions that could mitigate security concerns include:*

(a) the nature of the relationships with foreign persons, the country in which these persons are located, or the positions or activities of those persons in that country are such that it is unlikely the individual will be placed in a position of having to choose between the interests of a foreign individual, group, organization, or government and the interests of the U.S.;

(b) there is no conflict of interest, either because the individual's sense of loyalty or obligation to the foreign person, group, government, or country is so minimal, or the individual has such deep and longstanding relationships and loyalties in the U.S., that the individual can be expected to resolve any conflict of interest in favor of the U.S. interest;

(c) contact or communication with foreign citizens is so casual and infrequent that there is little likelihood that it could create a risk for foreign influence or exploitation;

(d) the foreign contacts and activities are on U.S. Government business or are approved by the cognizant security authority;

(e) the individual has promptly complied with existing agency requirements regarding the reporting of contacts, requests, or threats from persons, groups, or organizations from a foreign country;

(f) the value or routine nature of the foreign business, financial, or property interests is such that they are unlikely to result in a conflict and could not be used effectively to influence, manipulate, or pressure the individual.

GUIDELINE C: FOREIGN PREFERENCE

9. *The Concern.* When an individual acts in such a way as to indicate a preference for a foreign country over the United States, then he or she may be prone to provide information or make decisions that are harmful to the interests of the United States.

10. *Conditions that could raise a security concern and may be disqualifying include:*

(a) exercise of any right, privilege or obligation of foreign citizenship after becoming a U.S. citizen or through the foreign citizenship of a family member. This includes but is not limited to:

(1) possession of a current foreign passport;

(2) military service or a willingness to bear arms for a foreign country;

(3) accepting educational, medical, retirement, social welfare, or other such benefits from a foreign country;

(4) residence in a foreign country to meet citizenship requirements;

(5) using foreign citizenship to protect financial or business interests in another country;

(6) seeking or holding political office in a foreign country;

(7) voting in a foreign election;

(b) action to acquire or obtain recognition of a foreign citizenship by an American citizen;

(c) performing or attempting to perform duties, or otherwise acting, so as to serve the interests of a foreign person, group, organization, or government in conflict with the national security interest;

(d) any statement or action that shows allegiance to a country other than the United States: for example, declaration of intent to renounce United States citizenship; renunciation of United States citizenship.

11. *Conditions that could mitigate security concerns include:*

(a) dual citizenship is based solely on parents' citizenship or birth in a foreign country;

(b) the individual has expressed a willingness to renounce dual citizenship;

(c) exercise of the rights, privileges, or obligations of foreign citizenship occurred before the individual became a U.S. citizen or when the individual was a minor;

(d) use of a foreign passport is approved by the cognizant security authority;

(e) the passport has been destroyed, surrendered to the cognizant security authority, or otherwise invalidated;

(f) the vote in a foreign election was encouraged by the United States Government.

GUIDELINE D: SEXUAL BEHAVIOR

12. *The Concern.* Sexual behavior that involves a criminal offense, indicates a personality or emotional disorder, reflects lack of judgment or discretion, or which may subject the individual to undue influence or coercion, exploitation, or duress can raise questions about an individual's reliability, trustworthiness and ability to protect classified information. No adverse inference concerning the standards in this Guideline may be raised solely on the basis of the sexual orientation of the individual.

13. *Conditions that could raise a security concern and may be disqualifying include:*

(a) sexual behavior of a criminal nature, whether or not the individual has been prosecuted;

(b) a pattern of compulsive, self-destructive, or high risk sexual behavior that the person is unable to stop or that may be symptomatic of a personality disorder;

(c) sexual behavior that causes an individual to be vulnerable to coercion, exploitation, or duress;

(d) sexual behavior of a public nature and/or that reflects lack of discretion or judgment.

14. *Conditions that could mitigate security concerns include*:

(a) the behavior occurred prior to or during adolescence and there is no evidence of subsequent conduct of a similar nature;

(b) the sexual behavior happened so long ago, so infrequently, or under such unusual circumstances, that it is unlikely to recur and does not cast doubt on the individual's current reliability, trustworthiness, or good judgment;

(c) the behavior no longer serves as a basis for coercion, exploitation, or duress.

(d) the sexual behavior is strictly private, consensual, and discreet.

GUIDELINE E: PERSONAL CONDUCT

15. *The Concern.* Conduct involving questionable judgment, lack of candor, dishonesty, or unwillingness to comply with rules and regulations can raise questions about an individual's reliability, trustworthiness and ability to protect classified information. Of special interest is any failure to provide truthful and candid answers during the security clearance process or any other failure to cooperate with the security clearance process.

The following will normally result in an unfavorable clearance action or administrative termination of further processing for clearance eligibility:

(a) refusal, or failure without reasonable cause, to undergo or cooperate with security processing, including but not limited to meeting with a security investigator for subject interview, completing security forms or releases, and cooperation with medical or psychological evaluation;

(b) refusal to provide full, frank and truthful answers to lawful questions of investigators, security officials, or other official representatives in connection with a personnel security or trustworthiness determination.

16. *Conditions that could raise a security concern and may be disqualifying include*

(a) deliberate omission, concealment, or falsification of relevant facts from any personnel security questionnaire, personal history statement, or similar form used to conduct investigations, determine employment qualifications, award benefits or status, determine security clearance eligibility or trustworthiness, or award fiduciary responsibilities;

(b) deliberately providing false or misleading information concerning relevant facts to an employer, investigator, security official, competent medical authority, or other official government representative;

(c) credible adverse information in several adjudicative issue areas that is not sufficient for an adverse determination under any other single guideline, but which, when considered as a whole, supports a whole-person assessment of questionable judgment, untrustworthiness, unreliability, lack of candor, unwillingness to comply with rules and regulations, or other characteristics indicating that the person may not properly safeguard protected information;

(d) credible adverse information that is not explicitly covered under any other guideline and may not be sufficient by itself for an adverse determination, but which, when combined with all available information supports a whole-person assessment of questionable judgment, untrustworthiness, unreliability, lack of candor, unwillingness to comply with rules and regulations, or other characteristics indicating that the person may not properly safeguard protected information. This includes but is not limited to consideration of:

(1) untrustworthy or unreliable behavior to include breach of client confidentiality, release of proprietary information, unauthorized release of sensitive corporate or other government protected information;

(2) disruptive, violent, or other inappropriate behavior in the workplace;

(3) a pattern of dishonesty or rule violations;

(4) evidence of significant misuse of Government or other employer's time or resources;

(e) personal conduct, or concealment of information about one's conduct, that creates a vulnerability to exploitation, manipulation, or duress, such as (1) engaging in activities which, if known, may affect the person's personal, professional, or community standing, or (2) while in another country, engaging in any activity that is illegal in that country or that is legal in that country but illegal in the United States and may serve as a basis for exploitation or pressure by the foreign security or intelligence service or other group;

(f) violation of a written or recorded commitment made by the individual to the employer as a condition of employment;

(g) association with persons involved in criminal activity.

17. *Conditions that could mitigate security concerns include:*

(a) the individual made prompt, good-faith efforts to correct the omission, concealment, or falsification before being confronted with the facts;

(b) the refusal or failure to cooperate, omission, or concealment was caused or significantly contributed to by improper or inadequate advice of authorized personnel or legal counsel advising or instructing the individual specifically concerning the security clearance process. Upon being made aware of the requirement to cooperate or provide the information, the individual cooperated fully and truthfully.

(c) the offense is so minor, or so much time has passed, or the behavior is so infrequent, or it happened under such unique circumstances that it is unlikely to recur and does not cast doubt on the individual's reliability, trustworthiness, or good judgment;

(d) the individual has acknowledged the behavior and obtained counseling to change the behavior or taken other positive steps to alleviate the stressors, circumstances, or factors that caused untrustworthy, unreliable, or other inappropriate behavior, and such behavior is unlikely to recur;

(e) the individual has taken positive steps to reduce or eliminate vulnerability to exploitation, manipulation, or duress;

(f) the information was unsubstantiated or from a source of questionable reliability;

(g) association with persons involved in criminal activity has ceased or occurs under circumstances that do not cast doubt upon the individual's reliability, trustworthiness, judgment, or willingness to comply with rules and regulations.

GUIDELINE F: FINANCIAL CONSIDERATIONS

18. *The Concern.* Failure or inability to live within one's means, satisfy debts, and meet financial obligations may indicate poor self-control, lack of judgment, or unwillingness to abide by rules and regulations, all of which can raise questions about an individual's reliability, trustworthiness and ability to protect classified information. An individual who is financially overextended is at risk of having to engage in illegal acts to generate funds. Compulsive gambling is a concern as it may lead to financial crimes including espionage. Affluence that cannot be explained by known sources of income is also a security concern. It may indicate proceeds from financially profitable criminal acts.

19. *Conditions that could raise a security concern and may be disqualifying include*:

(a) inability or unwillingness to satisfy debts;

(b) indebtedness caused by frivolous or irresponsible spending and the absence of any evidence of willingness or intent to pay the debt or establish a realistic plan to pay the debt.

(c) a history of not meeting financial obligations;

(d) deceptive or illegal financial practices such as embezzlement, employee theft, check fraud, income tax evasion, expense account fraud, filing deceptive loan statements, and other intentional financial breaches of trust;

(e) consistent spending beyond one's means, which may be indicated by excessive indebtedness, significant negative cash flow, high debt-to-income ratio, and/or other financial analysis;

(f) financial problems that are linked to drug abuse, alcoholism, gambling problems, or other issues of security concern;

(g) failure to file annual Federal, state, or local income tax returns as required or the fraudulent filing of the same;

(h) unexplained affluence, as shown by a lifestyle or standard of living, increase in net worth, or money transfers that cannot be explained by subject's known legal sources of income;

(i) compulsive or addictive gambling as indicated by an unsuccessful attempt to stop gambling, "chasing losses" (i.e. increasing the bets or returning another day in an effort to get even), concealment of gambling losses, borrowing money to fund gambling or pay gambling debts, family conflict or other problems caused by gambling.

20. *Conditions that could mitigate security concerns include:*

(a) the behavior happened so long ago, was so infrequent, or occurred under such circumstances that it is unlikely to recur and does not cast doubt on the individual's current reliability, trustworthiness, or good judgment;

(b) the conditions that resulted in the financial problem were largely beyond the person's control (e.g., loss of employment, a business downturn, unexpected medical emergency, or a death, divorce or separation), and the individual acted responsibly under the circumstances;

(c) the person has received or is receiving counseling for the problem and/or there are clear indications that the problem is being resolved or is under control;

(d) the individual initiated a good-faith effort to repay overdue creditors or otherwise resolve debts;

(e) the individual has a reasonable basis to dispute the legitimacy of the past-due debt which is the cause of the problem and provides documented proof to substantiate the basis of the dispute or provides evidence of actions to resolve the issue;

(f) the affluence resulted from a legal source of income.

GUIDELINE G: ALCOHOL CONSUMPTION

21. *The Concern.* Excessive alcohol consumption often leads to the exercise of questionable judgment or the failure to control impulses, and can raise questions about an individual's reliability and trustworthiness.

22. *Conditions that could raise a security concern and may be disqualifying include:*

(a) alcohol-related incidents away from work, such as driving while under the influence, fighting, child or spouse abuse, disturbing the peace, or other incidents of concern, regardless of whether the individual is diagnosed as an alcohol abuser or alcohol dependent;

(b) alcohol-related incidents at work, such as reporting for work or duty in an intoxicated or impaired condition, or drinking on the job, regardless of whether the individual is diagnosed as an alcohol abuser or alcohol dependent;

(c) habitual or binge consumption of alcohol to the point of impaired judgment, regardless of whether the individual is diagnosed as an alcohol abuser or alcohol dependent;

(d) diagnosis by a duly qualified medical professional (e.g., physician, clinical psychologist, or psychiatrist) of alcohol abuse or alcohol dependence;

(e) evaluation of alcohol abuse or alcohol dependence by a licensed clinical social worker who is a staff member of a recognized alcohol treatment program;

(f) relapse after diagnosis of alcohol abuse or dependence and completion of an alcohol rehabilitation program;

(g) failure to follow any court order regarding alcohol education, evaluation, treatment, or abstinence.

23. *Conditions that could mitigate security concerns include*:

(a) so much time has passed, or the behavior was so infrequent, or it happened under such unusual circumstances that it is unlikely to recur or does not cast doubt on the individual's current reliability, trustworthiness, or good judgment;

(b) the individual acknowledges his or her alcoholism or issues of alcohol abuse, provides evidence of actions taken to overcome this problem, and has established a pattern of abstinence (if alcohol dependent) or responsible use (if an alcohol abuser);

(c) the individual is a current employee who is participating in a counseling or treatment program, has no history of previous treatment and relapse, and is making satisfactory progress;

(d) the individual has successfully completed inpatient or outpatient counseling or rehabilitation along with any required aftercare, has demonstrated a clear and established pattern of modified consumption or abstinence in accordance with treatment recommendations, such as participation in meetings of Alcoholics Anonymous or a similar organization and has received a favorable prognosis by a duly qualified medical professional or a licensed clinical social worker who is a staff member of a recognized alcohol treatment program.

GUIDELINE H: DRUG INVOLVEMENT

24. *The Concern.* Use of an illegal drug or misuse of a prescription drug can raise questions about an individual's reliability and trustworthiness, both because it may impair judgment and because it raises questions about a person's ability or willingness to comply with laws, rules, and regulations.

(a) Drugs are defined as mood and behavior altering substances, and include:

(1) Drugs, materials, and other chemical compounds identified and listed in the Controlled Substances Act of 1970, as amended (e.g., marijuana or cannabis, depressants, narcotics, stimulants, and hallucinogens), and

(2) inhalants and other similar substances;

(b) drug abuse is the illegal use of a drug or use of a legal drug in a manner that deviates from approved medical direction.

25. *Conditions that could raise a security concern and may be disqualifying include:*

(a) any drug abuse (see above definition);

(b) testing positive for illegal drug use;

(c) illegal drug possession, including cultivation, processing, manufacture, purchase, sale, or distribution; or possession of drug paraphernalia;

(d) diagnosis by a duly qualified medical professional (e.g., physician, clinical psychologist, or psychiatrist) of drug abuse or drug dependence;

(e) evaluation of drug abuse or drug dependence by a licensed clinical social worker who is a staff member of a recognized drug treatment program;

(f) failure to successfully complete a drug treatment program prescribed by a duly qualified medical professional;

(g) any illegal drug use after being granted a security clearance;

(h) expressed intent to continue illegal drug use, or failure to clearly and convincingly commit to discontinue drug use.

26. *Conditions that could mitigate security concerns include:*

(a) the behavior happened so long ago, was so infrequent, or happened under such circumstances that it is unlikely to recur or does not cast doubt on the individual's current reliability, trustworthiness, or good judgment;

(b) a demonstrated intent not to abuse any drugs in the future, such as:

(1) disassociation from drug-using associates and contacts;

(2) changing or avoiding the environment where drugs were used;

(3) an appropriate period of abstinence;

(4) a signed statement of intent with automatic revocation of clearance for any violation;

(c) abuse of prescription drugs was after a severe or prolonged illness during which these drugs were prescribed, and abuse has since ended;

(d) satisfactory completion of a prescribed drug treatment program, including but not limited to rehabilitation and aftercare requirements, without recurrence of abuse, and a favorable prognosis by a duly qualified medical professional.

GUIDELINE I: PSYCHOLOGICAL CONDITIONS

27. *The Concern.* Certain emotional, mental, and personality conditions can impair judgment, reliability, or trustworthiness. A formal diagnosis of a disorder is not required for there to be a concern under this guideline. A duly qualified mental health professional (e.g., clinical psychologist or psychiatrist) employed by, or acceptable to and approved by the U.S. Government, should be consulted when evaluating potentially disqualifying and mitigating information under this guideline. No negative inference concerning the standards in this Guideline may be raised solely on the basis of seeking mental health counseling.

28. *Conditions that could raise a security concern and may be disqualifying include*:

(a) behavior that casts doubt on an individual's judgment, reliability, or trustworthiness that is not covered under any other guideline, including but not limited to emotionally unstable, irresponsible, dysfunctional, violent, paranoid, or bizarre behavior;

(b) an opinion by a duly qualified mental health professional that the individual has a condition not covered under any other guideline that may impair judgment, reliability, or trustworthiness;

(c) the individual has failed to follow treatment advice related to a diagnosed emotional, mental, or personality condition, e.g., failure to take prescribed medication.

29. *Conditions that could mitigate security concerns include*:

(a) the identified condition is readily controllable with treatment, and the individual has demonstrated ongoing and consistent compliance with the treatment plan;

(b) the individual has voluntarily entered a counseling or treatment program for a condition that is amenable to treatment, and the individual is currently receiving counseling or treatment with a favorable prognosis by a duly qualified mental health professional;

(c) recent opinion by a duly qualified mental health professional employed by, or acceptable to and approved by the U.S. Government that an individual's previous condition is under control or in remission, and has a low probability of recurrence or exacerbation;

(d) the past emotional instability was a temporary condition (e.g., one caused by death, illness, or marital breakup), the situation has been resolved, and the individual no longer shows indications of emotional instability;

(e) there is no indication of a current problem.

GUIDELINE J: CRIMINAL CONDUCT

30. *The Concern.* Criminal activity creates doubt about a person's judgment, reliability, and trustworthiness. By its very nature, it calls into question a person's ability or willingness to comply with laws, rules and regulations.

31. *Conditions that could raise a security concern and may be disqualifying include:*

(a) a single serious crime or multiple lesser offenses;

(b) discharge or dismissal from the Armed Forces under dishonorable conditions;

(c) allegation or admission of criminal conduct, regardless of whether the person was formally charged, formally prosecuted or convicted;

(d) individual is currently on parole or probation;

(e) violation of parole or probation, or failure to complete a court-mandated rehabilitation program.

32. *Conditions that could mitigate security concerns include:*

(a) so much time has elapsed since the criminal behavior happened, or it happened under such unusual circumstances that it is unlikely to recur and does not cast doubt on the individual's reliability, trustworthiness, or good judgment;

(b) the person was pressured or coerced into committing the act and those pressures are no longer present in the person's life;

(c) evidence that the person did not commit the offense;

(d) there is evidence of successful rehabilitation; including but not limited to the passage of time without recurrence of criminal activity, remorse or restitution, job training or higher education, good employment record, or constructive community involvement.

GUIDELINE K: HANDLING PROTECTED INFORMATION

33. *The Concern.* Deliberate or negligent failure to comply with rules and regulations for protecting classified or other sensitive information raises doubt about an individual's trustworthiness, judgment, reliability, or willingness and ability to safeguard such information, and is a serious security concern.

34. *Conditions that could raise a security concern and may be disqualifying include:*

(a) deliberate or negligent disclosure of classified or other protected information to unauthorized persons, including but not limited to personal or business contacts, to the media, or to persons present at seminars, meetings, or conferences;

(b) collecting or storing classified or other protected information in any unauthorized location;

(c) loading, drafting, editing, modifying, storing, transmitting, or otherwise handling classified reports, data, or other information on any unapproved equipment including but not limited to any typewriter, word processor, or computer hardware, software, drive, system, gameboard, handheld, "palm" or pocket device or other adjunct equipment;

(d) inappropriate efforts to obtain or view classified or other protected information outside one's need to know;

(e) copying classified or other protected information in a manner designed to conceal or remove classification or other document control markings;

(f) viewing or downloading information from a secure system when the information is beyond the individual's need-to-know;

(g) any failure to comply with rules for the protection of classified or other sensitive information;

(h) negligence or lax security habits that persist despite counseling by management.

(i) failure to comply with rules or regulations that results in damage to the National Security, regardless of whether it was deliberate or negligent.

35. *Conditions that could mitigate security concerns include*:

(a) so much time has elapsed since the behavior, or it has happened so infrequently or under such unusual circumstances, that it is unlikely to recur and does not cast doubt on the individual's current reliability, trustworthiness, or good judgment;

(b) the individual responded favorably to counseling or remedial security training and now demonstrates a positive attitude toward the discharge of security responsibilities;

(c) the security violations were due to improper or inadequate training.

GUIDELINE L: OUTSIDE ACTIVITIES

36. *The Concern*. Involvement in certain types of outside employment or activities is of security concern if it poses a conflict of interest with an individual's security responsibilities and could create an increased risk of unauthorized disclosure of classified information.

37. *Conditions that could raise a security concern and may be disqualifying include*:

(a) any employment or service, whether compensated or volunteer, with:

(1) the government of a foreign country;

(2) any foreign national, organization, or other entity;

(3) a representative of any foreign interest;

(4) any foreign, domestic, or international organization or person engaged in analysis, discussion, or publication of material on intelligence, defense, foreign affairs, or protected technology;

(b) failure to report or fully disclose an outside activity when this is required.

38. *Conditions that could mitigate security concerns include*:

(a) evaluation of the outside employment or activity by the appropriate security or counterintelligence office indicates that it does not pose a conflict with an individual's security responsibilities or with the national security interests of the United States;

(b) the individual terminated the employment or discontinued the activity upon being notified that it was in conflict with his or her security responsibilities.

GUIDELINE M: USE OF INFORMATION TECHNOLOGY SYSTEMS

39. *The Concern.* Noncompliance with rules, procedures, guidelines or regulations pertaining to information technology systems may raise security concerns about an individual's reliability and trustworthiness, calling into question the willingness or ability to properly protect sensitive systems, networks, and information. Information Technology Systems include all related computer hardware, software, firmware, and data used for the communication, transmission, processing, manipulation, storage, or protection of information.

40. *Conditions that could raise a security concern and may be disqualifying include*:

(a) illegal or unauthorized entry into any information technology system or component thereof;

(b) illegal or unauthorized modification, destruction, manipulation or denial of access to information, software, firmware, or hardware in an information technology system;

(c) use of any information technology system to gain unauthorized access to another system or to a compartmented area within the same system;

(d) downloading, storing, or transmitting classified information on or to any unauthorized software, hardware, or information technology system;

(e) unauthorized use of a government or other information technology system;

(f) introduction, removal, or duplication of hardware, firmware, software, or media to or from any information technology system without authorization, when prohibited by rules, procedures, guidelines or regulations;

(g) negligence or lax security habits in handling information technology that persist despite counseling by management;

(h) any misuse of information technology, whether deliberate or negligent, that results in damage to the national security.

41. *Conditions that could mitigate security concerns include*:

(a) so much time has elapsed since the behavior happened, or it happened under such unusual circumstances, that it is unlikely to recur and does not cast doubt on the individual's reliability, trustworthiness, or good judgment;

(b) the misuse was minor and done only in the interest of organizational efficiency and effectiveness, such as letting another person use one's password or computer when no other timely alternative was readily available;

(c) the conduct was unintentional or inadvertent and was followed by a prompt, good-faith effort to correct the situation and by notification of supervisor.

Federal Register
Vol. 60, No. 151
Monday, August 7, 1995

Presidential Documents

Title 3—

The President

Executive Order 12968 of August 2, 1995

Access to Classified Information

The national interest requires that certain information be maintained in confidence through a system of classification in order to protect our citizens, our democratic institutions, and our participation within the community of nations. The unauthorized disclosure of information classified in the national interest can cause irreparable damage to the national security and loss of human life.

Security policies designed to protect classified information must ensure consistent, cost effective, and efficient protection of our Nation's classified information, while providing fair and equitable treatment to those Americans upon whom we rely to guard our national security.

This order establishes a uniform Federal personnel security program for employees who will be considered for initial or continued access to classified information.

NOW, THEREFORE, by the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

PART 1—DEFINITIONS, ACCESS TO CLASSIFIED INFORMATION, FINANCIAL DISCLOSURE, AND OTHER ITEMS

Section 1.1. *Definitions.* For the purposes of this order: (a) "Agency" means any "Executive agency," as defined in 5 U.S.C. 105, the "military departments," as defined in 5 U.S.C. 102, and any other entity within the executive branch that comes into the possession of classified information, including the Defense Intelligence Agency, National Security Agency, and the National Reconnaissance Office.

(b) "Applicant" means a person other than an employee who has received an authorized conditional offer of employment for a position that requires access to classified information.

(c) "Authorized investigative agency" means an agency authorized by law or regulation to conduct a counterintelligence investigation or investigation of persons who are proposed for access to classified information to ascertain whether such persons satisfy the criteria for obtaining and retaining access to such information.

(d) "Classified information" means information that has been determined pursuant to Executive Order No. 12958, or any successor order, Executive Order No. 12951, or any successor order, or the Atomic Energy Act of 1954 (42 U.S.C. 2011), to require protection against unauthorized disclosure.

(e) "Employee" means a person, other than the President and Vice President, employed by, detailed or assigned to, an agency, including members of the Armed Forces; an expert or consultant to an agency; an industrial or commercial contractor, licensee, certificate holder, or grantee of an agency, including all subcontractors; a personal services contractor; or any other category of person who acts for or on behalf of an agency as determined by the appropriate agency head.

(f) "Foreign power" and "agent of a foreign power" have the meaning provided in 50 U.S.C. 1801.

(g) "Need for access" means a determination that an employee requires access to a particular level of classified information in order to perform or assist in a lawful and authorized governmental function.

(h) "Need-to-know" means a determination made by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.

(i) "Overseas Security Policy Board" means the Board established by the President to consider, develop, coordinate and promote policies, standards and agreements on overseas security operations, programs and projects that affect all United States Government agencies under the authority of a Chief of Mission.

(j) "Security Policy Board" means the Board established by the President to consider, coordinate, and recommend policy directives for U.S. security policies, procedures, and practices.

(k) "Special access program" has the meaning provided in section 4.1 of Executive Order No. 12958, or any successor order.

Sec. 1.2. *Access to Classified Information.* (a) No employee shall be granted access to classified information unless that employee has been determined to be eligible in accordance with this order and to possess a need-to-know.

(b) Agency heads shall be responsible for establishing and maintaining an effective program to ensure that access to classified information by each employee is clearly consistent with the interests of the national security.

(c) Employees shall not be granted access to classified information unless they:

(1) have been determined to be eligible for access under section 3.1 of this order by agency heads or designated officials based upon a favorable adjudication of an appropriate investigation of the employee's background;

(2) have a demonstrated need-to-know; and

(3) have signed an approved nondisclosure agreement.

(d) All employees shall be subject to investigation by an appropriate government authority prior to being granted access to classified information and at any time during the period of access to ascertain whether they continue to meet the requirements for access.

(e)(1) All employees granted access to classified information shall be required as a condition of such access to provide to the employing agency written consent permitting access by an authorized investigative agency, for such time as access to classified information is maintained and for a period of 3 years thereafter, to:

(A) relevant financial records that are maintained by a financial institution as defined in 31 U.S.C. 5312(a) or by a holding company as defined in section 1101(6) of the Right to Financial Privacy Act of 1978 (12 U.S.C. 3401);

(B) consumer reports pertaining to the employee under the Fair Credit Reporting Act (15 U.S.C. 1681a); and

(C) records maintained by commercial entities within the United States pertaining to any travel by the employee outside the United States.

(2) Information may be requested pursuant to employee consent under this section where:

(A) there are reasonable grounds to believe, based on credible information, that the employee or former employee is, or may be, disclosing classified information in an unauthorized manner to a foreign power or agent of a foreign power;

(B) information the employing agency deems credible indicates the employee or former employee has incurred excessive indebtedness or has ac-

quired a level of affluence that cannot be explained by other information; or

(C) circumstances indicate the employee or former employee had the capability and opportunity to disclose classified information that is known to have been lost or compromised to a foreign power or an agent of a foreign power.

(3) Nothing in this section shall be construed to affect the authority of an investigating agency to obtain information pursuant to the Right to Financial Privacy Act, the Fair Credit Reporting Act or any other applicable law.

Sec. 1.3. *Financial Disclosure.* (a) Not later than 180 days after the effective date of this order, the head of each agency that originates, handles, transmits, or possesses classified information shall designate each employee, by position or category where possible, who has a regular need for access to classified information that, in the discretion of the agency head, would reveal:

(1) the identity of covert agents as defined in the Intelligence Identities Protection Act of 1982 (50 U.S.C. 421);

(2) technical or specialized national intelligence collection and processing systems that, if disclosed in an unauthorized manner, would substantially negate or impair the effectiveness of the system;

(3) the details of:

(A) the nature, contents, algorithm, preparation, or use of any code, cipher, or cryptographic system or;

(B) the design, construction, functioning, maintenance, or repair of any cryptographic equipment; but not including information concerning the use of cryptographic equipment and services;

(4) particularly sensitive special access programs, the disclosure of which would substantially negate or impair the effectiveness of the information or activity involved; or

(5) especially sensitive nuclear weapons design information (but only for those positions that have been certified as being of a high degree of importance or sensitivity, as described in section 145(f) of the Atomic Energy Act of 1954, as amended).

(b) An employee may not be granted access, or hold a position designated as requiring access, to information described in subsection (a) unless, as a condition of access to such information, the employee:

(1) files with the head of the agency a financial disclosure report, including information with respect to the spouse and dependent children of the employee, as part of all background investigations or reinvestigations;

(2) is subject to annual financial disclosure requirements, if selected by the agency head; and

(3) files relevant information concerning foreign travel, as determined by the Security Policy Board.

(c) Not later than 180 days after the effective date of this order, the Security Policy Board shall develop procedures for the implementation of this section, including a standard financial disclosure form for use by employees under subsection (b) of this section, and agency heads shall identify certain employees, by position or category, who are subject to annual financial disclosure.

Sec. 1.4. *Use of Automated Financial Record Data Bases.* As part of all investigations and reinvestigations described in section 1.2(d) of this order, agencies may request the Department of the Treasury, under terms and conditions prescribed by the Secretary of the Treasury, to search automated data bases consisting of reports of currency transactions by financial institutions, international transportation of currency or monetary instruments, foreign bank and financial accounts, transactions under $10,000 that are reported as possible money laundering violations, and records of foreign travel.

Sec. 1.5. *Employee Education and Assistance.* The head of each agency that grants access to classified information shall establish a program for employees with access to classified information to: (a) educate employees about individual responsibilities under this order; and

(b) inform employees about guidance and assistance available concerning issues that may affect their eligibility for access to classified information, including sources of assistance for employees who have questions or concerns about financial matters, mental health, or substance abuse.

PART 2—ACCESS ELIGIBILITY POLICY AND PROCEDURE

Sec. 2.1. *Eligibility Determinations.* (a) Determinations of eligibility for access to classified information shall be based on criteria established under this order. Such determinations are separate from suitability determinations with respect to the hiring or retention of persons for employment by the government or any other personnel actions.

(b) The number of employees that each agency determines are eligible for access to classified information shall be kept to the minimum required for the conduct of agency functions.

(1) Eligibility for access to classified information shall not be requested or granted solely to permit entry to, or ease of movement within, controlled areas when the employee has no need for access and access to classified information may reasonably be prevented. Where circumstances indicate employees may be inadvertently exposed to classified information in the course of their duties, agencies are authorized to grant or deny, in their discretion, facility access approvals to such employees based on an appropriate level of investigation as determined by each agency.

(2) Except in agencies where eligibility for access is a mandatory condition of employment, eligibility for access to classified information shall only be requested or granted based on a demonstrated, foreseeable need for access. Requesting or approving eligibility in excess of actual requirements is prohibited.

(3) Eligibility for access to classified information may be granted where there is a temporary need for access, such as one-time participation in a classified project, provided the investigative standards established under this order have been satisfied. In such cases, a fixed date or event for expiration shall be identified and access to classified information shall be limited to information related to the particular project or assignment.

(4) Access to classified information shall be terminated when an employee no longer has a need for access.

Sec. 2.2. *Level of Access Approval.* (a) The level at which an access approval is granted for an employee shall be limited, and relate directly, to the level of classified information for which there is a need for access. Eligibility for access to a higher level of classified information includes eligibility for access to information classified at a lower level.

(b) Access to classified information relating to a special access program shall be granted in accordance with procedures established by the head of the agency that created the program or, for programs pertaining to intelligence activities (including special activities but not including military operational, strategic, and tactical programs) or intelligence sources and methods, by the Director of Central Intelligence. To the extent possible and consistent with the national security interests of the United States, such procedures shall be consistent with the standards and procedures established by and under this order.

Sec. 2.3 *Temporary Access to Higher Levels.* (a) An employee who has been determined to be eligible for access to classified information based on favorable adjudication of a completed investigation may be granted temporary access to a higher level where security personnel authorized by the agency head to make access eligibility determinations find that such access:

(1) is necessary to meet operational or contractual exigencies not expected to be of a recurring nature;

(2) will not exceed 180 days; and

(3) is limited to specific, identifiable information that is made the subject of a written access record.

(b) Where the access granted under subsection (a) of this section involves another agency's classified information, that agency must concur before access to its information is granted.

Sec. 2.4. *Reciprocal Acceptance of Access Eligibility Determinations.* (a) Except when an agency has substantial information indicating that an employee may not satisfy the standards in section 3.1 of this order, background investi-gations and eligibility determinations conducted under this order shall be mutually and reciprocally accepted by all agencies.

(b) Except where there is substantial information indicating that the employee may not satisfy the standards in section 3.1 of this order, an employee with existing access to a special access program shall not be denied eligibility for access to another special access program at the same sensitivity level as determined personally by the agency head or deputy agency head, or have an existing access eligibility readjudicated, so long as the employee has a need for access to the information involved.

(c) This section shall not preclude agency heads from establishing additional, but not duplicative, investigative or adjudicative procedures for a special access program or for candidates for detail or assignment to their agencies, where such procedures are required in exceptional circumstances to protect the national security.

(d) Where temporary eligibility for access is granted under sections 2.3 or 3.3 of this order or where the determination of eligibility for access is conditional, the fact of such temporary or conditional access shall be conveyed to any other agency that considers affording the employee access to its information.

Sec. 2.5. *Specific Access Requirement.* (a) Employees who have been determined to be eligible for access to classified information shall be given access to classified information only where there is a need-to-know that information.

(b) It is the responsibility of employees who are authorized holders of classified information to verify that a prospective recipient's eligibility for access has been granted by an authorized agency official and to ensure that a need-to-know exists prior to allowing such access, and to challenge requests for access that do not appear well-founded.

Sec. 2.6. *Access by Non-United States Citizens.* (a) Where there are compelling reasons in furtherance of an agency mission, immigrant alien and foreign national employees who possess a special expertise may, in the discretion of the agency, be granted limited access to classified information only for specific programs, projects, contracts, licenses, certificates, or grants for which there is a need for access. Such individuals shall not be eligible for access to any greater level of classified information than the United States Govern-ment has determined may be releasable to the country of which the subject is currently a citizen, and such limited access may be approved only if the prior 10 years of the subject's life can be appropriately investigated. If there are any doubts concerning granting access, additional lawful investigative procedures shall be fully pursued.

(b) Exceptions to these requirements may be permitted only by the agency head or the senior agency official designated under section 6.1 of this order to further substantial national security interests.

PART 3—ACCESS ELIGIBILITY STANDARDS

Sec. 3.1. *Standards.* (a) No employee shall be deemed to be eligible for access to classified information merely by reason of Federal service or con-

tracting, licensee, certificate holder, or grantee status, or as a matter of right or privilege, or as a result of any particular title, rank, position, or affiliation.

(b) Except as provided in sections 2.6 and 3.3 of this order, eligibility for access to classified information shall be granted only to employees who are United States citizens for whom an appropriate investigation has been completed and whose personal and professional history affirmatively indicates loyalty to the United States, strength of character, trustworthiness, honesty, reliability, discretion, and sound judgment, as well as freedom from conflicting allegiances and potential for coercion, and willingness and ability to abide by regulations governing the use, handling, and protection of classified information. A determination of eligibility for access to such information is a discretionary security decision based on judgments by appropriately trained adjudicative personnel. Eligibility shall be granted only where facts and circumstances indicate access to classified information is clearly consistent with the national security interests of the United States, and any doubt shall be resolved in favor of the national security.

(c) The United States Government does not discriminate on the basis of race, color, religion, sex, national origin, disability, or sexual orientation in granting access to classified information.

(d) In determining eligibility for access under this order, agencies may investigate and consider any matter that relates to the determination of whether access is clearly consistent with the interests of national security. No inference concerning the standards in this section may be raised solely on the basis of the sexual orientation of the employee.

(e) No negative inference concerning the standards in this section may be raised solely on the basis of mental health counseling. Such counseling can be a positive factor in eligibility determinations. However, mental health counseling, where relevant to the adjudication of access to classified information, may justify further inquiry to determine whether the standards of subsection (b) of this section are satisfied, and mental health may be considered where it directly relates to those standards.

(f) Not later than 180 days after the effective date of this order, the Security Policy Board shall develop a common set of adjudicative guidelines for determining eligibility for access to classified information, including access to special access programs.

Sec. 3.2. *Basis for Eligibility Approval.* (a) Eligibility determinations for access to classified information shall be based on information concerning the applicant or employee that is acquired through the investigation conducted pursuant to this order or otherwise available to security officials and shall be made part of the applicant's or employee's security record. Applicants or employees shall be required to provide relevant information pertaining to their background and character for use in investigating and adjudicating their eligibility for access.

(b) Not later than 180 days after the effective date of this order, the Security Policy Board shall develop a common set of investigative standards for background investigations for access to classified information. These standards may vary for the various levels of access.

(c) Nothing in this order shall prohibit an agency from utilizing any lawful investigative procedure in addition to the investigative requirements set forth in this order and its implementing regulations to resolve issues that may arise during the course of a background investigation or reinvestigation.

Sec. 3.3. *Special Circumstances.* (a) In exceptional circumstances where official functions must be performed prior to the completion of the investigative and adjudication process, temporary eligibility for access to classified information may be granted to an employee while the initial investigation is underway. When such eligibility is granted, the initial investigation shall be expedited.

(1) Temporary eligibility for access under this section shall include a justification, and the employee must be notified in writing that further access is expressly conditioned on the favorable completion of the investigation and issuance of an access eligibility approval. Access will be immediately terminated, along with any assignment requiring an access eligibility approval, if such approval is not granted.

(2) Temporary eligibility for access may be granted only by security personnel authorized by the agency head to make access eligibility determinations and shall be based on minimum investigative standards developed by the Security Policy Board not later than 180 days after the effective date of this order.

(3) Temporary eligibility for access may be granted only to particular, identified categories of classified information necessary to perform the lawful and authorized functions that are the basis for the granting of temporary access.

(b) Nothing in subsection (a) shall be construed as altering the authority of an agency head to waive requirements for granting access to classified information pursuant to statutory authority.

(c) Where access has been terminated under section 2.1(b)(4) of this order and a new need for access arises, access eligibility up to the same level shall be reapproved without further investigation as to employees who were determined to be eligible based on a favorable adjudication of an investigation completed within the prior 5 years, provided they have remained employed by the same employer during the period in question, the employee certifies in writing that there has been no change in the relevant information provided by the employee for the last background investigation, and there is no information that would tend to indicate the employee may no longer satisfy the standards established by this order for access to classified information.

(d) Access eligibility shall be reapproved for individuals who were determined to be eligible based on a favorable adjudication of an investigation completed within the prior 5 years and who have been retired or otherwise separated from United States Government employment for not more than 2 years; provided there is no indication the individual may no longer satisfy the standards of this order, the individual certifies in writing that there has been no change in the relevant information provided by the individual for the last background investigation, and an appropriate record check reveals no unfavorable information.

Sec. 3.4. *Reinvestigation Requirements.* (a) Because circumstances and characteristics may change dramatically over time and thereby alter the eligibility of employees for continued access to classified information, reinvestigations shall be conducted with the same priority and care as initial investigations.

(b) Employees who are eligible for access to classified information shall be the subject of periodic reinvestigations and may also be reinvestigated if, at any time, there is reason to believe that they may no longer meet the standards for access established in this order.

(c) Not later than 180 days after the effective date of this order, the Security Policy Board shall develop a common set of reinvestigative standards, including the frequency of reinvestigations.

PART 4—INVESTIGATIONS FOR FOREIGN GOVERNMENTS

Sec. 4. *Authority.* Agencies that conduct background investigations, including the Federal Bureau of Investigation and the Department of State, are authorized to conduct personnel security investigations in the United States when requested by a foreign government as part of its own personnel security program and with the consent of the individual.

PART 5—REVIEW OF ACCESS DETERMINATIONS

Sec. 5.1. *Determinations of Need for Access.* A determination under section 2.1(b)(4) of this order that an employee does not have, or no longer has, a need for access is a discretionary determination and shall be conclusive.

Sec. 5.2. *Review Proceedings for Denials or Revocations of Eligibility for Access.* (a) Applicants and employees who are determined to not meet the standards for access to classified information established in section 3.1 of this order shall be:

(1) provided as comprehensive and detailed a written explanation of the basis for that conclusion as the national security interests of the United States and other applicable law permit;

(2) provided within 30 days, upon request and to the extent the documents would be provided if requested under the Freedom of Information Act (5 U.S.C. 552) or the Privacy Act (3 U.S.C. 552a), as applicable, any documents, records, and reports upon which a denial or revocation is based;

(3) informed of their right to be represented by counsel or other representative at their own expense; to request any documents, records, and reports as described in section 5.2(a)(2) upon which a denial or revocation is based; and to request the entire investigative file, as permitted by the national security and other applicable law, which, if requested, shall be promptly provided prior to the time set for a written reply;

(4) provided a reasonable opportunity to reply in writing to, and to request a review of, the determination;

(5) provided written notice of and reasons for the results of the review, the identity of the deciding authority, and written notice of the right to appeal;

(6) provided an opportunity to appeal in writing to a high level panel, appointed by the agency head, which shall be comprised of at least three members, two of whom shall be selected from outside the security field. Decisions of the panel shall be in writing, and final except as provided in subsection (b) of this section; and

(7) provided an opportunity to appear personally and to present relevant documents, materials, and information at some point in the process before an adjudicative or other authority, other than the investigating entity, as determined by the agency head. A written summary or recording of such appearance shall be made part of the applicant's or employee's security record, unless such appearance occurs in the presence of the appeals panel described in subsection (a)(6) of this section.

(b) Nothing in this section shall prohibit an agency head from personally exercising the appeal authority in subsection (a)(6) of this section based upon recommendations from an appeals panel. In such case, the decision of the agency head shall be final.

(c) Agency heads shall promulgate regulations to implement this section and, at their sole discretion and as resources and national security considerations permit, may provide additional review proceedings beyond those required by subsection (a) of this section. This section does not require additional proceedings, however, and creates no procedural or substantive rights.

(d) When the head of an agency or principal deputy personally certifies that a procedure set forth in this section cannot be made available in a particular case without damaging the national security interests of the United States by revealing classified information, the particular procedure shall not be made available. This certification shall be conclusive.

(e) This section shall not be deemed to limit or affect the responsibility and power of an agency head pursuant to any law or other Executive order to deny or terminate access to classified information in the interests

of national security. The power and responsibility to deny or terminate access to classified information pursuant to any law or other Executive order may be exercised only where the agency head determines that the procedures prescribed in subsection (a) of this section cannot be invoked in a manner that is consistent with national security. This determination shall be conclusive.

(f)(1) This section shall not be deemed to limit or affect the responsibility and power of an agency head to make determinations of suitability for employment.

(2) Nothing in this section shall require that an agency provide the procedures prescribed in subsection (a) of this section to an applicant where a conditional offer of employment is withdrawn for reasons of suitability or any other reason other than denial of eligibility for access to classified information.

(3) A suitability determination shall not be used for the purpose of denying an applicant or employee the review proceedings of this section where there has been a denial or revocation of eligibility for access to classified information.

PART 6—IMPLEMENTATION

Sec. 6.1. *Agency Implementing Responsibilities.* Heads of agencies that grant employees access to classified information shall: (a) designate a senior agency official to direct and administer the agency's personnel security program established by this order. All such programs shall include active oversight and continuing security education and awareness programs to ensure effective implementation of this order;

(b) cooperate, under the guidance of the Security Policy Board, with other agencies to achieve practical, consistent, and effective adjudicative training and guidelines; and

(c) conduct periodic evaluations of the agency's implementation and administration of this order, including the implementation of section 1.3(a) of this order. Copies of each report shall be provided to the Security Policy Board.

Sec. 6.2. *Employee Responsibilities.* (a) Employees who are granted eligibility for access to classified information shall:

(1) protect classified information in their custody from unauthorized disclosure;

(2) report all contacts with persons, including foreign nationals, who seek in any way to obtain unauthorized access to classified information;

(3) report all violations of security regulations to the appropriate security officials; and

(4) comply with all other security requirements set forth in this order and its implementing regulations.

(b) Employees are encouraged and expected to report any information that raises doubts as to whether another employee's continued eligibility for access to classified information is clearly consistent with the national security.

Sec. 6.3. *Security Policy Board Responsibilities and Implementation.* (a) With respect to actions taken by the Security Policy Board pursuant to sections 1.3(c), 3.1(f), 3.2(b), 3.3(a)(2), and 3.4(c) of this order, the Security Policy Board shall make recommendations to the President through the Assistant to the President for National Security Affairs for implementation.

(b) Any guidelines, standards, or procedures developed by the Security Policy Board pursuant to this order shall be consistent with those guidelines issued by the Federal Bureau of Investigation in March 1994 on Background Investigations Policy/Guidelines Regarding Sexual Orientation.

(c) In carrying out its responsibilities under this order, the Security Policy Board shall consult where appropriate with the Overseas Security Policy Board. In carrying out its responsibilities under section 1.3(c) of this order, the Security Policy Board shall obtain the concurrence of the Director of the Office of Management and Budget.

Sec. 6.4. *Sanctions.* Employees shall be subject to appropriate sanctions if they knowingly and willfully grant eligibility for, or allow access to, classified information in violation of this order or its implementing regulations. Sanctions may include reprimand, suspension without pay, removal, and other actions in accordance with applicable law and agency regulations.

PART 7—GENERAL PROVISIONS

Sec. 7.1. *Classified Information Procedures Act.* Nothing in this order is intended to alter the procedures established under the Classified Information Procedures Act (18 U.S.C. App. 1).

Sec. 7.2. *General.* (a) Information obtained by an agency under sections 1.2(e) or 1.3 of this order may not be disseminated outside the agency, except to:

(1) the agency employing the employee who is the subject of the records or information;

(2) the Department of Justice for law enforcement or counterintelligence purposes; or

(3) any agency if such information is clearly relevant to the authorized responsibilities of such agency.

(b) The Attorney General, at the request of the head of an agency, shall render an interpretation of this order with respect to any question arising in the course of its administration.

(c) No prior Executive orders are repealed by this order. To the extent that this order is inconsistent with any provision of any prior Executive order, this order shall control, except that this order shall not diminish or otherwise affect the requirements of Executive Order No. 10450, the denial and revocation procedures provided to individuals covered by Executive Order No. 10865, as amended, or access by historical researchers and former presidential appointees under Executive Order No. 12958 or any successor order.

(d) If any provision of this order or the application of such provision is held to be invalid, the remainder of this order shall not be affected.

(e) This Executive order is intended only to improve the internal management of the executive branch and is not intended to, and does not, create any right to administrative or judicial review, or any other right or benefit or trust responsibility, substantive or procedural, enforceable by a party against the United States, its agencies or instrumentalities, its officers or employees, or any other person.

(f) This order is effective immediately.

THE WHITE HOUSE,
August 2, 1995.

[FR Doc. 95-19654
Filed 8-4-95; 12:18 pm]
Billing code 3195-01-P

ATTACHMENT #5
LABOR HOUR BILLING INSTRUCTIONS

General: During performance and through final payment of this contract, the contractor is responsible for the accuracy and completeness of data within the Central Contractor Registration (CCR) database and for any liability resulting from the Government's reliance on inaccurate or incomplete CCR data.

The contractor shall prepare invoices/vouchers for reimbursement of costs in the manner and format described herein. FAILURE TO SUBMIT INVOICES/VOUCHERS IN ACCORDANCE WITH THESE INSTRUCTIONS WILL RESULT IN REJECTION OF THE INVOICE/VOUCHER AS IMPROPER.

Standard Forms: Claims shall be submitted on the payee's letterhead, invoice/voucher, or on the Government's Standard Form 1034, "Public Voucher for Purchases and Services Other than Personal," and Standard Form 1035, "Public Voucher for Purchases Other than Personal--Continuation Sheet."

Electronic Invoice/Voucher Submissions: The preferred method of submitting vouchers/invoices is electronically to the U.S. Department of the Interior's National Business Center, via email to: NRCPayments_NBCDenver@NBC.gov.

Hard-Copy Invoice/Voucher Submissions: If you submit a hard-copy of the invoice/voucher, a signed original and supporting documentation shall be submitted to the following address:

Department of the Interior
National Business Center
Attn: Fiscal Services Branch - D2770
7301 West Mansfield Avenue
Denver, CO 80235-2230

Purchase of Capital Property: *($50,000 or more with life of one year or longer)*

Contractors must report to the Contracting Officer, electronically, any capital property acquired with contract funds having an initial cost of $50,000 or more, in accordance with procedures set forth in NRC Management Directive (MD) 13.1, IV, C – "Reporting Requirements" (revised 2/16/2011).

Agency Payment Office: Payment will continue to be made by the office designated in the contract in Block 12 of the Standard Form 26, or Block 25 of the Standard Form 33, whichever is applicable.

Frequency: The contractor shall submit claims for reimbursement once each month, unless otherwise authorized by the Contracting Officer.

Format: Invoices/Vouchers shall be submitted in the format depicted on the attached sample form entitled "Invoice/Voucher for Purchases and Services Other Than Personal". Alternate formats are permissible only if they address all requirements of the Billing Instructions. The instructions for preparation and itemization of the invoice/voucher are included with the sample form.

Task Order Contracts: The contractor must submit a separate invoice/voucher for each individual task order with detailed cost information. This includes all applicable cost elements and other items discussed in paragraphs (a) through (q) of the attached instructions. In addition, the invoice/voucher must specify the contract number, and the NRC-assigned task/delivery order number.

Billing of Costs after Expiration of Contract: If costs are incurred during the contract period and claimed after the contract has expired, you must cite the period during which these costs were incurred. To be considered a proper expiration invoice/voucher, the contractor shall clearly mark it "EXPIRATION INVOICE" or "EXPIRATION VOUCHER".

Final invoices/vouchers shall be marked "FINAL INVOICE" or "FINAL VOUCHER".

Currency: Invoices/Vouchers must be expressed in U.S. Dollars.

INVOICE/VOUCHER FOR PURCHASES AND SERVICES OTHER THAN PERSONAL
(SAMPLE FORMAT - COVER SHEET)

1. Official Agency Billing Office

Department of the Interior
National Business Center
Attn: Fiscal Services Branch - D2770
7301 West Mansfield Avenue
Denver, CO 80235-2230

2. Invoice/Voucher Information

a. Payee's DUNS Number or DUNS+4. The Payee shall include the Payee's Data Universal Number (DUNS) or DUNS+4 number that identifies the Payee's name and address. The DUNS+4 number is the DUNS number plus a 4-character suffix that may be assigned at the discretion of the Payee to identify altemative Electronic Funds Transfer (EFT) accounts for the same parent concern.

b. Payee's Name and Address. Show the name of the Payee as it appears in the contract and its correct address. If the Payee assigns the proceeds of this contract as provided for in the assignment of claims terms of this contract, the Payee shall require as a condition of any such assignment, that the assignee shall register separately in the Central Contractor Registration (CCR) database at http://www.ccr.gov and shall be paid by EFT in accordance with the terms of this contract. See Federal Acquisition Regulation 52.232-33(g) Payment by Electronic Funds Transfer - Central Contractor Registration (October 2003).

c. Contract Number. Insert the NRC contract number (including Enterprise-wide Contract (EWC)), GSA Federal Supply Schedule (FSS), Governmentwide Agency Contract (GWAC) number, or Multiple Agency Contract (MAC) number, as applicable.

d. Task Order Number. Insert the task/delivery order number (If Applicable). **Do not include more than one task order per invoice or the invoice may be rejected as improper.**

e. Invoice/Voucher. The appropriate sequential number of the invoice/voucher, beginning with 001 should be designated. Contractors may also include an individual internal accounting number, if desired, in addition to the 3-digit sequential number.

f. Date of Invoice/Voucher. Insert the date the invoice/voucher is prepared.

g. Billing period. Insert the beginning and ending dates (day, month, year) of the period during which costs were incurred and for which reimbursement is requested.

h. Labor Hours Expended. Provide a general summary description of the services performed and associated labor hours utilized during the invoice period. Specify the Contract Line Item Number (CLIN) or SubCLIN, as applicable, and information pertaining to the contract's labor categories/positions, and corresponding authorized hours.

i. Property. For contractor acquired property, list each item with an initial acquisition cost of $50,000 or more and provide: (1) an item description, (2) manufacturer, (3) model number, (4) serial number, (5) acquisition cost, (6) date of purchase, and (7) a copy of the purchasing document.

j. Shipping. Insert weight and zone of shipment, if shipped by parcel post.

k. Charges for freight or express shipments. Attach prepaid bill if shipped by freight or express.

l. Instructions. Include instructions to consignee to notify the Contracting Officer of receipt of shipment.

m. For Indefinite Delivery contracts, the final invoice/voucher shall be marked "FINAL INVOICE" or "FINAL VOUCHER".

n. Direct Costs. Insert the amount billed for the following cost elements, adjustments, suspensions, and total amounts, for both the current billing period and for the cumulative period (from contract inception to end date of this billing period).

(1) Direct (Burdened) Labor. This consists of salaries and wages paid (or accrued) for direct performance of the contract itemized, including a burden (or load) for indirect costs (i.e., fringe, overhead, General and Administrative, as applicable), and profit component, as follows:

Labor Category	Hours Billed	Burdened Hourly Rate	Total	Cumulative Hours Billed

(2) Contractor-acquired property ($50,000 or more). List each item costing $50,000 or more and having a life expectancy of more than one year. List only those items of equipment for which reimbursement is requested. For each such item, list the following (as applicable): (a) an item description, (b) manufacturer, (c) model number, (d) serial number, (e) acquisition cost, (f) date of purchase, and (g) a copy of the purchasing document.

(3) Contractor-acquired property (under $50,000), Materials, and Supplies. These are equipment other than that described in (2) above, plus consumable materials and supplies. List by category. List items valued at $1,000 or more separately. Provide the item number for each piece of equipment valued at $1,000 or more.

(4) Materials Handling Fee. Indirect costs allocated to direct materials in accordance the contractor's usual accounting procedures.

(5) Consultant Fee. The supporting information must include the name, hourly or daily rate of the consultant, and reference the NRC approval (if not specifically approved in the original contract).

(6) Travel. Total costs associated with each trip must be shown in the following format:

Start Date		Destination		Costs
From	To	From	To	$

(Must include separate detailed costs for airfare, per diem, and other transportation expenses. All costs must be adequately supported by copies of receipts or other documentation.)

(7) Subcontracts. Include separate detailed breakdown of all costs paid to approved subcontractors during the billing period.

o. Total Amount Billed. Insert columns for total amounts for the current and cumulative periods.

p. Adjustments. Insert columns for any adjustments, including outstanding suspensions for unsupported or unauthorized hours or costs, for the current and cumulative periods.

q. Grand Totals.

3. Sample Invoice/Voucher Information

Sample Invoice/Voucher Information (Supporting Documentation must be attached)

This invoice/voucher represents reimbursable costs for the billing period from____through____.

		Amount Billed Current Period	Amount Billed Cumulative
(a)	**Direct Costs**		
(1)	Direct burdened labor	$_____	$_____
(2)	Government property ($50,000 or more)	$_____	$_____
(3)	Government property, Materials, and Supplies (under $50,000 per item)	$_____	$_____
(4)	Materials Handling Fee	$_____	$_____
(5)	Consultants Fee	$_____	$_____
(6)	Travel	$_____	$_____
(7)	Subcontracts	$_____	$_____
	Total Direct Costs:	$_____	$_____
(b)	**Total Amount Billed**	$_____	$_____
(c)	**Adjustments** (+/-)	$_____	$_____
(d)	**Grand Total**	$_____	$_____

(The invoice/voucher format provided above must include information similar to that included below in the following to ensure accuracy and completeness.)

SAMPLE SUPPORTING INFORMATION

The budget information provided below is for format purposes only and is illustrative.

Cost Elements:

1) Direct Burdened Labor - $4,800

Labor Category	Hours Billed	Burdened Rate	Total	Cumulative Hours Billed
Senior Engineer I	100	$28.00	$2,800	975
Engineer	50	$20.00	$1,000	465
Computer Analyst	100	$10.00	$1,000	320
			$4,800	1,760 hrs.

Burdened labor rates must come directly from the contract.

2) Government-furnished and contractor-acquired property ($50,000 or more) - $60,000

Prototype Spectrometer - item number 1000-01 = $60,000

3) Government-furnished and contractor-acquired property (under $50,000), Materials, and Supplies - $2,000

10 Radon tubes @ $110.00	=	$1,100
6 Pairs Electrostatic gloves @ $150.00	=	$ 900
		$2,000

4) Materials Handling Fee - $40

(2% of $2,000 in item #3)

5) Consultants' Fee - $100

Dr. Carney - 1 hour fully-burdened @ $100 = $100

6) Travel - $2,640

(i) Airfare: (2 Roundtrip trips for 1 person @ $300 per r/t ticket)

Start Date	End Date	Days	From	To	Cost
4/1/2011	4/7/2011	7	Philadelphia, PA	Wash, D.C.	$300
7/1/2011	7/8/2011	8	Philadelphia, PA	Wash, D.C.	$300

(ii) Per Diem: $136/day x 15 days = $2,040

7) Subcontracting - $30,000

Company A	=	$10,000
Company B	=	$20,000
		$30,000

(EX: Subcontracts for Companies A & B were consented to by the Contracting Officer by letter dated 6/15/2011.)

Total Amount Billed	$99,580
Adjustments (+/-)	- 0
Grand Total	$99,580

4. Definitions

Material handling costs. When included as part of material costs, material handling costs shall include only costs clearly excluded from the labor-hour rate. Material handling costs may include all appropriate indirect costs allocated to direct materials in accordance with the contractor's usual accounting procedures.

NRC FORM 187 (7-2008) NRCMD 12

U.S. NUCLEAR REGULATORY COMMISSION

CONTRACT SECURITY AND/OR CLASSIFICATION REQUIREMENTS

AUTHORITY
The policies, procedures and criteria of the NRC Security Program, NRCMD 12, apply to performance of this contract, subcontract or other activity

COMPLETE CLASSIFIED ITEMS BY SEPARATE CORRESPONDENCE

1. CONTRACTOR NAME AND ADDRESS

Mental Health Evaluation Services
NRC, Division of Facilities and Security
Personnel Security Branch
Rockville, MD 20852

A. CONTRACT NUMBER FOR COMMERCIAL CONTRACTS OR JOB CODE FOR DOE PROJECTS (Prime contract number must be shown for all subcontracts.)

B. PROJECTED START DATE: 10/14/2012

C. PROJECTED COMPLETION DATE: 10/13/2017

2. TYPE OF SUBMISSION

A. ORIGINAL

√ B. REVISED (Supersedes all previous submissions)

C. OTHER (Specify)

3. FOR FOLLOW-ON CONTRACT, ENTER PRECEDING CONTRACT NUMBER AND PROJECTED COMPLETION DATE

A. DOES NOT APPLY

B. CONTRACT NUMBER: DR-10-06-426

DATE:

4. PROJECT TITLE AND OTHER IDENTIFYING INFORMATION

Mental Health Evaluation Services

The contractor shall conduct mental health evaluations, on an as needed basis, on U.S. NRC employees, consultants, contractors and licensee personnel. These evaluations will aid in resolving any security concerns in accordance with personnel security Adjudicative Guidelines and to include the diagnosis and treatment of mental, emotional, and personnel disorders and the subspecialty of alcohol abuse and addictions.

5. PERFORMANCE WILL REQUIRE

	NOT APPLICABLE	NATIONAL SECURITY		RESTRICTED DATA	
		SECRET	CONFIDENTIAL	SECRET	CONFIDENTIAL
A. ACCESS TO CLASSIFIED MATTER OR CLASSIFIED INFORMATION: √ YES (If "YES," answer 1-7 below) / NO (If "NO," proceed to 5.C.)					
1. ACCESS TO FOREIGN INTELLIGENCE INFORMATION	√				
2. RECEIPT, STORAGE, OR OTHER SAFEGUARDING OF CLASSIFIED MATTER. (See 5.B.)	√				
3. GENERATION OF CLASSIFIED MATTER.			√		
4. ACCESS TO CRYPTOGRAPHIC MATERIAL OR OTHER CLASSIFIED COMSEC INFORMATION	√				
5. ACCESS TO CLASSIFIED MATTER OR CLASSIFIED INFORMATION PROCESSED BY ANOTHER AGENCY			√		
6. CLASSIFIED USE OF AN INFORMATION TECHNOLOGY PROCESSING SYSTEM.	√		√		
7. OTHER (Specify)					

B. IS FACILITY CLEARANCE REQUIRED? YES √ NO

C. UNESCORTED ACCESS IS REQUIRED TO NUCLEAR POWER PLANTS

D. ACCESS IS REQUIRED TO UNCLASSIFIED SAFEGUARDS INFORMATION

E. √ ACCESS IS REQUIRED TO SENSITIVE IT SYSTEMS AND DATA.

F. √ UNESCORTED ACCESS TO NRC HEADQUARTERS BUILDING

G. REQUIRE OPERATION OF GOVERNMENT VEHICLES OR TRANSPORT PASSENGERS FOR THE NRC

H. WILL OPERATE HAZARDOUS EQUIPMENT AT NRC FACILITIES

I. REQUIRED TO CARRY FIREARMS

J. FOUND TO USE OR ADMIT TO USE OF ILLEGAL DRUGS

FOR PROCEDURES AND REQUIREMENTS ON PROVIDING TEMPORARY AND FINAL APPROVAL FOR UNESCORTED ACCESS, REFER TO NRCMD 12.

NOTE: IMMEDIATELY NOTIFY DRUG PROGRAM STAFF IF BOX 5 A, C, D, G, H, I, OR J IS CHECKED.

6. INFORMATION PERTAINING TO THESE REQUIREMENTS OR THIS PROJECT, EVEN THOUGH SUCH INFORMATION IS CONSIDERED UNCLASSIFIED, SHALL NOT BE RELEASED FOR DISSEMINATION EXCEPT AS APPROVED BY:

NAME AND TITLE	SIGNATURE	DATE
Janice E. Kelsh, Project Officer		

7. CLASSIFICATION GUIDANCE

NATURE OF CLASSIFIED GUIDANCE IDENTIFICATION OF CLASSIFICATION GUIDES

8. CLASSIFIED REVIEW OF CONTRACTOR / SUBCONTRACTOR REPORT(S) AND OTHER DOCUMENTS WILL BE CONDUCTED BY:

AUTHORIZED CLASSIFIER (Name and Title) | DIVISION OF FACILITIES AND SECURITY

9. REQUIRED DISTRIBUTION OF NRC FORM 187 *Check appropriate box(es)*

- √ SPONSORING NRC OFFICE OR DIVISION (Item 10A)
- √ DIVISION OF CONTRACTS AND PROPERTY MANAGEMENT
- √ DIVISION OF FACILITIES AND SECURITY (Item 10B)
- CONTRACTOR (Item 1)

SECURITY/CLASSIFICATION REQUIREMENTS FOR SUBCONTRACTS RESULTING FROM THIS CONTRACT WILL BE APPROVED BY THE OFFICIALS NAMED IN ITEMS 10B AND 10C BELOW

10. APPROVALS

SECURITY/CLASSIFICATION REQUIREMENTS FOR SUBCONTRACTS RESULTING FROM THIS CONTRACT WILL BE APPROVED BY THE OFFICIALS NAMED IN ITEMS 10B AND 10C BELOW.

NAME (Print or type)	SIGNATURE	DATE
A. DIRECTOR, OFFICE OR DIVISION	SIGNATURE	DATE
Mary Jane Ross-Lee, Director, DFS		
B. DIRECTOR, DIVISION OF FACILITIES AND SECURITY	SIGNATURE	DATE
Mary Jane Ross-Lee		
C. DIRECTOR, DIVISION OF CONTRACTS AND PROPERTY MANAGEMENT (Not applicable to DOE agreements)	SIGNATURE	DATE
~~James Corbett~~ James Leedom		4/16/12

REMARKS