

DEPARTMENT OF THE NAVY
COMMANDER, NAVY REGION SOUTH
CORPUS CHRISTI, TEXAS 78419-5200

CHIEF OF NAVAL AIR TRAINING
CORPUS CHRISTI, TEXAS 78419-5041

NRSINST 5230.3
CNATRINST 5230.4
N6

30 MAR 2004

NRS INSTRUCTION 5230.3
CNATRA INSTRUCTION 5230.4

Subj: CNATRA-NRS POLICIES AND GUIDELINES FOR FOREIGN NATIONAL
(FN) PERSONNEL USING DON INFORMATION SYSTEMS (IS)
RESOURCES OR PROVIDING SUPPORT TO DEPARTMENT OF THE NAVY
(DON) INFORMATION MANAGEMENT AND INFORMATION TECHNOLOGY
(IMIT)

Ref: (a) COMNAVNETWARCOM NORFOLK VA 191152Z AUG 03
(b) CJCSM 6510.01
(c) DODD 8500.1
(d) DODI 8500.2
(e) DODD 5230.20
(f) DODD 5160.54
(g) DOD 5200.1-R
(h) DOD 5200.2-R
(i) DODD 5200.2
(j) DOD 5220.22-M
(k) DODI 5200.40
(l) DOD 5025.1-M
(m) DODD 8000.1
(n) CNATRINST 5000.2A
(o) CNATRINST 5200.7
(p) SECNAVINST 5239.3
(q) SECNAVINST 5510.30A
(r) SECNAVINST 5510.36
(s) OPNAVINST 5239.1B
(t) SECNAVINST 4950.4A

Encl: (1) List of Web Links to References
(2) Non Disclosure Form for U.S. Government Sponsored
Contractors

1. Purpose

a. To provide policies and guidelines on Foreign National
(FN) personnel using DON Information Systems (IS) resources, or
providing contract support for the Chief of Naval Air Training
(CNATRA) - Navy Region South (NRS) and Naval Air Training Command
(NATRACOM) units.

30 March 2004

b. To define the organizational structure of the policies and guidelines.

c. To issue policies and guidelines necessary for consistent and effective implementation throughout CNATRA-NRS and NATRACOM.

d. To apply basic policies and principles of administrative guidelines as they relate to Information Management and Information Technology (IMIT) and Information Systems (IS) associated with and connected to the CNATRA-NRS and NATRACOM Networks.

2. Objective. To provide Command policies and guidelines for Foreign National user accounts on the unclassified Navy Marine Corps Intranet (NMCI) network at CNATRA-NRS and NATRACOM units and Foreign National contract personnel in support of the development, maintenance and programming support of legacy systems, under the purview of the Command Information Officer (CIO).

3. Authority. The CNATRA-NRS Command Information Officer (CIO) is responsible for ensuring compliance with DOD and DON Information Management and Information Technology (IMIT) policy and guidance for Information Systems (IS). Reference (n) identifies this authority. Reference (o) identifies Information Assurance (IA) Program for Information Security (INFOSEC) guidelines. Reference (c) provides specific guidelines for Information Assurance policies. Reference (d) provides Information Assurance implementation guidelines and policies. Reference (b) (For Official Use Only (FOUO)) manual provides additional interactive understanding between directives, instructions and guidelines. The policies, procedures and principles presented in references (a) through (t) apply to all personnel at CNATRA-NRS and NATRACOM military, Government civilian, (including Government contractors and International Military Training personnel) who use IMIT resources or provide support to Information Systems (IS) within CNATRA-NRS and NATRACOM units.

4. Policies. The term Foreign National (FN) refers to all individuals who are non-US citizens. The groups are as follows:

a. Foreign National International Military Training (IMT) personnel:

30 March 2004

(1) IMT Aviation Pilot training students are covered under reference (t), Joint Security Assistance Training (JSAT) and do not require user account access on the unclassified NMCI network.

(2) IMT Aviation Pilot personnel who have been assigned to CNATRA-NRS and NATRACOM as Foreign Liaison Officers, Foreign Exchange Coordinators, Cooperative Program personnel, or Instructor Pilots, will have their access requirements defined in the delegation of disclosure authority letter related to their assignment. A Common Access Card (CAC) will be provided to these personnel to access NMCI.

b. Foreign national DOD employees, foreign national service members, and DOD foreign national contractor personnel.

(1) The decision to authorize a user account access to the NMCI unclassified network or to maintain legacy-type systems, rests with the Command granting access and should be based on the foreign national duties, need for access, meeting DON Personnel Security Program requirements and DON Information Assurance and Security Program regulations. Refer to reference (a) of this instruction for NMCI user account formats. The following criteria must be met:

(a) The U.S. Government conducts investigations of personnel who are assigned to positions that directly or indirectly affect the operation of unclassified information management and information technology (IMIT) resources and information systems (IS) that process DOD information, to include For Official Use Only (FOUO), Privacy Act, DON proprietary and other controlled sensitive but unclassified information. A non-disclosure form must be signed by each contract employee at time of hiring and copy provided to employee and another kept at contractor's and U.S. Government COR/ACTR office files. Refer to enclosure (2) of this instruction for format(s).

(b) Requirements for these investigations are outlined in reference (h). Personnel occupying an IT Position shall be designated as filling one of the IT Position Categories listed below. The contractor shall include all of these requirements in any subcontracts involving IT support.

(c) The Contracting Officer's Representatives (COR) or the Activity Customer Technical Representative (ACTR) at the CIO office will determine if they or the contractor will assign

30 March 2004

the IT Position Category to contractor personnel and inform the contractor of their determination. If it is decided the contractor will make the assignment, the COR/ACTR will concur with the designation.

(d) Reference (c), paragraph 4.8 states "Access to all DOD information systems shall be based on a demonstrated need-to-know, and granted in accordance with applicable laws and DOD.5200.2R for background investigations, special access and IT position designations and requirements." references (h) and (i) require all persons assigned to sensitive positions or assigned to sensitive duties be U.S. citizens. All personnel assigned to IT-I and IT-II positions, as well as all persons with access to controlled unclassified information (without regard to degree of IT access) or performing other duties that are considered "sensitive" as defined in references (i) and (h) must be U.S. citizens. Furthermore, access by non-U.S. citizens to unclassified export controlled information is contained in reference (g).

(e) IT-I (High Risk). The responsibilities, not all-inclusive, are:

1. Responsibility or development and administration of Government computer security programs, including direction and control of risk analysis and/or threat assessment.

2. Significant involvement in life-critical or mission-critical systems.

3. Responsibility for the preparation or approval of data into a system, which does not necessarily involve personal access to the system, but with relatively high risk for effecting grave damage or realizing significant personal gain.

4. Relatively high risk assignments associated with or directly involving the accounting, disbursement, or authorization for disbursement from systems of (1) dollar amounts of \$10 million per year or greater, or (2) lesser amounts if the activities of the individual are not subject to technical review by higher authority in the IT-I category to ensure the integrity of the system.

5. Positions involving major responsibility for the direction, planning, design, testing, maintenance,

30 March 2004

operation, monitoring, and/or management of systems hardware and software.

6. Other positions as designated by DON that involve relatively high risk for effecting grave damage or realizing significant personal gain.

7. Personnel whose duties meet the criteria for IT-I Position designation require favorably adjudicated Single Scope Background Investigation (SSBI) or SSBI Periodic Reinvestigation (SSBI-PR). The SSBI or SSBI-PR shall be updated every 5 years. Personnel whose duties meet the criteria for an IT-I Position require a favorably adjudicated National Agency Check (NAC).

(f) IT-II Position (Moderate Risk). Responsibility for systems design, operation, testing, and/or monitoring that is carried out under technical review of higher authority in the IT-I category, include but is not limited to:

1. Access to and/or processing of proprietary data, information requiring protection under the Privacy Act of 1974, and Government-developed privileged information involving the award of contracts.

2. Accounting, disbursement, or authorization from system of dollar amounts less than \$10 million per year. Other positions are designated by DON that involve a degree of access to a system that creates a significant potential for damage or personal gain less than that in the IT-I Position. Personnel whose duties meet the criteria for an IT-II Position require a favorably adjudicated National Agency Check (NAC).

(g) IT-III Position (Low Risk). These are all other positions involving Federal IT activities.

1. Incumbents in this position have non-privileged access to one or more DOD information systems/applications or database to which they are authorized access.

2. Personnel whose duties meet the criteria for an IT-III Position designation require a favorably adjudicated National Agency Check (NAC).

3. Qualified cleared personnel do not require trustworthiness investigations. If an employee is in a position that **does not** require a personnel security clearance, do not

30 March 2004

submit a request for clearance, simply submit the Public Trust Position Application, Standard Form (SF) 85P, for trustworthiness determination. If an employee has already been granted a personnel security clearance at the appropriate level without a break in service for more than 24 months, such as in the case of IT-I Position, and has had a completed Personnel Security Investigation (a Single Scope Background Investigation-SSBI) less than 5 years old, there is no need to submit an additional investigation for the trustworthiness determination.

5. Guidelines and procedures for submitting U.S. Government Trustworthiness Investigations.

a. The contractor will ensure personnel designated IT-I, IT-II, or IT-III will complete either the hard copy Standard Form 85P (SF85P) or the online - electronic version of the SF85P (Electronic Personnel Security Questionnaire - EPSQ) version. Respective local Installation Personnel Security offices will assist in obtaining forms and how to complete the SF85P. In addition to the OPM SF85P form, contractor and contractor employee will fill out and sign the Non-Disclosure Form for U.S. Government Sponsored Contractors found at enclosure (2), forward the form to the ACTR, COR and CIO for approval/disapproval. Initial instructions completing SF85P are found below.

(1) The investigative request package for the SF85P is found at the Office of Personnel Management (OPM) web site (non-EPSQ) version and consists of the following:

- (a) Completed and Validated Error-free SF85P.
- (b) OPM Fingerprint Card FD 258.
- (c) Facility Security Officer's (FSO) portion of the SF85P.
- (d) Signed Privacy Act release (to include a signed Medical release, when applicable).

(2) In the "Your Employment Activities" block add the contract number requiring the Trustworthiness Investigation. Note: Do not complete a separate OPM coversheet if using this SF85P form. The SF85P is available from OPM at http://www.opm.gov/forms/pdf_fill/SF85P.pdf with additional assistance at <http://www.dss.mil>.

30 March 2004

(3) When using the electronic SF85P-EPSQ version, the submitted package shall include:

(a) A hard copy of the SF85P.

(b) All pertinent signed release forms.

(c) OPM Fingerprint Card FD 258.

(d) Employee's and Facility Security Officer's (FSO) validation certificates.

(e) An OPM coversheet signed and dated by the employee and FSO.

(4) In the "Your Employment Activities" block add the contract number requiring the Trustworthiness Investigation. The FSO is responsible for completing the OPM coversheet that is available for downloading with instructions at <http://www.opm.gov/extra/investigate/IS-15.pdf>. For item "J" on this coversheet, use your company's Submitting Office Number (SON). If this is not available, contact OPM-FIPC Program Services Office (PSO) to apply for a SON by calling (724) 794-5612 x-7501. For item "L" insert "N030". For item "N" enter "DSS-IND".

(5) The contractor shall review the SF85P for completeness and use reference (q), appendix G available at <http://neds.nebt.daps.mil/551030.htm> to determine if any adverse information is present. Only hard copy SF85P are acceptable by OPM-FIPC. Additional guidance for requesting investigations from OPM is found at <http://www.opm.gov/extra/investigate/IS-15.pdf>. Completed SF85P packages will be mailed to: The U.S. Office of Personnel Management (OPM) Federal Investigations Processing Center OPM-FIPC, P.O.Box 618, 1137 Branchton Road, Boyers, PA. 16018-0618. Note: All forms must be signed within 120 days of the date of submission to OPM. Submitted forms, which are not received within 120 days, will be delayed or returned. If no change has occurred, forms must be re-dated and initialed by the subject/employee.

(6) A favorable Background Investigation (BI) and National Agency Check (NAC) by OPM will determine trustworthiness. If individuals receive a negative trustworthiness determination, they will be immediately removed from their position of trust, the contractor will follow the employee termination processing below, and they will replace any

30 March 2004

individual who has received a negative trustworthiness determination.

(a) The contractor shall:

1. Immediately notify the COR/COTR of the employee's termination.

2. Send e-mail to respective COR/COTR.

3. FAX a termination Visit Authorization Letter (VAL) to COR/COTR.

4. Return any badge(s), vehicle decal, CAC, building access card to COR/COTR.

(7) Refer to Table E3.T1 of reference (d) for investigative levels for user with Information Assurance (IA) Management Access to DOD unclassified Information Systems for the following Information Technology (IT) Position Categories for handling unclassified but sensitive data, such as Privacy Act of 1974 with amendments, For Official Use Only (FOUO), personal privacy, unclassified technical data, DON proprietary data. IT Position Categories are:

(a) IT-I (Privileged) reserved for US citizens.

(b) IT-II (Limited Privileged) reserved for US citizens.

(c) IT-III (Non-Privileged) open to Foreign Nationals and U.S. citizens.

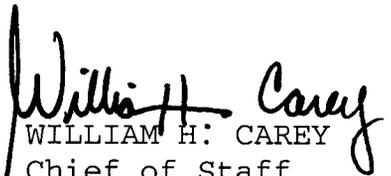
(8) Periodic reviews of work by contractors and unannounced checks will be performed by management to ascertain the quality of work within the network enclaves and the robustness of data are maintained in accordance with the IA parameters and security requirements.

(9) At no time, will contract employees transfer data from a Government computer into a media, copy proprietary data or onto personal laptop for work outside of the work area or to a home, unless authorized by the immediate Government supervisor/manager, in writing. Laptop will not contain a modem card for dialing out.

30 MAR 2004

6. Responsibility. CNATRA-NRS CIO is the official approval authority for Information Management and Information Technology (IMIT), which include operations and support of Information Systems (IS) for CNATRA-NRS and NATRACOM units. All support actions and documentations relative to Information Systems (IS) administration will be channeled and coordinated through the respective chain, the Contacting Officer Representative (COR), the Activity Customer Technical Representative (ACTR), then to the CNATRA-NRS CIO office. Unit Commanding Officers will implement these policies, administration, guidelines and procedures within their commands.

7. Information. Name, address, phone numbers and e-mail of CNATRA-NRS CIO: Mr. Thomas Albro, CNATRA-NRS CIO, Code N6, 250 Lexington Boulevard, Suite 265, Corpus Christi, TX 78419-5041, DSN 861-1430 or (361) 961-1430 and e-mail: thomas.albro@navy.mil.


WILLIAM H. CAREY
Chief of Staff

Distribution:

CNATRINST 5215.1R

List I

List III

NS Ingleside

NRS RBO

Copy to:

COMDRAWING TWO (Coop File)

NETC

30 March 2004

Web Links to References

COMNAVNETWARCOM MESSAGE NMCI INFORMATION BULLETIN
TWO CHARLIE (NIB 2C) FOREIGN NATIONAL ACCESS TO NMCI
19 AUG 2003



R 191152Z AUG 03
COMNAVNETWARC..

CJSCM 6510.01 is a FOUO document available at the INFOSEC web site.

DODD 8500.1

http://www.dtic.mil/whs/directives/corres/pdf/d85001_102402/d85001p.pdf

DODI 8500.2

http://www.dtic.mil/whs/directives/corres/pdf/i85002_020603/i85002p.pdf

DODD 5230.20

http://www.dtic.mil/whs/directives/corres/pdf/d523020_081298/d523020p.pdf

DODD 5160.54

http://www.dtic.mil/whs/directives/corres/pdf/d516054_012098/d516054p.pdf

DOD 5200.1-R

http://www.dtic.mil/whs/directives/corres/pdf/d52001_121396/d52001p.pdf

DOD 5200.2-R

http://www.dtic.mil/whs/directives/corres/pdf/52002r_0187/p52002r.pdf

DODD 5200.2

http://www.dtic.mil/whs/directives/corres/pdf/d52002_040999/d52002p.pdf

DOD 5220.22-M

http://www.dss.mil/isec/nispom_0195.htm

DODI 5200.40

(rev July 24, 2003) DITSCAP

<http://iase.disa.mil/ditscap/index.html>

Enclosure (1)

NRSINST 5230.3
CNATRAINST 5230.4

30 March 2004

DOD 5025.1-M

http://www.dtic.mil/whs/directives/corres/pdf/50251m_030503/p50251m.pdf

DODD 8000.1

http://www.dtic.mil/whs/directives/corres/pdf/d80001wch1_022702/d80001p.pdf

SECNAVINST 4950.4a

http://neds.nebt.daps.mil/Directives/4950_4a.pdf

CNATRAINST 5000.2A

<https://cnatra.navaltx.navy.mil/cnatra/folder2/5000.2A.pdf>

CNATRAINST 5200.7

<https://cnatra.navaltx.navy.mil/cnatra/folder2/5200.7.pdf>

SECNAVINST 5239.3

http://neds.nebt.daps.mil/Directives/5239_3.pdf

SECNAVINST 5510.30a

<http://neds.nebt.daps.mil/Directives/551030/551030a.pdf>

SECNAVINST 5510.36

http://neds.nebt.daps.mil/Directives/5510_36w.pdf

OPNAVINST 5239.1B

http://neds.nebt.daps.mil/Directives/5239_1b.pdf

30 March 2004

**NON-DISCLOSURE FORM FOR
U.S. GOVERNMENT SPONSORED CONTRACTORS**

Contractor completes blocks 1, 2 and 3, then provides copy to the ACTR for the U.S. Government COR to complete Block 4. CNATRA-NRS CIO completes Block 5, then returns to the ACTR. ACTR will fax or mail this complete form to contractor. **PLEASE TYPE OR PRINT CLEARLY.**

This is a Department of Defense (DOD) computer system. DOD computer systems are provided for the processing of official U.S. Government information only. All data contained on DOD computer systems is owned by the Department of Defense, may be monitored, intercepted, recorded, read, copied, or captured in any manner and disclosed in any manner, by authorized personnel. There is no right to privacy in this system. System personnel may give to law enforcement officials any potential evidence of crime found on DOD computer systems. Use of this system by any user, authorized or unauthorized, constitutes consent to this monitoring, interception, recording, reading, copying, or capturing and disclosure. Disclosure to unauthorized personnel of Privacy Act material, DON or Command proprietary data, copyrighted material or related to Aviation training may be prosecuted to the fullest extent of military and civil laws.

Block 1. COMPANY NAME AND MAILING ADDRESS of SUPPORT CONTRACTOR

MANAGER Name: _____

MANAGER Signature authorizing action and date:

Company Name: _____

Street Address/PO Box: _____

City/State/ZIP Code:

City/Country _____

Commercial Phone: _____ DSN: _____

FAX: _____ Email: _____

Contract Number: _____

LENGTH OF CONTRACT:

Start Date of contract:

30 March 2004

End Date of contract:

LEVEL OF ACCESS;

_____ Proprietary Information

_____ Unclassified but Sensitive Information

_____ Classified or Other (specify)

Block 2. User Information. This block must be filled and signed by the contractor employee requesting access.

As a support personnel for CNATRA-NRS/NATRACOM data systems, I acknowledge my responsibility to conform to the following requirements and conditions as established by CNATRA-NRS management:

I understand the need to protect the data, databases, reports, password(s) and user access. I will NOT share my password(s) and/or user account access.

I understand that I am responsible for all actions taken under my account. I will NOT attempt to "hack" the network or any connected information system or network, or attempt to gain access to data for which I am not specifically authorized.

I acknowledge my responsibility to comply with all Privacy Act, personal and proprietary data, copyright laws both federal and state (where applicable).

I understand my use of CNATRA-NRS/NATRACOM information systems is subject to monitoring to ensure proper functioning, to protect against improper or unauthorized use or access, and to verify the presence or performance of applicable security features or procedures. By using the information system I consent to such monitoring.

I acknowledge my responsibility to conform to the requirements stated above when using CNATRA-NRS/NATRACOM information systems or networks. I also acknowledge that failure to comply with these requirements and conditions may constitute a security violation resulting in denial of access to CNATRA-NRS/NATRACOM information systems, networks or facilities and that such violations will be reported to appropriate authorities for further action as deemed appropriate.

30 March 2004

I understand the need to protect the data, databases, reports, my password(s) and user account access. I will NOT share my password(s) and/or user account access. If I no longer need access to the CNATRA-NRS data or databases, it is my responsibility to notify my manager and the Government COR/ACTR.

USER SIGNATURE _____

Printed Name: _____

Social Security Number (last six digits):

Standard LOGON or User ID:

(Complete only if you currently have access to other CNATRA-NRS/NATRACOM systems and have been assigned this standard User ID)

Email:

Commercial Phone: _____ DSN: _____

Location/Office, employee is/will be assigned: _____

(See your supervisor for instruction sheet for Personal Password/Identification Information)

Contractor Employee will fill out Block 3.

Block 3. Employee Non-Disclosure Agreement Statement. This statement must be filled and signed by each contractor employee requesting access to the CNATRA-NRS/NATRACOM data and databases. Signed copy will be retained by contractor and respective ACTR.

**NON-DISCLOSURE AGREEMENT
FOR CNATRA-NRS / NATRACOM DATA AND DATABASES INFORMATION**

1. To carry out the duties in contract support using DOD and DON Information Systems (IS) resources for the Chief of Naval Air Training (CNATRA) - Navy Region South (NRS) and NATRACOM units, CNATRA-NRS CIO may disclose information to authorized representatives of the United States (U.S.) Government. This Non-Disclosure Agreement ("Agreement") covers information provided to the Department of Defense (DOD) under a mandate for federal contractors as described in 48 CFR, Parts 204, 212, and 252 and the Debt Collection Improvement Act of 1996, Public Law 104-134. The disclosure, of such information, to the public or

30 March 2004

outside of the Government shall be in accordance with all conditions and limitations set forth herein.

2. This Agreement is entered into between CNATRA-NRS and

(The Data Receiver). The Data Receiver has a requirement(s) for such data to perform certain tasks on behalf of the U.S. Federal Government. Because of this requirement(s), The Data Receiver is considered "authorized" for the purpose of this Agreement, after a favorable background investigation (BI) and favorable National Agency Check (NAC) for the employee named in Block 2. Block 1 request signifies that subject requirements of the BI and NAC have been initiated by contractor and forwarded to OPM for trustworthiness review and disposition. In the event results from the BI and NAC are not favorable, the employee's employment with contractor will be terminated.

3. CNATRA-NRS hereby determines that disclosure of information described in these paragraphs are necessary, so that The Data Receiver may perform the duties required of them by the U.S. Federal Government.

4. CNATRA-NRS shall grant access to information described hereon until such time as the information is no longer required for the performance of work on behalf of the U.S. Federal Government or the Data Receiver request termination of access or CNATRA-NRS terminates access.

5. The Data Receiver accepts the obligations contained in this Agreement in consideration of being granted access to the information described in paragraphs herein. The Data Receiver acknowledges that all obligations imposed by this agreement concerning the use and disclosure of such information apply for the duration of the requirement and at all times thereafter.

6. The Data Receiver agrees that it shall use the information described in these paragraphs only for the purpose of the work required by the U.S. Federal Government and shall not use such data for commercial purposes.

7. The Data Receiver agrees it shall not disclose or provide access to information described in these paragraphs to anyone unless it has verified that the recipient has been properly authorized by CNATRA-NRS management in writing to receive such information, e.g., employees of The Data Receiver contractor or contractors who have signed Employee/Subcontractor Non-Disclosure Agreements pursuant to this Agreement.

30 March 2004

8. The Data Receiver agrees to adopt operating procedures and physical security measures to properly safeguard such information from unauthorized use and from disclosure or release to unauthorized third parties.

9. The Data Receiver agrees to return to CNATRA-NRS/NATRACOM all copies of any abstracts or extracts of data described in paragraphs herein, of which it has possession pursuant to this Agreement, upon request of CNATRA-NRS or the completion or termination of the tasks set forth by the U.S. Federal Government, whichever comes first.

10. The Data Receiver agrees to obtain a written agreement to honor the terms of the Agreement from each contractor, sub-contractor and employee of the contractor or subcontractor who will have access to such information before the contractor, sub-contractor or employee is allowed such access.

11. The Data Receiver hereby acknowledges that no contractor, sub-contractor, consultant or employee who will have access to such information is debarred, suspended or otherwise ineligible to perform on a U.S. Federal Government contract.

12. The Data Receiver hereby acknowledges that any violation or breach of this Agreement on the part of a contractor, sub-contractor, consultant or any employee of a contractor or subcontractor shall constitute grounds for termination of access to such information; suit for damages; suit to enforce the Agreement, including but not limited to, application for a court order prohibiting disclosure or use of information in violation or breach of this Agreement; and or suit for civil fines or penalties. The Data Receiver further acknowledges that the unauthorized use, disclosure or retention of the information may constitute a violation of the U.S. criminal laws, including provisions of sections 641, 793, 794, and 1905, title 18 U. S. Code, and that nothing in this Agreement constitutes a waiver by the U. S. of the right to prosecute for any statutory violation.

13. Signature of acknowledging party:

Type or Print name: _____

Date of acknowledgement: _____

30 March 2004

Block 4. COR Sponsor Information - This block must be completed and signed by the U.S. Government Contracting Officer Representative (COR).

U.S. GOVERNMENT SPONSOR BRANCH OF SERVICE: _____
(Example: Army, Navy, Air Force, DLA, GSA, Marine Corps, FAA, VA, NASA).

MAJOR COMMAND: _____
(Example: Army Materiel Command, Air Force Materiel Command, Naval Supply Command, NAVAIR, NETC, etc.)

GOVERNMENT CONTRACT OFFICE REPRESENTATIVE (COR)
(By signing this block, you agree that the employee in Block 2, employed by the contractor named in Block 1, requires access to CNATRA-NRS/NATRACOM data and databases in support and performance of their contractual obligations at your agency.)

COR Signature: _____ Date _____

COR Name (print): _____

Office Symbol/Code/Mail Stop:

Organization: _____

Street/PO Box: _____

City/State/ZIP Code: _____

City/Country (If APO or FPO address):

Commercial Phone: _____ DSN: _____

Email Address: _____

FAX: _____

Block 5. Approval or Disapproval. TO BE COMPLETED BY CNATRA-NRS CIO.

DOD Federal Agency sponsored contractors requesting access to Government data or databases must be approved by the Command CIO:

30 March 2004

Mr. Thomas Albro, CNATRA-NRS CIO, Phone 361-961-1430 or DSN
861-1430. FAX 361-961-3217 e-mail: Thomas.albro@navy.mil

Non DOD Federal Agency sponsored contractors requesting access
to Government data or databases must be approved by the Command
CIO.

Please use information as above.

Signature of Approving Official:

_____ Date _____

Printed Name: _____

Title: _____

Commercial Phone: _____ DSN: _____

Disposition:

1 copy to ACTR

1 copy to be FAXed or mailed by ACTR to contractor