nearly 20 million persons with a hospital episode, 7 million with home-health episodes, and over 170 million with prescription drug use (397 million total). For the remaining four years of the five year period, we have estimated that one-quarter to three-quarters of patients without an encounter in the first year will enter the system.''

On page 60016 in the second column, the sentence starting on line five currently reads, ''The cost for this would be $0.75 over five years.'' This sentence should read, ''The cost for health plans to issue notice would be $0.75 over five years.''

On page 60017 in table 2, the cost of notice development for all entities in the initial or first year cost (2000) column should be 30,000,000 rather than 20,000,000.

On page 60018 in table 2, the total cost of the regulation in the initial or first year cost (2000) column should be $1,185,230,000 rather than $1,165,230,000.

On page 60024 in the first column, 5 currently says, ''Right to Restrict Uses and Disclosures.'' It should read, ''Right to Request Restrictions on Uses and Disclosures.''

On page 60024 in the second full paragraph in the second column, the sentence, ''Limiting the right to restrict to self-pay patients also would reduce the number of requests that would be made under this provision,'' should read, ''Limiting the right to request restrictions to self-pay patients also would reduce the number of requests that would be made under this provision.''

On page 60037 in the first paragraph of the first column, the sentence that currently reads, ''These small businesses represent 83.8% of all health entities we have examined,'' should read, ''These small businesses represent 84.9% of all health entities we have examined.''

On page 60039 in the second column, c. currently says, ''Right to restrict.'' It should read, ''Right to request restrictions on uses and disclosures.''

On page 60041 in the first column under ''i. Documentation requirements for covered entities,'' the sentence that currently reads, ''These areas would include use within the entity; informing business partners; disclosures with and without authorizations; limitations on use and disclosure for self-pay; inspection and copying; amendment or correction; accounting for uses and disclosure; notice development, maintenance, and dissemination; sanctions; and complaint procedures.,'' should read, ''These areas would include use within the entity; informing business partners; disclosures with and without authorization; inspection and copying; amendment or correction; accounting for disclosure; notice development, maintenance, and dissemination; sanctions; and complaint procedures.''

On page 60045 in the table summarizing the PRA burden hours, the line that says, ''§ 164.515 Accounting for uses and disclosures of protected health information,'' should read, ''§ 164.515 Accounting for disclosures of protected health information.''

On page 60046 column three the heading ''Section 164.515 Accounting for Uses and Disclosures of Protected Health Information'' should be changed to ''Section 164.515 Accounting for Disclosures of Protected Health Information.''

On page 60049 in the first column, the title **Appendix to the Preamble: Sample Contact of Provider Notice** should read **Appendix to the Preamble: Sample Content of Provider Notice.**

On page 60053 in the third column, under 164.506(a)(1), (i) currently reads, ''Except for research information unrelated to treatment, to carry out treatment, payment, or health care operations;.'' It should read, ''Except for research information unrelated to treatment and psychotherapy notes, to carry out treatment, payment, or health care operations;''

On page 60055 in the third column, (3)(iii) currently reads, ''A covered entity may not condition treatment, enrollment in a health plan, or payment on a requirement that the individual authorize use of disclosure of psychotherapy notes relating to the individual.'' It should read, ''A covered entity may not condition treatment, enrollment in a health plan, or payment on a requirement that the individual authorize use or disclosure of research information unrelated to treatment or psychotherapy notes relating to the individual.''

On page 60057 in the third column, the following should be deleted because it duplicates information in the second column:

(5) *Urgent circumstances.* The disclosure is of the protected health information of an individual who is or is suspected to be a victim of a crime, abuse, or other harm, if the law enforcement official represents that:

(i) Such information is needed to determine whether a violation of law by a person other than the victim has occurred; and

(ii) Immediate law enforcement activity that depends upon obtaining such information may be necessary.

Dated: December 27, 1999.

Brian P. Burns,

Deputy Assistant Secretary for Information Resources Management.

[FR Doc. 00–124 Filed 1–4–00; 8:45 am]

BILLING CODE 4150–04–M

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

48 CFR Parts 1804 and 1852

Security Requirements for Unclassified Information Technology Resources

AGENCY: National Aeronautics and Space Administration.

ACTION: Proposed rule.

SUMMARY: This is a proposed rule to amend the NASA FAR Supplement (NFS) to include a requirement for contractors and subcontractors working with NASA Information Technology Systems to take certain Information Technology (IT) security related actions, to document those actions, and submit related reports to NASA.

DATES: Comments should be submitted on or before March 6, 2000.

ADDRESSES: Interested parties should submit written comments to Karl Beisel, NASA Headquarters Office of Procurement, Analysis Division (Code HC), Washington, DC 20546. Comments may also be submitted by email to *Karl.Beisel@hq.nasa.gov.*

FOR FURTHER INFORMATION CONTACT: KARL BEISEL, 202–358–0416, EMAIL: KARL.BEISEL@HQ.NASA.GOV.

SUPPLEMENTARY INFORMATION:

A. Background

This revision to the NASA FAR Supplement will require NASA contractors and subcontractors to comply with the security requirements outlined in NASA Policy Directive (NPD) 2810.1, ''Security of Information Technology,'' and NASA Procedures and Guidelines (NPG) 2810.1, ''Security of Information Technology,'' and to comply with additional safeguarding requirements delineated in the proposed contract clause.

Currently NASA contractors have no definitive contractual requirement to follow NASA directed policy in safeguarding unclassified NASA data held via information technology (computer systems). This proposed rule establishes these requirements in a contract clause. The clause also requires compliance with additional safeguarding requirements. These policies apply to all IT systems and networks under NASA's purview

operated by or on behalf of the Federal Government, regardless of location.

B. Regulatory Flexibility Act

An initial Regulatory Flexibility Analysis has not been prepared because the proposed change is not expected to have a significant economic impact on a substantial number of small business entities. The proposed changes merely formalize standard procedures in using Government computer systems and databases. It is not expected that the proposed NFS changes will have an economic impact on small entities, nor is it expected that small entities will need to significantly revise internal procedures to satisfy the NFS changes. Comments from small business entities concerning the affected NASA FAR Supplement subparts will be considered in accordance with 5 U.S.C. 601. Such comments should be submitted separately and should cite 5 U.S.C 601, *et seq.*

C. Paperwork Reduction Act

An Office of Management and Budget (OMB) approval for data collection is being sought under 44 U.S.C. 3501, *et seq.*

List of Subjects in 48 CFR Parts 1804 and 1852

Government procurement.

Tom Luedtke,

Associate Administrator for Procurement.

Accordingly, 48 CFR parts 1804 and 1852 are proposed to be amended as follows:

1. The authority citation of 48 CFR parts 1804 and 1852 continue to read as follows:

Authority: 42 U.S.C. 2473(c)(1).

PART 1804—ADMINISTRATIVE MATTERS

2. Sections 1804.470–2, 1804.470–3, and 1804.470–4 are revised to read as follows:

1804.470–2 Policy.

(a) NASA policies and procedures on security for automated information technology are prescribed in NPD 2810.1, Security of Information Technology, and in NPG 2810.1, Security of Information Technology. Security requirements for safeguarding sensitive information contained in unclassified Federal computer systems are required in the following:

(1) All contracts for information technology resources or services. This includes, but is not limited to information technology hardware, software, and the management, operation, maintenance, programming, and system administration of information technology resources to include computer systems, networks, and telecommunications systems.

(2) Contracts under which contractor personnel must have physical or electronic access to NASA's sensitive information contained in unclassified systems or information technology services that directly support the mission of the Agency.

(b) NASA information processed, stored, or transmitted by contractor equipment does not give the contractor rights to use or to redistribute the information.

1804.470–3 Security plan for unclassified Federal Information Technology systems.

When considered appropriate for contract performance, the contracting officer, with the concurrence of the requiring activity and the Center IT Security Manager, may require the contractor to submit for post-award Government approval, a detailed Security Plan for Unclassified Federal Information Technology Systems. The plan shall be required as a contract data deliverable that will be subsequently incorporated into the contract as a compliance document after Government approval. The plan shall demonstrate thorough understanding of NPG 2810.1 and NPD 2810.1 and shall include, as a minimum, the security measures and program safeguards to ensure that the information technology resources acquired and used by contractor and subcontractor personnel—

(a) Are protected from unauthorized access, alteration, disclosure, or misuse of information processed, stored, or transmitted;

(b) Can maintain the continuity of automated information support for NASA missions, programs, and functions;

(c) Incorporate management, general, and application controls sufficient to provide cost-effective assurance of the systems' integrity and accuracy;

(d) Have appropriate technical, personnel, administrative, environmental, and access safeguards; and

(e) Document and follow a virus protection program for all IT resources under its control;

1804.470–4 Contract clauses.

The contracting officer shall insert the clause as stated at 1852.204–76, Security Requirements for Unclassified Information Technology Resources, in solicitations and contracts involving unclassified information technology resources.

PART 1852—SOLICITATION PROVISIONS AND CONTRACT CLAUSES

3. Section 1852.204–76 is revised to read as follows:

1852.204–76 Security Requirements for Unclassified Information Technology Resources.

As prescribed in 1804.470–4, insert the following clause:

Security Requirements for Unclassified Information Technology Resources (XXX)

(a) The Contractor shall comply with the security requirements outlined in NASA Policy Directive (NPD) 2810.1, ''Security of Information Technology,'' and NASA Procedures and Guidelines (NPG) 2810.1, ''Security of Information Technology''. These policies apply to all IT systems and networks under NASA's purview operated by or on behalf of the Federal Government, regardless of location.

(b)(1) The Contractor shall ensure compliance by its employees with Federal directives and guidelines that deal with IT Security including, but not limited to, OMB Circular A–130, ''Management of Federal Information Resources'', OMB Circular A–130 Appendix III, ''Security of Federal Automated Information Resources'', and the Computer Security Act of 1987 (40 U.S.C. 1441 *et seq.*).

(2) All Federally owned information is considered sensitive to some degree and must be appropriately protected by the Contractor as specified in applicable IT Security Plans. Types of sensitive information that may be found on NASA systems that the Contractor shall have access to include, but are not limited to—

(i) Privacy Act information (5 U.S.C. 552a *et seq.*);

(ii) Resources protected by the International Traffic in Arms Regulation (22 C.F.R Parts 120–130); and

(iii) National security information.

(3) The Contractor shall ensure that all systems connected to a NASA network or operated by the Contractor for NASA conform with NASA and Center security policies and procedures.

(c) In addition to complying with any functional and technical security requirements set forth in the schedule and the clauses of this contract, the Contractor shall initiate personnel screening checks for each contractor employee requiring unescorted or unsupervised physical or electronic access to restricted or limited areas, or privileged access to NASA systems, programs, and data.

(1) The Contractor shall ensure that all such employees have at least a National Agency Check investigation. The Contractor shall submit a personnel security questionnaire (NASA Form 531, Name Check Request for National Agency Check (NAC) investigation, and Standard Form 85P, Questionnaire for Public Trust Positions, (for specified sensitive positions), and a Fingerprint Card (FD–258 with NASA overprint in Origin Block) to the Center Chief of Security for each Contractor employee

who requires screening. The required forms may be obtained from Center Chief of Security. In the event that the NAC is not satisfactory, access shall not be granted. At the option of the Government, background screenings may not be required for employees with recent or current Federal Government investigative clearances.

(2) The Contractor shall have an employee checkout process that ensures—

(i) Return of badges, keys, electronic access devices and NASA equipment;

(ii) Notification to NASA within three working days for normal terminations and by the close of business for terminations for cause to disable any user accounts or network accesses that may have been granted to the employee; and

(iii) That the terminated employee has no continuing access to systems under the operation of the Contractor for NASA. Any access must be disabled the day the employee separates from the Contractor.

(3) Granting a non-permanent resident alien (foreign national) access to NASA IT resources requires special authorization. The Contractor shall obtain authorization from the Center Chief of Security prior to granting a non-permanent resident alien access to NASA IT systems and networks.

(d) The Contractor shall ensure that its employees with access to NASA information resources receive annual IT security awareness and training in NASA IT Security policies, procedures, computer ethics, and best practices.

(1) The Contractor shall employ an effective method for communicating to all its employees and assessing that they understand any ITS policies and guidance provided by the Center Information Technology Security Manager (CITSM) and/or Center CIO (CCIO) as part of the new employee briefing process. The Contractor shall ensure that all employees represent that they have read and understand any new ITS policy and guidance provided by the CITSM and CCIO over the duration of the contract.

(2) The Contractor shall ensure that its employees performing duties as system and network administrators in addition to performing routine maintenance possess specific IT security skills. These skills include the following:

(i) Utilizing software security tools.

(ii) Analyzing logging and audit data.

(iii) Responding and reporting to computer or network incidents.

(iv) Preserving electronic evidence.

(v) Recovering to a safe state of operation.

(3) The Contractor shall provide training to employees to whom they plan to assign system administrator roles. That training shall provide the employees with a full level of proficiency to meet all NASA system administrators' functional requirements. The contractor shall have methods or processes to document that employees have mastered the training material, or have the required knowledge and skills. This applies to all system administrator requirements.

(e) The Contractor shall promptly report to the Center IT Security Manager any suspected computer or network security incidents occurring on any system operated by the Contractor for NASA or connected to a NASA network. If it is validated that there is an incident, the Contractor shall provide access to the affected system(s) and system records to NASA and any NASA designated third party so that a detailed investigation can be conducted.

(f) The Contractor shall develop procedures and implementation plans that ensure that IT resources leaving the control of an assigned user (such as being reassigned, repaired, replaced, or excessed) has all NASA data and sensitive application software removed by a NASA-approved technique. NASA-owned applications acquired via a ''site license'' or ''server license'' shall be removed prior to the resources leaving NASA's use. Damaged IT storage media for which data recovery is not possible shall be degaussed or destroyed. If the assigned task is to be assumed by another duly authorized person, at the Government's option, the IT resources may remain intact for assignment and use of the new user.

(g) The Contractor shall afford NASA access to the Contractor's and subcontractor's facilities, installations, operations, documentation, databases and personnel to the extent required to carry out a program of IT inspection and audit to safeguard against threats and hazards to the integrity, availability and confidentiality of NASA data.

(h) The Contractor shall document all vulnerability testing and risk assessments conducted in accordance with NPG 2810.1 and any other current IT security requirements.

(1) The results of these tests shall be provided to the Center IT Security Manager. Any contractor system(s) connected to a NASA network or operated by the contractor for NASA may be subject to vulnerability assessment or penetration testing as part of the Center's IT security compliance assessment and the Contractor shall be required to assist in the completion of these activities.

(2) A decision to accept any residual risk shall be the responsibility of NASA. The Contractor shall notify the NASA system owner and the NASA data owner within 5 working days if new or unanticipated threats or hazards are discovered by the Contractor, made known to the Contractor, or if existing safeguards fail to function effectively. The Contractor shall make appropriate risk reduction recommendations to the NASA system owner and/or the NASA data owner and document the risk or modifications in the IT Security Plan.

(i) The Contractor shall develop a procedure to accomplish the recording and tracking of IT System Security Plans, IT system penetration and vulnerability tests for all NASA systems under its control or for systems outsourced to them to be managed on behalf of NASA. The Contractor must report the results of these actions directly to the Center IT Security Manager.

(j) When directed by the contracting officer, the contractor shall submit for NASA approval a post-award security implementation plan outlining how the contractor intends to meet the requirements of NPG 2810. The plan shall subsequently be incorporated into the contract as a compliance document after Government approval. The plan shall demonstrate thorough understanding of NPG 2810 and shall include as a minimum, the security measures and program safeguards to ensure that IT resources acquired and used by contractor and subcontractor personnel—

(1) Are protected from unauthorized access, alteration, disclosure, or misuse of information processed, stored, or transmitted;

(2) Can maintain the continuity of automated information support for NASA missions, programs, and functions;

(3) Incorporate management, general, and application controls sufficient to provide cost-effective assurance of the systems' integrity and accuracy;

(4) Have appropriate technical, personnel, administrative, environmental, and access safeguards; and

(5) Document and follow a virus protection program for all IT resources under its control.

(k) The Contractor shall incorporate this clause in all subcontracts where the requirements identified in this clause are applicable to the performance of the subcontract.

(End of clause)

[FR Doc. 00–181 Filed 1–4–00; 8:45 am]

BILLING CODE 7510–01–P

DEPARTMENT OF COMMERCE

National Oceanic and Atmospheric Administration

50 CFR Part 648

[Docket No. 991228354–9354–01; I.D. No. 111299C]

RIN 0648–AM49

Fisheries of the Northeastern United States; Atlantic Mackerel, Squid, and Butterfish Fisheries; 2000 Specifications

AGENCY: National Marine Fisheries Service (NMFS), National Oceanic and Atmospheric Administration (NOAA), Commerce.

ACTION: Proposed 2000 initial specifications; request for comments.

SUMMARY: NMFS proposes initial specifications for the 2000 fishing year for the Atlantic mackerel, squid, and butterfish (MSB) fisheries. This action also announces a proposed inseason adjustment to the 2000 mackerel joint venture processing (JVP) annual specifications, a proposal to allocate the domestic annual harvest (DAH) for *Loligo* squid into three 4-month periods, and a proposal to prohibit the use of any combination of mesh or liners that effectively decreases the mesh size below the minimum mesh size of 1⅞ in (48 mm). Regulations governing these fisheries require NMFS to publish specifications for the 2000 fishing year and management measures to assure