Attachment A: New 2011 FEHB Contract Security Clauses

Section 1.31 Definition of Information Security (JAN 2011)

As indicated in FAR Subpart 2.1, information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide —

1. Integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity; or destruction.

2. Confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and

3. Availability, which means ensuring timely and reliable access to, and use of, information.

Section 1.32 Carrier Personnel Security Requirements (JAN 2011)

(a) The U.S. Office of Management and Budget (OMB) Memorandum M-05-24, referenced in paragraph (a) of FAR 52.204-9, Personal Identity Verification of Contractor Personnel, is available on-line at http://www.whitehouse.gov/omb/memoranda/fy2005/m05-24.pdf.

(b) The minimum level of investigation required under Homeland Security Presidential Directive (HSPD) 12 is a National Agency Check with Written Inquiries (NACI), which will be requested on a Standard Form (SF) 85, "Questionnaire for Non-Sensitive Positions." The Government has determined that a Moderate Risk, Public Trust Background Investigation (MBI) is required for performance of this contract. Carriers with supervisory-type responsibilities require a High Risk, Public Trust (BI) Investigation. The Carrier must obtain these clearances. (OPM will not allow Carrier employees without clearance in any of its facilities, if applicable). The Carrier must obtain these clearances by using the e-QIP system. If satisfactory security arrangements cannot be made with the Carrier, the required services must be obtained from other sources.

(c) The level of classified access required will be indicated on DD-254 or other appropriate form incorporated into each request requiring access to classified information. Carriers are required to have background investigations for suitability if they occupy positions of trust (e.g., systems administration) even if they do NOT have access to classified information.

(d) Necessary facility and/or staff clearances must be in place.

(e) Carriers are responsible for the security, integrity and appropriate authorized use of their systems interfacing with the Government and or used for the transaction of any and all Government business. The Government, through the Government's Contracting Officer, may require the use or modification of security and/or secure communications technologies related to Government systems access and use.

(f) The Government, at its discretion, may suspend or terminate the access and/or use of any or all Government access and systems for conducting business with any/or all Carriers when a security or other electronic access, use or misuse issue gives cause for such action. The suspension or termination may last until such time as the Government determines that the situation has been corrected or no longer exists.

Section 1.33 Information Technology Systems Security (JAN 2011)

Carriers must comply with OPM IT Security and Privacy, NIST and OMB requirements for system users. Based upon the Federal Information Processing Standards Publication 199 (FIPS PUB 199), the Government has determined that a Level Moderate, applies to the sensitivity of the data contained in the Federal Automated Information System (AIS) and a Level Moderate, which applies to the operational criticality of the data processing capabilities of the AIS. (Note: FIPS PUB 199 is accessible on line at: http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf.)

Carriers must demonstrate that they comply with the end-user security requirements the Federal Information Security Management Act of 2002 (FISMA, Public Law 107-347, 44 U.S.C. 3531-3536); Office of Management and Budget (OMB) Circular A-130, Appendix III, "Security of Federal Automated Information Systems" and an acknowledgement of their understanding of the security requirements in the contract. (Note: OMB Circular A-130, Appendix III is accessible on line at: http://www.whitehouse.gov/omb/circulars/a130/appendix_iii.pdf.)

Section 1.34 Carrier Access to OPM IT Systems (JAN 2011)

Each Carrier employee is required to utilize individual identification and authorization to access OPM IT systems. Using shared accounts to access OPM IT systems is strictly prohibited. OPM will disable accounts and access to OPM IT systems will be revoked and denied if carriers share accounts. Users of the systems will be subject to periodic auditing to ensure compliance to OPM Security and Privacy Policy. In addition, Carriers are required to comply with the following NIST 800-53 security control to include at a minimum: Access Control (AC) - Controls falling under the AC category ensure that proper restrictions are in place to limit access to authorized users with a need to know.

The Carrier must:

(1) Provide to the OPM Letter of Credit (LOC) Security Officer listed in OPM's "Letter of Credit Drawdown System User Manual For Experience Rated Carriers" - Contacts for Questions and Problem Resolution, an initial and complete list of employees' names that require access to OPM information systems;

(2) By the fifth day of each month thereafter, send a staffing change report to the Contracting Officer's Representative, contract administrator and LOC Security Officer. The report must contain the listing of all staff members who left or were hired under this contract in the past 60 days. This form must be submitted even if no separation has occurred during this period. Failure to submit a 'Contractor Staffing Change Report' each month will result in the suspensions of all user IDs associated with this contract; and

(3) Anyone who accesses an OPM IT resource must complete OPM's IT Security and Privacy Awareness Training (ITPSA) annually and upon the initial access. This requirement applies to all Carriers.

Section 1.35 Procedures for Reporting a Security Breach (JAN 2011)

(1) A breach of data, system access, etc. includes loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or unauthorized access of information whether physical or electronic. As an agency, OPM is required to immediately report all potential security and data breaches -- whether they involve paper documents or electronic information. In order to meet this responsibility, OPM has established a new internal procedure for reporting the loss or possible compromise of any data, and this clause conforms to that procedure.

(2) OPM Carriers must report any breach or potential breach to the OPM Situation Room and the Contracting Officer within 30 minutes of becoming aware of the risk – regardless of the time or day of the week. Breaches should be reported, even if it is believed the breach is limited, small, or insignificant. OPM's IT security experts, who will determine when a breach needs additional focus and attention. The OPM Situation Room is available 24 hours per day, 365 days per year. Report the breach to the OPM Situation Room and the Contracting Officer either by phone or by e-mail; however, be sure NOT to include PII in the e-mail.

(1) OPM Carriers must report a breach or potential security breach to the OPM Situation Room at: sitroom@opm.gov, (202) 418-0111, Fax (202) 606-0624.

(2) When notifying the Situation Room, please copy the Contracting Officer.

(3) To get help with WinZip, please contact the OPM Help Desk at: helpdesk@opm.gov, (202) 606-4927, TTY (202) 606-1295.

(4) If you have questions regarding these procedures, contact the Contracting Officer.

Section 5.67 Personal Identity Verification of Contractor Personnel (SEP 2007) (FAR 52.204-9)

(a) The Contractor shall comply with agency personal identity verification procedures identified in the contract that implement Homeland Security Presidential Directive-12 (HSPD-12), Office of Management and Budget (OMB) guidance M-05-24 and Federal Information Processing Standards Publication (FIPS PUB) Number 201.

(b) The Contractor shall insert this clause in all subcontracts when the subcontractor is required to have routine physical access to a Federally-controlled facility and/or routine access to a Federally-controlled information system.

Section 5.68 Privacy or Security Safeguards (AUG 1996) (FAR 52.239-1)

(a) The Contractor shall not publish or disclose in any manner, without the Contracting Officer's written consent, the details of any safeguards either designed or developed by the Contractor under this contract or otherwise provided by the Government.

(b) To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of Government data, the Contractor shall afford the Government access to the Contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases.

(c) If new or unanticipated threats or hazards are discovered by either the Government or the Contractor, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party.