

Proposed Draft of New Security Contract Language Explanation

## Background

Currently, the Department has security verbiage clauses that state:

\*\*\*\*\*

### CPSS, 307-13, Department Security

The Contractor and its subcontractors shall comply with Department Security policy requirements as set forth in:

- A. The Statement of Work of this contract;
- B. The Privacy Act of 1974 (P.L. 93-579, U.S.C. 552a);
- C. The U.S. Department of Education, Information Technology Security Policy (October 2001); and
- D. The U.S. Department of Education, ACS Directive OM:5-101, Contractor Employee Personnel Security Screenings.

The Contractor may request copies of the above referenced documents by contacting the Contract Specialist at telephone number xxxxx or via e-mail at xxxxx.

The Contractor shall include this provision in any subcontract(s) awarded pursuant to this contract.

The referred documents can be viewed on the OICO website in ConnectEd.

\*\*\*\*\*

### 201-39.5202-5, PRIVACY OR SECURITY SAFEGUARDS (OCT 90 FIRMR)

(a) The details of any safeguards the contractor may design or develop under this contract are the property of the Government and shall not be published or disclosed in any manner without the contracting officer's express written consent.

(b) The details of any safeguards that may be revealed to the contractor by the Government in the course of performance under this contract shall not be published or disclosed in any manner without the contracting officer's express written consent.

(c) The Government shall be afforded full, free, and uninhibited access to all facilities, installations, technical capabilities, operations, documentation, records, and data bases for the purpose of carrying out a program of inspection to ensure continued efficacy and efficiency of safeguards against threats and hazards to data security, integrity, and confidentiality.

(d) 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. Mutual agreement shall then be reached on changes or corrections to existing safeguards or institution of new safeguards, with final determination of appropriateness being made by the Government. The Government's liability is limited to an equitable adjustment of cost for such changes or corrections, and the Government shall not be liable for

claims of loss of business, damage to reputation, or damages of any other kind arising from discovery of new or unanticipated threats or hazards, or any public or private disclosure thereof.

(End of clause)

\*\*\*\*\*  
^{201-39.1001-1} Security specifications.

Specifications for security of FIP resources shall include, as appropriate:

- (a) Agency rules of conduct that a contractor shall be required to follow.
- (b) A list of the anticipated threats and hazards that the contractor must guard against.
- (c) A description of the safeguards that the contractor must specifically provide.
- (d) The security standards applicable to the contract.
- (e) A description of the test methods, procedures, criteria, and inspection system necessary to verify and monitor the operation of the safeguards during contract performance and to discover and counter any new threats or hazards.
- (f) A description of the procedures for periodically assessing the security risks involved.
- (g) A description of the personnel security requirements.
- (h) Consistent with the guidelines for Federal computer security training issued by the National Institute of Standards and Technology (NIST) and regulations issued by the Office of Personnel Management (OPM), a description of the security training that the contractor is required to provide to its employees.
- (i) Consistent with the guidelines issued by the Office of Management and Budget (OMB) in OMB Bulletin 88-16, a description of the plan the contractor must develop or follow to provide for the security and privacy of FIP resources the contractor is required to operate.

\*\*\*\*\*

This language can be used in RFPs and contracts to describe the security requirements of the contractors.

While this is a good start for contract language, FSA would like to augment the language with additional verbiage.

Primarily, the security program has grown since CPSS 307-13 and the other clauses were created and this language does not adequately reflect the security requirements. FSA drafted new language that is more comprehensive than the existing language and will ensure security is appropriately covered in projects. The new language will better meet the security needs because it is more up to date, covers everything that is missing from the existing language, is more thorough, and also highlights the important aspects of security that contractors must be aware of. The draft language is based upon NIST and tailored for FSA, but could easily be modified for the Department of Education as a whole.

There are a number of gaps in the existing language that the new language addresses. First, the policy requirement noted in C, the Information Technology Security Policy, is outdated; the newest version is dated 6/10/2003. Also, there are new federal regulations

that contractors must adhere to that are not currently mentioned. This includes the E-Government Act, which is not mentioned in any of the documents in CPSS 307-13. There has been new NIST guidance that has been published that is not mentioned in any of the documents, for instance NIST 800-47. Contractors still need to follow this guidance. There have been changes within the Department's policies since the last version of 6/10/2003, such as the final draft of the Incident Handling/Response Procedures. According to the 6/10/2003 version of the IT Security Policy, that document is still in draft, however, the document has actually been finalized for many months. If the contractors went by CPSS 307-13 as is, then they probably would not have to comply with the Incident Response Procedures, which would not be in compliance with the Department. Finally, some of the language comes from the day-to-day experiences and recognizing what the language is lacking. One example of this is a recent issue that arose within the Department because a contractor did scans and then refused to turn over the scan results. There is a line in the new language that addresses this type of issue; stating, "The results of testing activities, such as scan results, are the property of the Department."

Essentially, the new draft language fills in existing gaps for security contracting language.

## **Current Status of Proposed Language**

FSA submitted a draft to their contracting specialists for review and made their changes. FSA contract specialists, in turn, submitted the language to the main Department for review. The Department asked FSA to review the language and remove any overlaps with the proposed language and the existing verbiage. FSA has made the changes.

In the proposed language, there are sections that are in italics, which represent optional language or comments. The comments would, naturally, not go in the actual contracts, they are meant for guidance purposes. Also, some of the italicized sections represent suggested language that FSA would like to further discuss with the Department and decide which language is most appropriate.

FSA is going to work with the Department Information Assurance Office to have the proposed language turned into an ACS Directive. Then, the FSA contracting specialists can add a line item to contracts which would encompass the security requirements and not take up a large amount of space within the contracts.