FREDERIC G. ANTOUN, JR.
ATTORNEY AT LAW
14 NORTH MAIN STREET, SUITE 406
CHAMBERSBURG PA 17201-1814

717-261-0998
Fax: 717-263-7328
website: http://www.printlaw.com email: antoun@printlaw.com

May 14, 2007

TO: Publication and Government Information Security Group
IMPORTANT UPDATE
FROM: Fred Antoun

The group was formed as a PIA GPIC group at the direction of then-Chairman Mike Burrows. Members included government agency representatives and several GPO vendors. The purpose of the group was to examine the government's methodology of handling the various categories (over 100 as of the beginning of this year) of Official Use (FOUO) or sensitive but not classified materials that the publishing agency or publishing subgroup felt should not be in the hands of the general public.

PIA had received questions and what can honestly be called complaints about the government's failure to include security requirements in printing and CD-ROM specifications issued by the U.S. Government Printing Office (GPO). The group held several meetings, and Minutes were produced. The bottom line was that agency publishers did not always seem to understand the security requirements for the documents they were turning over to agency print procurement departments, the print procurement departments did not have the authority (or, some felt, the "duty") to create a set of security requirements, and finally, the GPO felt it would be exceeding its role and statutory authority to review a document or publication and decide it should not be generally distributed, and impose security restrictions in the specifications.

GPO is still the gateway through which agency publications and information pass on their way to private sector contractors, and it is critical to maintaining security. An underlying problem is that under U.S. law, unless a government publication is classified or copyrighted (usually as a result of inclusion of some protected private sector content) there is nothing to keep someone from reproducing the material and selling it or giving it away.

As a result, information that should not reach the general public, let alone terrorist groups, was being made available not only on the internet, but also through eBay for sale.

The Group began to formulate a policy that would include many of the security requirements contained in the classified materials production guidelines, and suggest that GPO include an option to utilize these security requirements in their ordering forms, so

that agencies could more easily protect sensitive but unclassified, FOUO, and other publications.

As the project progressed, it became obvious that it was simply too big a task to deal with each agency. As a result, we worked with Homeland Security, the Homeland Security Committees, and other governmental agencies that had a broad, government-wide scope. Since the rules (and amendments thereto) regarding classification of materials have generally been promulgated through Executive Order, the possibility of only dealing with one branch of the government (run by "the decider") seemed like it might provide the best methodology of actually getting something done. Nevertheless, the Homeland Security Committees in the House and Senate have been actively involved in trying to understand this problem and potential resolutions.

Although other agencies and office in the executive branch were involved, the primary impetus for addressing the security problem came from the Office of the Director for National Intelligence. For more than a year, that office has been working to understand the ways in which agencies are attempting to protect sensitive and FOUO materials, and gather together the number of different names and designations that various agencies have given to these materials. We have interfaced with that office, as well as the Information Security Oversight Office (ISOO) in an effort to make sure that the Executive Branch and intelligence related agencies that are reviewing this issue understand that:

1. Government information is printed, published, duplicated, replicated, etc. primarily through the Government Printing Office.
2. The Government Printing Office handles the production of most of the classified materials.
3. Very few GPO specifications (notably IRS and Social Security) have security requirements for sensitive but not classified or FOUO materials, primarily because the ordering Agency does not provide them, and because no uniform standards exist.
4. Printer contractors are aware of the fact that there are no security requirements on publications and materials that they receive which everyone knows should have some type of security requirements for subcontracting prepress off-shore, the production of the work, the maintenance of the privacy of the information, destruction of leftover materials, handling of digital materials, etc., etc.
5. GPO is in a particularly good position to provide agencies with the option of using check block security designation once the security systems are established.
6. GPO would not decide if a publication should have production security, but simply give the agency publishers or agency print procurement staff an easy and efficient way to require basic security to insure that everyone in the process was a part of the security solution, not the security problem.

The Director for National Intelligence has developed a designation for materials that are in the area of sensitive but not classified, and FOUO, and has cut down the number of designations that will be permitted to be used. In addition, they may establish security requirements for the government and private sector contractors in the handling of these materials. Their recommendations have been sent to the White House, and are currently being reviewed. The expectation is that they will be approved (perhaps with some modifications) and will be adopted as an Executive Order, hopefully this year.

At that time, GPO will need to incorporate those requirements (in the check block type methodology we have been discussing) and publish the list of requirements in their specifications or as additions to their boilerplate Contract Terms, so that there is no doubt that everyone knows what the security requirements are. In the meantime, we will ask GPO to adopt some interim requirements to protect the security of sensitive, but unclassified, FOUO, and similarly designated documents and materials that pass through or to GPO and its private sector contractors.

In addition, we have asked GPO to develop a system for requiring a security plan from vendors, so that the GPO and its agency customers will have the benefit of knowing that the contractor didn't just say "yeah, no problem – I'll do that security stuff." A security plan reviewed by GPO would provide good assurance that the contractor actually has both the ability and a working plan to effectuate the security requirements. This would be of extreme value to not only the contractors and the agencies, but also to the security of the United States.

One outgrowth of the recognition that there is a serious publication security problem will certainly be a more careful review by agencies as to whether or not materials should be classified, and an attendant increase in classification to the lowest of the three classified levels (Confidential). It seems reasonable that publications dealing with things like the technical specifications for the Apache helicopter, surveillance and equipment training manuals for the Transportation Security Agency employees, Border Patrol enforcement methods and procedures, and terrorist surveillance methodologies, etc., could be classified as Confidential under the current Executive Order amendment.

Should you have any questions, or feel that there is a need for a meeting of the work group, please don't hesitate to contact me.

FGA/mhw