Terrorism and Trafficking - Grant and Contract Provisions

Author: COGR

We have reported on the introduction of language in grant awards from the Ford, Rockefeller and Sloan Foundations prohibiting the promotion of or engagement in violence, terrorism, bigotry or the destruction of any state. All of these new provisions that place prohibitions on terrorist financing, restrictions on nonimmigrant or foreign national participation in research, or, in the case of the CDC described below, US government opposition to prostitution and related activities, require a particular diligence on the part of universities.

Published Date: 08/26/2004

GRANT AND CONTRACT PROVISIONS ON TERRORISM AND TRAFFICKING

We have reported on the introduction of language in grant awards from the Ford, Rockefeller and Sloan Foundations prohibiting the promotion of or engagement in violence, terrorism, bigotry or the destruction of any state. All of these new provisions that place prohibitions on terrorist financing, restrictions on nonimmigrant or foreign national participation in research, or, in the case of the CDC described below, US government opposition to prostitution and related activities, require a particular diligence on the part of universities. Some will require a simple affirmation of institutional compliance; others as noted require flow-down and monitoring of sub-receipients. The non-profit foundations' restrictions on all university funds pose particularly difficult challenges to academic freedom.

PRIVATE FOUNDATIONS

In April, 2004, nine university provosts, asked the Ford and Rockefeller Foundations to modify their grant provisions by narrowing the scope of the prohibition to only those funds provided by the Foundations, in order to avoid conflicts with the protection of free academic speech on campuses.

These restrictions on the use of funds have been motivated in part as a response to Executive Order (EO) 13224 of September 23, 2001. This Order prohibits transactions in funds, goods, or services with persons or entities that commit, threaten to commit or support terrorism including state sponsors of terrorism. The Executive Order includes an annexed list of prohibited individuals and organizations like Al Qaida and the Taliban and the list as been amended with additional names since the Order was signed in 2001.

The foundations have been reluctant to modify the new prohibitions in their award letters but have accepted, in some cases, university statements affirming compliance with EO 13224 in the use of the foundation's funds. Examples of this type of statement are: "The Grantee agrees that it will use the grant funds in compliance with all applicable anti-terrorist financing and asset control laws and regulations" or "in compliance with Executive Order 13224 of September 23, 2001 as amended."

To add the list of private foundations requiring compliance with anti-terrorism laws and regulations, the MacArthur Foundation asks recipients to represent and warrant that Foundation funds will not be spent to support persons or entities on any Federal exclusion list. Some universities have accepted the provision because the restriction is limited to Foundation funds (unlike the Ford and Rockefeller) and requires compliance with applicable laws. As in negotiations with some of the other Foundations, universities have been successful in deleting the provisions but MacArthur has indicated the provision will remain as one of the conditions of its awards. Universities will want to continue to monitor these private foundation grants and determine what approach best reflects the university's perspective.

Federal Agencies

COGR has been monitoring changes in Federal regulations or policies directed toward compliance with various security and anti-terrorism laws, notably the National Science Foundation's (NSF) implementation of the Cyber Security Research and Development Act grant provisions and the National Institutes of Health (NIH) contract provisions requiring compliance with the agency's Information Systems Security program.

NSF Cyber Security Implementation

The National Science Foundation (NSF) implemented the Cyber Security Research and Development Act by establishing new grant conditions focused on the review of employee and student immigration status, including restrictions on aliens from named countries, and setting up reporting and record-keeping requirements. COGR representatives had met with NSF staff to discuss how to demonstrate compliance with these new grant conditions and in April, 2004, COGR sent a letter to Amy Northcutt, NSF Deputy General Counsel, outlining a general university interpretation for meeting the new requirements.

On May 12, 2004, NSF issued a notice describing the Implications of the Cyber Security Research and Development Act on NSF research and training programs. The notice is available at: https://www.ehr.nsf.gov/ehr/cyber_security_act.html. As described, use of this special language should make it easier for institutions to comply with NSF's requirements.

Beginning with FY 2004, NSF will add special language to selected research and training awards made by the Directorates for in the Computer and Information Science and Engineering (CISE) and Education and Human Resources (EHR). Grantees will be required to ensure that no grant funds go to an individual in violation of his/her immigration status or an alien from country determined to be a state sponsor of international terrorism unless that person has a visa permitting them to enter and remain in the US. Grantee institutions will be required to report to NSF any suspension or termination of their ability to receive nonimmigrant students or exchange visitors.

NIH Information Systems Security

Some member institutions received a requirement in NIH contracts and RFPs for compliance with provisions of the DHHS Handbook for an Information Systems Security Program. The Handbook sets forth six levels of position sensitivity. Depending on the level of sensitivity of the information, this may require government background checks for faculty and other university personnel involved in the contract as well as other compliance requirements such as training programs. NIH has applied the requirement to a wide range of information system activities, including contracts involving establishment of websites for information on particular diseases and databases on clinical medical research. Universities have taken the position with previous requirements of this

nature (i.e. NASA) that universities will conduct appropriate background checks consistent with university policy, but have resisted government performance of background checks on their faculty and staff.

COGR contacted NIH to express concern that the requirement is being applied to a range of activities beyond delivery of automated information systems to the government, where we might agree that the requirements of OMB Circular A-130 (the basis for the DHHS Handbook) should apply. In a November 2003 message from NIH's Director of Acquisition Policy, NIH explained the background of the Automated Information Systems Security Program (AISSP) and indicated that NIH will determine AISSP applicability based on operational criticality and sensitivity levels of the automated information system involved in the contract.

COGR agreed that whether a contractor designed information system is a "federal automated information system" may not be entirely limited to cases where the information is "delivered" to the government noting situations where the government has a duty to operate a database and may contract with a private party to design and deliver the software/hardware to the government so that the government can perform the function. Alternately, a contract to design a website, where the government would then mount and maintain the website as a ".gov site," might be another example where the AISSP might properly apply. However, cases where the government is providing support to a group of researchers to collect clinical data and maintain them in a database for other researchers are a different matter. In such cases the information system and/or database being generated are to further the research objectives. They are not intended for delivery to the government nor does the government intend to maintain the database as a "federal automated information system."

In response, COGR received an electronic message in December2003 from NIH's acquisition policy office. The message noted that NIH is committed to safeguarding information developed or accessed by federal employees and contractor personnel. The message acknowledged the validity of the concerns expressed by COGR and indicated that NIH is developing additional internal policy and guidance to address these issues.

At a February 2004 meeting, the NIH procurement analysts informed COGR that any database generated by a university under an NIH contract that is "delivered" to the government is considered to be a "Federal Automated Information System" (FAIS) and hence subject to the requirement. The DHHS Information Systems Security Program implements the Computer Security Act of 1987. In response to questions as to why DHHS/NIH has only now begun to include the provisions in contracts, OAMP indicated that it was due to "heightened concerns" about information security. DHHS/OAMP believe where NIH is contracting for a database, NIH is responsible for assuring the integrity of the data. The background check requirement will apply to any individual who develops the database and/or is capable of manipulating the data in the database. The NIH Project Officer will be responsible for determining the applicability of the requirements to a particular contract, in consultation with the contracting officer. New NIH solicitations will identify applicability of the requirements; however, NIH is

considering reviewing existing contracts to determine if they need to be modified to make the requirements applicable. More information about the information security program requirements is contained in the NIH Center for Information Technology web site (http://www.cit.nih.gov/home.asp).

COGR cautioned the OAMP representatives that overbroad application of these requirements to university faculty and staff would have major implications for universities, especially if they are extended to existing contracts. Issues include the nature of the personal information required to be submitted, who performs the background checks, where the database is maintained, whether retroactive application is subject to the contracts dispute process, etc. COGR urged NIH to consult with other agencies such as NASA and NIST who also have considered application of federal information systems security standards to universities. However, it appears likely that NIH will continue to apply the FAIS requirements to university contracts.

USAID Anti-Terrorism Certification

The US Agency for International Development (USAID) issued a revised policy directive in March 2004 that began appearing in assistance agreements in June. The Acquisition and Assistance Policy Directive (AAPD) 04-07 clarifies the language of its Terrorist Financing certification and describes the grantee's liability with regard to terrorist financing. USAID usually provides support to universities for project or demonstration activities rather than basic or applied research and, consistent with USAID's mission, these activities almost always include work done in foreign countries with some of the USAID funds spent in-country.

A USAID requirement for anti-terrorism certification has been in place since December 2002 and implements EO 13224 – the same Executive Order that serves as the basis for the non-profit foundations' provisions. This revised directive makes clear that certification requires the recipient to verify that it has not, does not and will not knowingly provide support or resources to individuals and entities on the US Department of Treasury's Office of Foreign Assets Control (OFAC) Specially Designated Nationals and Blocked Persons master list, the United Nation Security Council 1267 (sanctions) Committee list, or any one that the recipient has knowledge or information about drawn from public sources like the news media. The recipient is expected to implement reasonable monitoring and oversight procedures to ensure USAID funds are not directly or indirectly supporting these individuals. The recipient is liable for the actions of its subrecipients.

CDC Prohibition on Prostitution and Sex Trafficking

A Centers for Disease Control (CDC) grant agreement clause places additional restrictions on foreign subrecipients. Like the USAID program, the requirement appeared in a project-based grant and, in this case, prohibits the use of CDC funds to promote or advocate the legalization or practice of prostitution or sex trafficking. The restriction does not include providing palliative care, treatment or post exposure

commodities, e.g., drugs, test kits, etc. There are additional exclusions in the requirement but it does require that any information about the use of condoms shall be medically accurate and include information on the public health benefit and failure rates of condom use.

The clause must flow-down in any sub-agreements and foreign sub recipients must have a policy explicitly opposing prostitution and sex trafficking. The language for the very simple the recipient and sub-recipient certification is included. Any violation by the prime or subrecipient is grounds for termination of the agreement and the refund of the entire amount furnished by the agreement.

This CDC "Prostitution and Related Activities" provision does not provide a statement of authority but it clearly is linked to US Code Title 28, Chapter 78, Trafficking Victims Protection, a result of the passage of PL 106-386 in 2000. The Act was reauthorized in 2003 by PL 108-193, Trafficking Victims Protection Reauthorization Act, which included the provisions for termination of assistance agreements.

The USAID and CDC clauses raise specific challenges for programs conducted in whole or in part in a foreign country. Universities will want to assess their financial management and monitoring mechanisms, particularly in country, to ensure continued compliance with the certification.