ON TARGET NEWSLETTER

A newsletter covering industrial security issues.

Volume 1, Issue 2 June , 2007

In this issue:

ON TARGET NEWSLETTER
A security newsletter for MSU
Not approved for public release
Submit comments and questions to:
Neil E. Lewis, 5-8682

Balancing security and academic freedom

By Graham B. Spanier

A few months after Sept. 11, 2001, a few visitors stopped by my office in the heart of Penn State's University Park campus. My administrative assistant was a bit nervous when she told me, with raised eyebrows, that two gentlemen from the Federal Bureau of Investigation wanted to see me.

If special agents of the FBI pop in for a visit, you can be pretty sure they aren't there to congratulate you on your stellar class of incoming students. Needless to say, they were there on official business.

In fact, in the aftermath of Sept. 11, communications with federal security agencies have become more common for college and university administrators as we collectively deal with issues such as terrorism, cyber-security intrusions, immigration policy and visa regulations, deemed exports, handling of chemical and biological agents and classified or sensitive research.

While our country struggles to strengthen homeland security, we in academe are especially attuned to the matter of balance: the balance between our government's duty to provide for the security of our nation and higher education's historical commitment to academic freedom and openness, our long-standing open door policy with scholars from around the world and our strong inclination toward civil rights.

Colleges and universities in particular have fostered a climate of free inquiry and discovery. As a core ingredient of American higher education, the free marketplace of ideas has led to vast technological breakthroughs and new discoveries that have translated into tremendous progress for our nation.

In fact, the research conducted at American universities has played a significant role in ensuring our nation's security.

Historically there has been a certain level of distrust between universities and the nation's defense, law enforcement and intelligence establishment. New regulations have intensified those feelings as many academics fear that an overly restrictive atmosphere will lead to cultural isolation and the loss of our worldwide pre-

eminence in critical areas of science and innovation.

These are reasonable concerns. That is why a new advisory board was formed last year to open the doors of communication between higher education and the nation's national security, law enforcement and intelligence communities.

In an unprecedented move, the FBI has taken the lead on behalf of other partner government agencies to establish The National Security Higher Education Advisory Board. Consisting of presidents and chancellors of 17 prominent U.S. universities, the board is expected to foster outreach and promote understanding, as well as develop opportunities through research, education and public-service collaboration to further aid our nation's security interests.

As chair of this advisory board, I have seen a remarkable and productive dialogue begin to flourish in the first year of our work.

Through the National Security Higher Education Advisory Board, we are generating meaningful discussion on a broad range of issues including the importance of international students and scholars; immigration policy; implications of the Patriot Act; the dissemination of research data; export policy; security of information networks; our leadership in science and technology; and the best use of the extraordinary talent found in our universities to mitigate any new security threats.

This advisory board is creating a cross-fertilization of ideas that can only come from informed and ongoing discourse.

Finding the proper balance between national security mandates and the fundamental values underlying higher education is critical to U.S. leadership, economic strength and productivity, as well as the potential of our universities.

Higher education has a critical role to play in the national security of a free society. In fact, we were part of an exciting announcement with the launch of a new International Center for the Study of Terrorism dedicated to reducing the global threat of terrorism and minimizing its impact on society by an international alliance of leading universities. Led by Penn State, researchers from the United States, United Kingdom, Europe and People's Republic of China will investigate the root causes of this worldwide phenomenon, understand its long-term effects on society and identify new ways of safeguarding individuals, organizations and communities.

The National Security Higher Education Advisory Board promises to help universities and government work toward a balanced and rational approach that will allow science and education to progress and our nation to remain safe.

****

Graham B. Spanier is president of Penn State and chairman of the National Security Higher Education Advisory Board.

The other members of the National Security Higher Education Advisory are:

William Brody, President, Johns Hopkins University
Albert Carnesale, Chancellor, University of California, Los Angeles
Jared Cohon, President, Carnegie Mellon University
Marye Ann Fox, Chancellor, University of California, San Diego
Robert Gates, President, Texas A&M University
Gregory Geoffroy, President, Iowa State University

Amy Gutmann, President, University of Pennsylvania
David C. Hardesty Jr., President, West Virginia University
Susan Hockfield, President, Massachusetts Institute of Technology
Martin Jischke, President, Purdue University
Bernard Machen, President, University of Florida
James Moeser, Chancellor, University of North Carolina, Chapel Hill
C.D. Mote, President, University of Maryland, College Park
John Wiley, Chancellor, University of Wisconsin, Madison
Mark Emmert, President, University of Washington

****

FOUO – What is it?

FOUO or For Official Use Only is a document designation and not a classification. This designation can cause a lot of harm due to the fact that personnel are not aware of what FOUO really signifies, and the protection it must afforded. FOUO is used by the Department of Defense (DoD) and some other agencies to identify information or material which, although, unclassified, may not be appropriate for public release.

There is no national policy governing the FOUO designation. DoD Directive 5400.7 defines For Official Use Only information as "unclassified information that may be exempt from mandatory release to the public under the Freedom of Information Act (FOIA)". The policy is implemented by DoD Regulation 5400.7-R and 5200.1-R.

FOUO is also used by the CIA and a number of other federal agencies, but each is responsible for determining how it should be used. The categories of protected information may be quite different from one agency to another, although in every case the protected information must be covered by one of the nine categories of information that are exempt from public release under FOIA.

The public has a right to information concerning the activities of its government. The Freedom of Information Act or FOIA requires all Federal Agencies to conduct their activities in an open manner and to have a system for providing the public with the maximum of accurate and timely information allowed by law. Agencies commonly have a FOIA office for processing public requests for information.

The FOIA allows nine exemptions from this mandatory release policy. The purpose of the exemptions is to preclude the unauthorized disclosure of information that requires protection. These exemption categories reflect laws, executive orders, regulations, or court decisions that either require or permit protection of certain classes of information.

DoD regulation 5200.1-R appendix C describes the nine FOIA exemptions as:

1. Information which is currently and properly classified.
2. Information that pertains solely to the internal rules and practices of the agency. (This exemption has two profiles "high" and "low". The "high" profile permits withholding of a document that, if released, would allow circumvention of an agency rule, policy or statue thereby impeding the agency in the conduct of its mission. The "low" profile permits withholding if there is no public interest in the document, and it would be an administrative burden to process the request.)
3. Information specifically exempted by statue particular criteria for withholding. The language of the statue must clearly state that the information will not be disclosed.
4. Information such as trade secrets and commercial or financial information obtained from a company on a privileged or confidential basis that, if released, would result in competitive harm to the company, impair the government's ability to obtain like information in the future or to protect

the government's interest in compliance with program effectiveness. (This opens the door to an article on the Economic Espionage Act of 1996 and Proprietary Information & Trade Secrets, which will addressed in a future issue.)

5. Inter-agency memoranda that are deliberative in nature; this exemption is appropriate for internal documents that are part of the decision making process and contain subjective evaluations, opinions and recommendations.
6. Information the release of which could reasonably be expected to constitute a clearly unwarranted invasion of the personal privacy of individuals.
7. Records or information complied for law enforcement purposes that (a) could reasonably be expected to interfere with law enforcement proceedings; (b) would deprive a person of a right to a fair trail or impartial adjudication; (c) could reasonably be expected to constitute an unwarranted invasion of the personal privacy of others; (d) disclose the identity of a confidential source; (e) disclose investigative techniques or procedures; (f) could reasonably be expected to endanger the life or physical security of any individual.
8. Certain records of agencies responsible for the supervision of financial institutions.
9. Geological and geophysical information concerning wells.

With the above said just because information says it is FOUO does not mean it is automatically exempt from public release under the FOIA. If a request is received for information it must meet the FOIA dual test: (1) Does it fit into one of the nine exemption categories, and (2) Is there a legitimate government purpose for withholding the information. On the other hand, the absence of FOUO or other marking does not automatically mean the information must be released in response to a FOIA request.

Each government agency defines what information should be protected and how it is protected. DoD FOUO may be disseminated within DoD components and between officials of the DoD components and DoD contractors, consultants and grantees as necessary in the conduct of official business.

How are FOUO documents marked?

- FOUO documents will be marked FOR OFFICIAL USE ONLY at the bottom of the front cover (if there is one), the title page (if there is one), the first page and the outside back cover (if there is one).
- Pages of the document that contain FOUO information shall be marked FOR OFFICIAL USE ONLY at the bottom.
- Each paragraph containing FOUO information shall be marked with the abbreviation FOUO in parentheses at the beginning of the FOUO portion
- Material other than paper documents (for example slides, computer media, films, etc.) shall bear markings which alert the holder that the material contains FOUO information.
- FOUO documents and material transmitted outside of the DoD must bear expanded marking on the face of the document so that non-DoD holders understand the status of the information. Use of a statement similar to:

This document contains information exempt from mandatory disclosure under the FOIA. Exemption(s)___ apply.

Safeguarding FOUO

FOUO information should be handled in a manner that provides reasonable assurance that unauthorized persons do not gain access.

During working hours, reasonable steps should be taken to minimize risk of access by unauthorized personnel. After working hours, FOUO may be stored as a minimum in unlocked containers, desks or cabinets if government or government-contract building security is provided. If government or government-contract building security is not provided, it must be stored at a minimum in a locked desk, file cabinet, bookcase, locked room, or similar place.

FOUO documents and material may be transmitted via first class mail, parcel post, or -- for bulk shipments -- fourth class mail.

Fax or e-mail transmission of FOUO information (voice, data or facsimile) should be by encrypted communications systems whenever practical. FOUO information may be put on an Internet web site only if access to the site is limited to a specific target audience and the information is encrypted.

DoD Technical Information, For Official Use Only information, export-controlled information, Unclassified Nuclear Information, and Privacy Act information may not be posted on an unencrypted web site. Decisions on the handling of proprietary or trade secret information in the private sector are made by the owners of that information.

DoD guidelines also require that judgments about the sensitivity of information take into account the potential consequences of "aggregation." The term "sensitive by aggregation" refers to the fact that information on one site may seem unimportant, but when combined with information from other web sites it may form a larger and more complete picture that was neither intended nor desired. In other words, the combination of information from multiple web sites may amount to more than the sum of its parts. Similarly, the compilation of a large amount of information together on one site may increase the sensitivity of that information and make it more likely that site will be accessed by those seeking information that can be used against us.

FOUO documents may be destroyed by shredding or tearing into pieces and discarding the pieces in a regular trash container unless circumstances suggest a need for more careful protection.

For additional information concerning FOUO guidelines please contact your FSO.

♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦

ASK SECURITY:

Q: Do I have to advise and obtain permission from the FSO for any foreign travel?

A: The only personnel required to advise and obtain permission for foreign travel are those with special access program (SAP) and special compartmented access clearances (SCI). You will know if you have such a clearance.

However, you are to report any suspicious contacts that occur during your travel to the FSO.

Also it is a good idea to keep the FSO informed of any foreign travel you plan to take. The FSO has access to databases, Department of State/Diplomatic Security, FBI, etc., that has information on travel alerts, conditions and warnings.

****

Security is a team effort!

One State, One Team.