# ON TARGET NEWSLETTER

*A newsletter covering industrial security issues.*

Volume 1, Issue 3 October, 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, telephone 5-8682,
E-mail nelewis@fso.msstate.edu

## Security Debriefing

A security debriefing is essentially a reiteration of your responsibilities to safeguard classified information. However, it is completed when you no longer have a requirement for a clearance. Reasons for the debriefing are employment separation for whatever purpose, the project on which you were working is completed, you are transferred to another project that has no clearance requirement, or maybe some other dreadful reason.

When your security clearance was granted, you made a contract between yourself and the U.S. Government (USG). This contract also known as the Non Disclosure Agreement or SF 312 contained a lot of government jargon and legalese about how bad it would be if you ever divulged classified info. The SF-312 contained two important phases, one is that you agree to never divulge classified information, and the second is, unless released in writing by an authorized representative of the USG all conditions and obligations imposed by signing the SF-312 apply during the time you were granted access to classified information and at all times thereafter. The important words are "never divulge" and "at all times thereafter", this is a lifelong commitment. Unless of course someone happens to give that release in writing, please don't hold your breath waiting for this one to happen. Consequently even when you leave Mississippi State University for retirement, to take another position, whatever the reason, you have the responsibility to protect and not divulge the information to which you had access, as it could cause harm to the Unites States, your former co-workers and friends.

You have an obligation to never divulge any classified information to which you had access; you also have a second obligation. That is to inform the FSO in a timely manner when you no longer have the need for a clearance. Yes the FSO will probably do a clearance review once a year, but this does not always catch everyone, especially if someone left employment between the clearance reviews.

Once a clearance is removed, it can easily be reinstated within a period of 2 years. A clearance never really expires; it is the background investigation on which the clearance is based that has the time limit.

If after you have had your clearance removed or you have moved on, there is ever a question regarding what you can do, say, or if you feel someone is asking too many questions about what you used to do, you can always call the FSO at your former facility for assistance and guidance. This information should be provided to you as part of the debriefing.

**********

# Information Security: A Difficult Balance

## Dr. Linwood H. Rose

Protecting the critical infrastructure of our country is essential to the preservation of our lives as we now live them. My personal interest in this area began somewhat serendipitously, following a meeting with one of our faculty members at James Madison University (JMU). I was intrigued with the work he was conducting on information security. The subject seemed like a natural fit for our new College of Integrated Science and Technology.

So I became a "champion" for our efforts in information assurance. I learned what I could, but perhaps most important, I provided encouragement, some additional resources, and visibility for the program. I began to envision that JMU might play a significant role in the nation's efforts against cyber-terrorism when, in January 2000, I stood in the White House Rose Garden as President Bill Clinton signed the "National Plan for Information Systems Protection: An Invitation to Dialogue." Then came the tragic events for September 11, which still haunt us all. JMU lost several talented alumni on that day, and I know the same can be said for many institutions.

Though the 9/11 attack was a physical assault, it was at least partially attributable to imperfections in security systems. In addition, cyber-attacks occur every day. These attacks, not necessarily from terrorists, are designed to detect system vulnerabilities, to acquire or destroy information, and to delay access. Clearly, as scholars, researchers, and educators, those of us in higher education have a key role to play in helping to promote a secure environment for our businesses, our government, our public institutions, and our families.

As a university president, I have awakened to a new reality. The time has come for leaders in higher education to recognize and creatively respond to the opportunity and realities of protecting the national critical infrastructure. To do this effectively, the academy must embrace and implement a vision that is truly interdisciplinary in program development, balances basic research with applied research and integrates this vision into the curriculum, facilitates technology transfer, is engaged through strategic alliances and collaborative efforts, and balances public interest/national security with individual rights.

Leaders model the way. When my father, a bogey golfer, taught me to play the game, he often said: "Do as I say, not as I do." That won't work in information security. Leaders must have credibility, and that comes from first taking care of business at home. We must all become much more vigilant in the provision of secure systems, in intrusion detection, in rapid response, and especially in education. We must practice, teach, and infuse all aspects of security into our campus lives. The goal is to go beyond reasonable policy and precaution and to assist students and others in the development of what are now essential life skills. We must challenge faculty to move from gaining simple literacy about information assurance to understanding and communicating the necessity and use of information assurance in student's personal and professional lives.

Information security is no longer a fields of study isolated to the computer science department. The need for understanding and study information of information security is pervasive across all academic fields. Political science students need to study the power and influence of information dominance in today's political environments. Business students must study and learn how to treat information security as an integral part of, indeed even anew line of business.

In addition, college faculty members working in information assurance have a new task in their already overburdened lives: informing and educating administrators and other faculty about the need for fundamental precautions as well as new institutional policies and practices. For example, at JMU a universal information security awareness program has been put in place. Students, staff, and faculty must proceed through a tutorial/quiz to obtain or change a password. The experience is totally online; it is not onerous, but does require that attention be devoted to information ownership, management, and protection issues. How many colleges and universities have something similar in place?

Achieving a balanced, university-wide approach to solving information assurance challenge is critical when some researchers are conducting only basic research and others are linked to the private sector through applied research. Too much isolationism or too much commercialism will doom information security efforts. This is not to say that the results of research and development are misguided; it simply underlines the need for a balance approach to the information assurance challenge for the academy. Some researchers should be encouraged to link up with the private sector – but not all of them.

In addition to the dilemma of balancing basic and applied research, there is the question of the structures of academic programs and the focus on pedagogy in the academy. These factors have a direct effect on information security through the quality of the labor pool working on the problem and the related research activities of institutions. But without leadership – particularly presidential leadership – there will be no reconceptualization of how academic curricula and programs need to be developed. The traditional

organizational structure and approach of higher education encourage small-scale, programmatic innovation along the fringes, such as incremental modifications of existing programs. We are doing better, but if the academy is to make a difference in the information assurance arena, it must bring about systems-level, paradigm-shifting curricular reforms. We must focus on programs, not academic units, and on pedagogy driven by solving problems through research.

Task forces and interdisciplinary teams designed to collaboratively examine threats and opportunities should be used creatively and strategically. Any opportunity that facilitates interaction between people who do not traditionally communicate should be pursued. In their well –intended zeal to establish information security profession or discipline, colleges should not close the door to political scientists, lawyers, mathematicians, psychologists and business faculty, who have much to offer.

Carefully crafted and flexible employment contracts and faculty activity plans that focus energies on mission–supporting activities can also be useful in achieving an effective systems-level intervention. Senior administrators may need to step in when traditional reward structures leading to promotion, tenure, and improved compensation do not function effectively in today's environment. Within higher education, we must stop talking about collaboration and start practicing it. Collaboration is hard and often inconvenient. It requires give as well as take.

Higher education must also do a better job of setting strategic priorities and must, through negotiation, establish an improved plan for who will do what. College presidents and faculty may have to surrender some of their traditional freedom to pursue research and instruction as they like and instead consider who will contribute the individual components of an integrated solution to information assurance.

We also need to admit that this three-legged stool of government, higher education, and business is a bit wobbly. Examples of higher education and business working together do come to mind frequently. Likewise, government and the private sector have come together, especially since September 11, in discussing the need for a commitment to security in technology products. But there are few examples of the three sectors joining to provide solutions to information assurance needs. That can-and must – happen.

Finally, we have an obligation to consider the balance of public interests and security with privacy and individual rights. When feeling threatened, Americans have been willing to give some personal freedoms over the past half-century. For example, my parents grew up in a rural society in which doors to homes were locked only when residents were away for summer vacation. Keys were left in auto ignitions overnight, and no one gave a thought to walking alone. But times and conditions change, and now my parent's grandchildren always secure their home and their car and would never think about being out alone late at night. Similarly, in an earlier time, information security precautions might have been thought of intrusions into personal freedoms, but in today's environment of terrorist threats, they are sensible as locking the door at night. Opinion polls after the 9/11 attacks have suggested that the public is willing to trade some civic liberties for more personal security.

This willingness must be approached cautiously, however. As the president of an institution named for one of our Founding Fathers, I believe in the words of James Madison are instructive: "As a man is said to have the right to his property, he may be equally said to have a property in his rights. Where an excess of power prevails, property of no sort is duly respected. No man is safe in his opinions, his person, his faculties or his possessions." We need all of the resources of the higher education academy to achieve this difficult legal, technological, and policy balance.

The above article is by Dr. Linwood Rose, President of James Madison University. It appeared in the September/October 2004 of the EDUCAUSE review.

## National Security Higher Education Advisory Board (NSHEAB)

The NSHEAB had their quarterly meeting at the FBI HQS in Washington, D.C. and there were some changes to the board.

Three charter members have retired Purdue University President Martin C. Jischke, West Virginia University President David C. Hardesty, Jr., and Texas A&M University President Robert M. Gates.

The new members are as follows:
Association of American Universities President Robert Berdahl.
Arizona State University President Michael Crow.
Rice University President David Leebron.
University of Colorado-Boulder Cancellor G.P. "Bud" Peterson.
New York University President John Sexton.
Michigan State University President Lou Ana Simon.
Cornell University President David Skorton.

These new members join the current Board which includes:

The Pennsylvania State University President Graham B. Spanier (Chairman).
Carnegie Mellon University President Jared L. Cohon.
Iowa State University President Gregory L. Geoffroy.
Massachusetts Institute of Technology President Susan Hockfield.
The Johns Hopkins University President William R, Brody.
University of California- Los Angeles Chancellor Albert Carnesale.
University of California – San Diego Chancellor Marye Anne Fox.
University of Florida President J. Bernard Machen
University of Maryland – College Park President C.D. Mote, Jr.
University of North Carolina – Chapel Hill Chancellor James (Charles) Moeser
University of Pennsylvania President Amy Gutmann
University of Washington President Mark (Allen) Emmert
University of Wisconsin – Madison Chancellor John D. Wiley

The mission of the NHEAB includes the promotion of the understanding of the unique culture, traditions and practices of higher education, including the openness and academic freedom and the importance of international collaboration. The NSHEAB also serves as a means to open doors of understanding and cooperation with leaders in higher education on matters related to national security, terrorism, counterintelligence, cyber threats and certain criminal matters.

**********

## Security is a team effort!