Briefing to CSIS Commission on Cyber Security for the 44th Presidency

By Rodney Petersen and Jack Suess on behalf of the EDUCAUSE/Internet2 Security Task Force

March 12, 2008

COMPUTER AND NETWORK SECURITY TASK FORCE

Established by EDUCAUSE and Internet2 in July 2000, the EDUCAUSE/Internet2 Computer and Network Security Task Force works to improve information security and privacy across the higher education sector by actively developing and promoting effective practices and solutions for the protection of critical IT assets and infrastructures. For more information, visit www.educause.edu/security.

Briefing to CSIS Commission on Cyber Security for the 44th Presidency
By Rodney Petersen and Jack Suess on behalf of the
EDUCAUSE/Internet2 Security Task Force
March 12, 2008

Remarks of Rodney Petersen:

Thank you, Howard. Good morning. I would like to thank Jim Lewis for the invitation to appear today before the Commission. I began having conversations with Jim and Phil Reitinger in the fall about how the higher education community could participate in the work of this Commission. Jim described plans for a forum where we could brief the Commission, and I am pleased to be with you today as a result of his follow-through on that request. I also want to thank the Commission cochairs and members for the important work they are doing on behalf of our country.

We are here today on behalf of the higher education sector to comment on how the next administration can assist the cybersecurity needs of colleges, universities, and our nation. The higher education sector is extremely large and diverse, comprising over 6,000 colleges and universities, including over 4,000 nonprofit institutions of higher learning. The types of institutions range from two-year commuter colleges to some of the largest research universities in the world. The vast majority of institutions are private colleges and universities with no official ties to or direct funding from their state government. However, there are a significant number of public colleges and universities, such as Jack's institution, the University of Maryland, Baltimore County, which are often considered a branch of state government and therefore subject to state oversight and regulation. This diverse set of institutions are represented by six major higher education associations representing two-year schools or community colleges, private colleges, state and land-grant universities, and research universities. The unifying voice for all of these presidential associations is the American Council on Education.

There are several ways in which higher education and cybersecurity intersect. I want to share them with you so as you develop your recommendations you are clear about the role that academia can play. First, through its core mission of *teaching and learning*, higher education is the main source of our future leaders, innovators, and technical workforce. Second, through *research*, higher education is the basic source of much of our new knowledge and subsequent technologies. Finally, as complex institutions, colleges and universities operate some of the world's largest collections of computers and high-speed networks.

As many of you know, EDUCAUSE has been a significant player in the cybersecurity arena. EDUCAUSE joined forces with Internet2 in 2000 to form a Computer and Network Security Task Force. In 2002, I was detailed from the University of Maryland to support the Security Task Force and eventually transitioned to become a full-time EDUCAUSE employee. Through the Security Task Force, EDUCAUSE has

participated in the National Strategy to Secure Cyberspace, the National Cyber Security Partnership, the National Cyber Security Alliance, the Partnership for Critical Infrastructure Security, and the Cross-Sector Cyber Security Working Group to ensure that our efforts our integrated into and informed by national cybersecurity efforts.

I am pleased to introduce Jack Suess, a former cochair of our Security Task Force and the current chair of the Executive Advisory Group for the Research and Educational Networking Information Sharing and Analysis Center (REN-ISAC). Jack is the vice president for IT and CIO at the University of Maryland, Baltimore County. He is also a member of the EDUCAUSE Network Policy Council. Jack is a highly respected national leader, both among his CIO peers and in the higher education security professional community.

Remarks of Jack Suess:

Thank you, Rodney. We want to share with you today some of our successes and challenges within the higher education sector and leave you with some recommendations as you prepare your report for the next administration.

First, our strength in higher education is our ability to collaborate. Consequently, higher education as a sector is far more organized today than it was five years ago.

We have a very active Security Discussion Group with over 2,200 subscribers where security professionals can ask questions, receive advice and information, exchange best practices, and discuss operational concerns.

In the spring we will hold our 6th Annual Security Conference with over 500 attendees. The event brings together government, industry, and higher education security practitioners to exchange ideas for how to improve cybersecurity on campus.

The Higher Education Security Task Force is a very active community organization with six working groups and over 125 active volunteers representing 90 different institutions. The task force is supported by professional and support staff from both EDUCAUSE and Internet2. Notable this past year is the development of effective practice documents for institutions on confidential data handling and Payment Card Industry Data Security Standards (PCI DSS).

In 2003, we established the Research and Education Networking Information Sharing and Analysis Center at Indiana University. The REN-ISAC has 467 individual members from 226 different institutions of higher education. The REN-ISAC works closely with DHS, US-CERT, and the other sector ISACs.

Second, cybersecurity is a much higher priority on campus.

The EDUCAUSE Center for Applied Research (ECAR) did large-scale studies of approximately 400 institutions in 2002 and 2005. ECAR saw a doubling in the number of

institutions having a full-time security officer and dramatic increases in the use of network security devices such as firewalls and intrusion detection or intrusion prevention systems. Institutions reported feeling more secure than two years before despite being in a perceived riskier environment.

Data security breaches combined with several states enacting security breach notification laws have forced institutions of higher education to take a serious look at how they handle notifications following incidents. More importantly, they are working to prevent data exposures in the first place through aggressive data protection initiatives. As mentioned earlier, the Security Task Force has assembled a Data Incident Notification Toolkit and a Blueprint for Handling Sensitive Data to assist campuses in both of these areas.

In preparation for this briefing today and in anticipation of a future opportunity to refine our input to the Commission, we have asked our community the following questions:

1. What role has the federal government played to improve cybersecurity these past few years that has been useful for the higher education sector?
2. Are there ways in which the federal government has hindered progress? If so, please describe.
3. Are there new initiatives you would like to see from the federal government to help improve cybersecurity?

While we are not prepared at this stage to provide a detailed report of the input received, we have identified a few trends and have reached a few conclusions that lead us to recommend the following to the Commission.

Recommendation #1: The federal government should continue to invest in programs and resources, such as the Federal Trade Commission, the Cyber Security Division of the National Institute for Standards in Technology, the National Cyber Security Alliance, and US-CERT, that will serve the government and nonprofit sector.

In response to the first question (what role has the federal government played to improve cybersecurity), the higher education community has repeatedly pointed out the value of partnerships and the programs and resources that are funded by the federal government.

The higher education sector has benefited from partnerships with both the government and private sector these past few years. For example, the National Cyber Security Alliance has supported our annual student awareness video contest and a number of other awareness efforts. Thanks to Assistant Secretary Greg Garcia and Guy Copeland, higher education participates in the Cross-Sector Cyber Security Working Group. These partnerships are critical to colleges and universities continuing to be part of the solution.

It is difficult for nonprofit organizations to build the costs for security into the products and services they sell. At a time when state funding is declining and rising tuition prices are under increased scrutiny, colleges and universities as nonprofit organizations must be creative and resourceful in addressing the cybersecurity challenge.

In that regard, NIST has been an invaluable resource to the nonprofit sector. NIST standards and guidelines, especially the 800 series, are highly valued resources within the higher education community, though some would appreciate greater brevity and simplification in the documentation provided.

US-CERT, while it has not fully reached its potential, is recognized as an important source of information for the community.

The NSA and DHS National Centers of Excellence in Information Assurance Education and Training have stimulated academic degree programs that both expand the cybersecurity workforce and generate interest and enthusiasm among students, faculty, and academic administrators that in turn helps our cause.

The Federal Trade Commission, through its consumer awareness and education efforts in the areas of identity theft and information security, has been a tremendous resource for campus awareness efforts.

Campuses also report a positive experience with the FBI's InfraGard program as they participate in local chapters and receive educational briefings, network with other campuses, and participate in the information-sharing network organized by InfraGard.

Recommendation #2: The federal government should develop laws, regulations, standards, and guidelines that are more uniform in approach and less complex in execution.

In response to our second question (in what ways has the federal government hindered progress), the higher education community has remarked on Congress's failure to establish a uniform data security incident notification law, which means our colleges and universities must understand and comply with as many as 39 different state laws. We also hear complaints about the confusing and complex regulatory environment under which institutions of higher education must operate.

We enter cautiously into a recommendation that more or better federal government regulation is desirable, due to a concern that the regulatory climate may become more complex and burdensome.

Let me cite an example of why we want clarity. Campuses face the following compliance challenges today. We are subject to the HIPAA security rule, but not the privacy rule, for health information. Although not financial institutions, certain aspects of college and university operations are subject to the Safeguards Rules under the

Gramm-Leach-Bliley Act. In both cases, we are exempt from the privacy rules because a different federal law applies to the privacy of student education records—the Family Educational Rights and Privacy Act (FERPA) from 1974.

While we are not subject to Sarbanes-Oxley, many members of our governing boards come from the commercial sector and expect SOX-like compliance of the institutions they now govern. And as recipients of federal contracts and grants, we are increasingly being held to FISMA-like standards in the contract agreements and grant terms that our institutions are asked to consent to. Add PCI DSS compliance, another contractual obligation, and you can begin to appreciate the patchwork of laws and regulations that are intended to guide our information security programs.

Making matters worse, universities are often required to track students by SSN for mandatory reporting to the federal government for financial aid or IRS purposes. We have made efforts through our publications, conferences, and documentation of best practices to come up with a model for a uniform approach to information security compliance. Nonetheless, we operate in a confusing and complex environment. We would welcome the opportunity to work with the next administration and Congress to develop a more coherent and effective set of information security standards for the education industry, possibly based on the ISO 27001 standard.

Recommendation #3: Continue to exert pressure and influence on the IT sector to improve the security of products and services.

We appreciate the efforts of the federal government to exert influence over the IT industry in the development of more secure products and services. We, too, have engaged in cooperative dialogue with industry partners through the efforts of the Security Task Force and the various higher education advisory boards to the IT industry. It is difficult, however, for the higher education sector to speak with one voice in the area of IT procurement, and our bargaining power at the contract and licensing table is impaired because of our nonprofit status. Additionally, we do not typically engage in industry-wide purchasing, except in the cases of system administrations such as the University System of Maryland. We applaud efforts such as the Core Configuration Desktop Deployment and similar initiatives.

On the other hand, we experience a particularly difficult situation in that many computers that connect to our campus networks are personally owned by students, faculty, and in some cases staff. Consequently, computer security is subject to the vagaries of the supply chain, which usually results in the sale of computers, operating systems, wireless routers, and other devices that are not secure by default. We would urge the government to consider ways that it could encourage retail stores, suppliers, and Internet service providers to help consumers purchase and deploy more secure systems in the home, campus residence halls, and the workplace by turning security on by default.

Recommendation #4: Make cybercrime a priority for federal criminal law enforcement.

Quite often the IT industry deflects attention from the insecurity of their products to the need to prosecute "bad guys" that exploit the very vulnerabilities they create. As representatives of the business or user communities, we do not appreciate that tactic, but we do agree that cybercrime enforcement must continue to be a high priority. In particular, federal criminal law enforcement is the only entity that can combat the global organized crime groups now using the Internet for criminal activities. We urge the federal government to become more vigilant in pressing for action.

Recommendation #5: The federal government should elevate the participation of higher education as a "critical asset" or "key resource" for purposes of cybersecurity preparedness and response.

We appreciate the invitation to appear before you here today. We also want to thank Howard Schmidt, Richard Clarke, and others who were part of the President's Critical Infrastructure Protection Board for including higher education in 2002 during the development of the original national strategy. You may recall that the higher education sector was specifically identified in the national strategy as an important sector in the nation's efforts to improve cybersecurity.

Six years later, we are considered the Higher Education Subsector of the Educational Facilities Subsector of the Government Facilities Sector as part of the National Infrastructure Protection Plan. We find this diminished status and role unacceptable. Additionally, the majority of our nation's colleges and universities are private institutions; therefore, it is inappropriate to categorize our sector as a "government facility."

Given what we know about the vast computing power and intellectual capacity at our nation's colleges and universities, we must recognize the higher education sector as a "critical asset" or "key resource" in protecting the nation's cyberspace. Rodney Petersen and the EDUCAUSE staff are available to participate and assist the federal government along with the other sectors, and we encourage the government and private sector to engage us at every possible opportunity.

In conclusion, higher education is deeply committed to improving the state of cybersecurity at our nation's colleges and universities and wants to be part of the solution to any national effort to secure cyberspace. We hope that by our presence today we have communicated our progress, identified the remaining challenges, and demonstrated our commitment to help the federal government realize the potential of a secure Internet.