

**Office of Operations Review and Audit**



**Program Review**

**Safeguarding Student Social Security Numbers  
in the UW System**

**August 2005**

## Table of Contents

	<b>Page</b>
Executive Summary	i
Scope	1
Background	1
Discussion and Recommendations	3
Collecting Social Security Numbers	3
Alternatives to Social Security Numbers	6
Student Identification Number	6
Record Identifiers	6
Student Records Access and Safeguards	9
Paper Records	9
Electronic Records	10
Employee Training and Other Safeguards	12
Systemwide Guidance on Social Security Number Collection and Use	12
Conclusion	13
Appendix 1	14
Appendix 2	15
Appendix 3	16

## **EXECUTIVE SUMMARY**

Identity theft is the fastest growing white-collar crime in the United States. Various studies indicate that Social Security numbers (SSNs) play a pivotal role in identity theft, and that SSNs are still widely used for various purposes by higher educational institutions. This report describes practices UW System institutions use when soliciting SSNs from students, some ways UW System institutions have used student SSNs, and measures and efforts UW System institutions have taken to safeguard student SSNs.

### **Collecting Social Security Numbers**

The federal Privacy Act of 1974 requires any federal, state, or local governmental agency to provide proper notice when requesting that an individual disclose his or her SSN. The review found that while many UW institution forms no longer ask for the SSN, some forms still ask students to provide the SSN, even though the SSN does not appear to be necessary, and some of these forms do not include the required notice. The report recommends that UW institutions review all institutional forms soliciting SSNs from students to determine whether SSNs are necessary and, if they are, that institutions include the proper notice.

### **Alternatives to Social Security Numbers**

The review found that all UW System institutions have stopped using the SSN as the student identification (ID) number, as required by Chapter 36, Wis. Stats. Although SSNs are stored in student data systems, UW System institutions no longer use the SSN as a record identifier. Some institutions have also limited the display of the SSN on student data systems or official documents. The report recommends each UW institution review its current uses of student SSNs and establish a process for determining appropriate future uses of student SSNs.

### **Student Records Access and Safeguards**

The review found that UW System institutions have taken steps to ensure that only authorized personnel have access to student records that contain personally identifiable and confidential information. These steps include granting access only to those who must have the access to perform their job functions, shredding documents that are no longer needed, and employing proper technologies to secure computer networks. Some institutional officials acknowledged that securing paper records on students remains a challenge, as these records are maintained at various locations on campus and storage space is limited.

### **System Guidance on Social Security Number Collection and Uses**

In order to ensure consistent safeguards across the UW System, a sample or boilerplate notice for SSN disclosure may be helpful. Increasing student and staff awareness about identity theft and limiting the collection and use of SSNs will help to reduce the risk of students becoming victims of identity theft. The report recommends that UW System Board of Regents or System Administration provide guidance on the collection, use, and maintenance of student SSNs.

## **SCOPE**

The University of Wisconsin System Office of Operations Review and Audit reviewed University of Wisconsin (UW) System institutions' practices in regard to collecting, using, and safeguarding student Social Security numbers. During the review, we talked to staff at UW-Eau Claire, Extension, Madison, Milwaukee, Stevens Point, Stout, and Superior, and UW Colleges. These staff were identified by the institutions and most were the registrars or supervisors of student records. We also contacted registrars at the remaining institutions. In addition, we interviewed staff from the admissions, financial aid, business, graduate school, student affairs, and information technology offices at some UW institutions. Finally, we reviewed forms that UW System institutions and some other higher educational institutions had posted on their websites.

## **BACKGROUND**

Social Security numbers were first created by the federal government in 1936 to track employees' earnings and retirement benefits. Since 1936, numerous legislative actions expanded the collection and use of SSNs. Because of their unique and unchanging characteristics, SSNs have also been used for purposes other than those authorized by federal or state laws. While such collection and use are permissive, certain steps are necessary to protect Social Security numbers, since their characteristics make them susceptible to identity theft. [Identity theft is the use of someone's name, address, Social Security number (SSN), bank or credit card account number, or other identifying information without his or her knowledge, to commit fraud or other crimes.]

Identity theft is the fastest growing white-collar crime in the United States.<sup>1</sup> According to a 2003 survey conducted by the Federal Trade Commission (FTC), identity theft losses to businesses and financial institutions totaled nearly \$48 billion, and consumer victims reported \$5 billion in out-of-pocket expenses in 2002 alone.<sup>2</sup> Since November 1999, when the FTC began to track the number of identity theft complaints, the number of complaints the FTC has received has increased steadily. In calendar year 2003, the FTC received 215,000 identity theft complaints, a 33 percent increase from 2002.<sup>3</sup> Not all incidents of identity theft are filed with the FTC. The Office of the Inspector General in the Social Security Administration estimates that there were about a half million identity theft incidents in 2000 and expects the number to more than triple, to 1.7 million, in 2005.<sup>4</sup>

Various analyses indicate that SSNs play a pivotal role in identity theft. A 1999 study conducted by the U.S. Sentencing Commission found that SSNs are used as breeder information to create

<sup>1</sup> Sakamoto, Jan. "Identity Theft: Arm Yourself." October 1, 2004 <<http://www.crimestoppers-honolulu.org/tips/idtheft.htm>>.

<sup>2</sup> Federal Trade Commission. "Identify Theft Survey Report." October 1, 2004 <<http://www.ftc.gov/os/2003/09/synovatoreport.pdf>>.

<sup>3</sup> Federal Trade Commission, *National and State Trends in Fraud and Identity Theft, January – December 2003* (Washington, D.C.: January 22, 2004).

<sup>4</sup> Office of the Inspector General, Social Security Administration. "Social Security Number Misuse, Identity Theft and the Internet." November 4, 2004 <[http://www.ssa.gov/oig/executive\\_operations/factsheet1.htm](http://www.ssa.gov/oig/executive_operations/factsheet1.htm)>.

false identification documents, such as drivers' licenses, and both the SSNs and drivers' licenses are most frequently used to generate fraudulent identifiers.<sup>5</sup> Some identity theft court cases also confirm that the SSN is central to committing fraud.

Evidence suggests that university students, faculty, and staff are not immune to identity theft. For instance:

- The *Bulldog News*, a University of Pennsylvania newspaper, reported that in November 2002 a man was arrested for stealing the names and SSNs of some 150 students from the University of California-Riverside and using the stolen information to obtain credit cards, running up more than \$200,000 in charges in the students' names.<sup>6</sup>
- The *Daily Egyptian*, a Southern Illinois University (SIU) newspaper, reported on a former student who wanted to prove a point about how easily students' SSNs can fall into unauthorized hands by picking through a garbage dumpster. The former student found an appointment list containing names, SSNs, addresses, and telephone numbers of several SIU students.<sup>7</sup>
- The *SecurityFocus.com* reported that in 2003 a University of Texas student was charged for breaking into a school database and stealing more than 55,000 student, faculty, and staff names and SSNs.<sup>8</sup>

More recently, there are reports of hackers gaining access to some university computer systems. While there is no indication the hackers have used the information for illegal activity, the incidents have cost the affected institutions time and money to notify students and staff whose personal information may have been compromised and have embarrassed the institutions.

These and other incidents are significant because it appears that SSNs are still widely used as identifiers by higher educational institutions. A 2002 survey by the American Association of Collegiate Registrars and Admissions Officers showed that nearly half of the colleges nationwide still use SSNs as the primary means of tracking students in academic databases.<sup>9</sup> Some institutions still use SSNs as student identification numbers, and the SSNs are printed on the face of the student identification cards.

<sup>5</sup> U.S. Sentencing Commission, *Identity Theft Final Report* (Washington, D.C.: Dec. 15, 1999).

<sup>6</sup> Bowen, Debra. "Don't Be a Victim of Identity Theft." *The Bulldog News*, December 16, 2002.

<sup>7</sup> Katzman, Dave. "Student ID Numbers Found in Garbage." April 24, 2003 <<http://www.dailyegyptian.com/spring96/050296/security.html>>.

<sup>8</sup> Brulliard, Karin. "Student Charged with Hacking at U-Texas." October 19, 2004 <<http://www.securityfocus.com/news/3174>>.

<sup>9</sup> Foster, Andrea L. "ID Theft Turns Students Into Privacy Activists, Colleges respond by reducing reliance on Social Security numbers in databases." *Chronicle of Higher Education*, August 2, 2002.

## **DISCUSSION AND RECOMMENDATIONS**

The goal of this review was to gauge UW System institutions' practices specific to student SSNs. Since federal laws and regulations specifically require SSNs for payroll and tax records and for financial aid, we focused our review on the collection and use of student SSNs on academic records, where such requirements do not exist. This report describes: 1) practices UW System institutions use when soliciting SSNs from students; 2) some ways UW System institutions have used student SSNs; and 3) measures and efforts UW System institutions have taken to safeguard student SSNs.

### **COLLECTING SOCIAL SECURITY NUMBERS**

In response to the widespread use of Social Security numbers and the growing concern for the privacy risks associated with their use, Congress passed the Privacy Act of 1974. The Act requires any federal, state, or local government agency that requests an individual to disclose his or her social security number to inform him or her: 1) whether the disclosure is mandatory or voluntary; 2) by what statutory or other authority the number is solicited; and 3) what uses will be made of the number.

We obtained some institutional forms from UW staff and UW System institutions' websites. The forms are used mainly in the registrar's office, admissions, and financial aid offices; and they do not represent all of the forms used in these offices. We found that some of the forms ask students to provide only their student identification (ID) number, and some forms ask the students for either the ID number or the SSN. We did find a number of forms on which only the SSN is requested, and we reviewed these forms. We analyzed the notice provided to students for consistency with the Privacy Act of 1974 and discussed with UW staff the need for the SSN on some of the forms where an SSN may not be required:

- *Admission Applications*: Applying for admission to the UW System institutions is done largely online. All UW System institutions use the UW System electronic application for undergraduate admissions, and all but UW-Madison use the UW System electronic application for graduate admissions, as well. UW-Madison generates a slightly different paper application for its paper recruiting materials. UW-Madison's professional schools and the School of Business also have their own admission applications. In addition to the application for admission, the individual schools may require supplemental admission information. All of the admission applications we reviewed ask for the SSN. UW staff indicated that the SSN is collected to crossmatch against existing student records, and leaving out the SSN does not nullify the application. The table below summarizes the results of our analysis of the admission applications we reviewed.

**Analysis of Social Security Number Collection in Various UW Admissions Applications  
and the Notice Provided to Students: Fall 2004**

<b>UW INSTITUTION</b>	<b>APPLICATION</b>	<b>NOTICE PROVIDED TO STUDENTS</b>
Systemwide	UW System Application for Undergraduate Admission (electronic application)	Notice is consistent with the Privacy Act of 1974.
	UW System Application for Undergraduate Admission (paper application)	Notice is consistent with the Privacy Act of 1974.
	UW System Application for Graduate Admission (electronic application)	Notice is consistent with the Privacy Act of 1974.
	University Special Student Application (electronic application)	Notice contains statutory authority and uses of the SSN but not whether submission of the SSN is voluntary or mandatory.
Eau Claire	Special Student Application (paper application)	Notice does not include source of authority to solicit SSN.
La Crosse	Upward Bound Student Application (paper application)	No notice provided.
Madison	UW-Madison Application for Undergraduate Admission (paper application)	Notice is consistent with the Privacy Act of 1974.
	UW-Madison Online Application for Graduate School	Notice does not include source of authority to solicit SSN.
	University Special and Guest Student Application (paper application)	No notice provided.
	Supplemental Application to the Doctoral Degree in Library and Information Studies (paper application)	No notice provided.
	Association of American Veterinary Medical Colleges Web Application (UW-Madison School of Veterinary Medicine )	Notice does not include source of authority to solicit SSN.
	School of Pharmacy Application for Admission to the Doctor of Pharmacy Program (electronic application)	No notice provided.
	UW Law School Application for Admission (paper application)	No notice provided.
	Milwaukee	Application for Graduate Non-Degree Admission (paper application)
Superior	Application for Admission to the Extended Degree Program (paper application)	Notice is consistent with the Privacy Act of 1974.

Sources: UW System institutions and websites.

- *Financial Aid-Related Forms:* The main application for financial aid is the Federal Free Application for Student Aid (FAFSA). UW System institutions have also customized some federal forms for institutional use, including student loan promissory notes, loan payment

deferral forms, and entrance and exit interview forms. These forms ask for the SSN, and UW staff indicated that they collect the SSN to meet federal requirements.

Some UW System institutions have also developed institutional forms for financial aid-related purposes. Examples of these institutional forms include Veterans Certification, verification worksheets for dependent and independent students, Statement of Non-Tax Filer, Scholarship Notification, Prior Degree/Verify Enrollment Form, Verification of Parent College Enrollment, and Athletic Award Notification. These forms ask the students to provide their SSNs, but the required notice is not given. Some UW institutions are considering revising some of the institutional forms where the SSN is not necessary.

- *Course and Grade Forms:* We reviewed forms that UW System institutions have developed for adding or dropping courses, changing grades, repeating a course, verifying enrollment, and requesting transcripts. Most ask for a student number, either the ID number or the SSN, or both. However, we found some forms that request only the SSN, and these forms do not provide any notice to students as required by the Privacy Act of 1974.
- *Other Forms:* We noticed some miscellaneous forms on which the SSN is requested without the required notice and for which the need was not apparent. Examples include an online form prospective students use to request additional information about the UW institution and a teacher intern application.

Asking students to provide their SSNs is required by law in some cases. In other cases, the SSNs are not required by law but are necessary for UW operations. This determination is best made by the UW System institutions, weighing the need for SSNs for program operations against the risk to student privacy. Thus, ***we recommend that UW System institutions: 1) review all institutional forms soliciting the SSN from students to determine whether SSNs are necessary and, if they are, 2) include the proper notice, consistent with the Privacy Act of 1974.*** The University of Texas System and the University of Illinois have developed sample and boilerplate notices for their institutions. (See Appendix 2 for University of Texas System sample notices.) Since our review, a number of UW System institutions have indicated they will review their institutional forms and include the proper notice.

Some higher educational institutions have taken formal steps to limit the collection of the SSN to better protect student privacy. For instance:

- Purdue University authorizes only the Office of Admissions and the Graduate School to produce forms asking applicants to provide a SSN.
- The University of Pennsylvania Task Force on Privacy and Personal Information, created in response to concerns about increasing threats to personal privacy, recommended that SSNs not be required on any university form unless mandated by law.
- The University of Illinois allows SSNs to be collected only in circumstances where the collection is mandated by a government agency.

- All university forms or documents requesting the SSN at the University of Northern Colorado must be approved by the institution's Social Security Usage Committee.

These and some other higher educational institutions took actions to reduce the collection of SSNs largely on their own initiatives. However, a number of states have enacted legislation specifically aimed at protecting SSNs and, in some cases, reducing the collection of SSNs is suggested as a means to better protect SSNs.

## **ALTERNATIVES TO SOCIAL SECURITY NUMBERS**

Because of their unique characteristics, SSNs are used for a variety of purposes. We reviewed how UW System institutions have used student SSNs as student and record identifiers and what alternatives are available.

### **Student Identification Numbers**

The main concern with the use of student SSNs as an identifier is the protection of student privacy. Uses must be consistent with state law and federal requirements, such as the Family Educational Rights and Privacy Act (FERPA).

Wisconsin is one of a number of states, including California, Colorado, Maryland, Michigan, New York, Texas, and Washington, that have enacted or proposed legislation aimed at limiting the use of the SSN as the student identification number in public higher educational institutions. Chapter 36, Wis. Stats, limits the use of the SSN as an ID number in the UW System. Section 36.11(35), Wis. Stats., prohibits the UW System from assigning students an ID number that is identical to or incorporates the students' SSNs.

A number of higher educational institutions in other states have also established policies or are moving toward limiting the use of SSNs as ID numbers. These institutions include Georgia Institute of Technology, Rutgers University, Indiana State University, the University of Florida, the University of Iowa, and the University of Minnesota-Twin Cities.

Staff at all but two of the degree-granting UW System institutions reported that they have assigned students randomly-generated numbers as their ID numbers. UW-Madison and UW-Milwaukee assign all new students random ID numbers but allow continuing students to keep their old ID cards, which still have the students' SSNs printed on them. As of the fall 2004 semester, the registrars at UW-Madison and UW-Milwaukee reported that about four percent and 25 percent, respectively, of the total number of enrolled students still had the old ID cards. Both institutions have undertaken efforts to urge these students to replace their old ID cards and to automatically assign returning students a randomly-generated ID number.

### **Record Identifiers**

UW System institution staff reported that the SSN is not the only key information that UW System institutions use to identify student records. We reviewed information related to student

databases, transcripts, and loan payment invoices at seven degree-granting institutions and the UW-Extension to determine the extent to which SSNs are used for student records:

- *Student Information Databases*: Most degree-granting UW System institutions use the PeopleSoft database for student-record administration, and PeopleSoft uses the random ID number, rather than the SSN, as the key record identifier and for record linkage in student information databases. Four UW System institutions – UW-Eau Claire, La Crosse, Stevens Point, and Stout – use other systems, and these systems have also been programmed to use information other than the SSN as the key record identifier. In all of these student-record systems, the SSN is a data element stored in the system databases and is displayed on certain database screens.

Some UW institution staff with whom we spoke indicated that the SSN remains a popular key identifier in record searches, as students often do not remember their ID number. While the student's name and date of birth combined can also be an identifier, they don't produce the match as accurately and efficiently as the SSN. These staff also believe that the SSN will be used less over time as students grow accustomed to their random ID numbers. However, it is unlikely that the random ID numbers will ever achieve the popularity of the SSN, as the random ID is unique to the institution in which the student is enrolled.

- *Transcripts*: Six of the seven degree-granting UW System institutions whose staff we interviewed reported that their institutions do not include the SSN on unofficial transcripts. However, most of these seven include the SSN on the official transcript. UW-Milwaukee did not include the SSN on the official transcript, but is now doing so again because of the demand from students and institutions to which these students apply. On the other hand, UW-Madison used to have the SSN on the official transcript, but has recently stopped doing so because of the increased concern for privacy.

Practices at other institutions vary. UW-Madison's registrar informally surveyed higher educational institutions that are members of the American Association of Universities and found that three-quarters of the 44 schools that responded to the survey include the SSN on the student's official transcript. However one-third of this group plans to remove the SSN soon or to use a truncated SSN. We contacted five Big Ten institutions and found that two of them do not include the SSN on the official transcript; two currently include the SSN on the official transcript but will remove the SSN when the migration to a new student record system is complete; and one of the five plans to keep the SSN on the official transcript. On the other hand, UW-Madison indicates it has never used the SSN on the official transcript.

- *Loan Payment Invoices*: UW System contracts with University Accounting Services (UAS) and Educational Computer Systems, Inc. (ECSI) to process billing for federal loans and most long-term institutional loans. According to UAS, student SSNs are included on the paper loan payment invoices. Since our review, UW-Madison indicates that ECSI has removed the SSNs from their invoices based on a request from UW-Madison. UW-Madison also directly processes billing for Perkins Loans taken out at UW-Madison, UW-Green Bay, and UW Colleges. These invoices currently do include student SSNs, but UW-Madison indicates it is working to limit the view to all but the last four digits.

Limiting the use of SSNs in student records is important to ensure compliance with FERPA. UW institution staff indicated that they do not disclose personally identifiable information, such as SSNs, from student records without the prior written consent of the students. However, class rosters and grade reports containing students' names and ID numbers are sometimes posted or made available for public view. Such posting or public display is considered by some to be a violation of FERPA, as the disclosure of the SSN for students who still have the SSN as their ID numbers is done without prior consent of the affected students. Transcripts, loan payment invoices, and other academic records containing the students' SSNs delivered to the wrong address may also increase the risk of loss of privacy.

To ensure that student SSNs are used only when absolutely necessary and in compliance with state or federal laws, some higher educational institutions have established structures for determining how their institutions use student SSNs. While the actions are viewed by some as being bureaucratic, the structures have been hailed by others as models for higher education institutions:

- *University of Texas System*: Upon passage of a Texas law protecting the confidentiality of SSNs, the university system convened a task force to evaluate and recommend a strategy for a comprehensive, coordinated approach to the collection, maintenance, and dissemination of SSNs on a systemwide basis. One product of the task force was the system's policy on protecting the confidentiality of SSNs. The policy calls for reduced use and display of SSNs.
- *University of Illinois*: To better protect information the University of Illinois collects about individual students, faculty, and staff, the Vice President for Business and Finance formed a committee to draft a policy for the university on the collection, maintenance, and use of SSNs. The policy the university adopted calls for each of its three campuses to appoint an administrator, the "SSN czar," who is responsible for overseeing the use of SSNs.
- *University of Northern Colorado*: To implement the Colorado law to protect the confidentiality of the SSN, the university established the Social Security Number Usage Committee. The committee is composed of the Registrar, Director of Admissions, Director of Human Resources, Assistant Vice President for Information Technology or their designee, and Director of Institutional Research. The committee must approve all forms soliciting the students' SSNs and uses of students' SSNs.

Continuing use of the student SSNs will continue to be critical for some UW System institution operations. However, each use must be consistent with state and federal laws, and then only after a determination that the use is necessary. To ensure that this is achieved, ***we recommend that each UW System institution review its current uses of student SSNs and establish a process for determining the appropriate future uses of student SSNs.*** Transcripts and loan payment invoices are just two of the areas in which a determination is necessary. At most of the UW System institutions included in our review, the registrar already functions as the institutional contact for FERPA-related issues. It would be natural for the registrar to have a key role in any process considered.

## **STUDENT RECORDS ACCESS AND SAFEGUARDS**

Student SSNs are found among many student records, both paper and electronic. Social Security numbers do not necessarily require extra protection. Once collected, however, the SSNs become a part of other confidential and private information that must be protected. We reviewed UW System institutions' practices on UW employee access to paper student records, measures UW System institutions put in place to protect electronic records from external access, and employee training and other safeguards.

### **Paper Records**

Some UW institution staff indicated that storage space is a problem at their institutions and the limited storage space limits their ability to protect paper student records. A number of UW System institutions have moved or are considering moving toward digitizing their paper records. These records could include admission applications, financial aid-related forms, course change forms, and other department-generated forms. However, UW institutions still have large volumes of paper records at various locations on campus.

Active student records are typically maintained in or near the individual university offices generating the records. Some records are maintained in a locked room, whether a separate storage room or a supervisor's office. Some are maintained in file drawers or on shelves in a designated area, often an area that is accessible to anyone who enters the office. However, staff indicated that university employees affiliated with offices that would typically have authorized access to the records would seek permission before accessing the files.

Older student records are kept in designated storage rooms, and UW officials reported that these rooms are locked and few university individuals have access to these rooms. Some records are disposed of after the required record-retention period.

The process for accessing individual student paper record files varies. Some offices use a log and require university staff to sign in to check out student files. Others operate on a less formal basis.

Some UW officials acknowledged that their institutions' measures to secure paper records could be strengthened. In addition to the lack of storage space, paper records on students are maintained across campus, making it challenging to properly secure all of the records. Limited storage space and decentralized recordkeeping will likely remain challenges for UW System institutions. One option is to move toward digitizing the paper records. Another option is to reduce the collection of personally identifiable information, the direction preferred by some higher educational institutions.

To the extent that paper records continue to include SSNs, during this review we identified some simple good practices for protecting paper records. These include: 1) closing and putting away student folders after use; and 2) shredding documents containing personally identifiable information that are no longer needed.

## **Electronic Records**

We identified some of the technologies UW System institutions use to protect student information in electronic databases and computer networks. Some computer experts agree that no student-record database and computer network are absolutely failsafe against unauthorized external access. However, UW institution officials expressed confidence that the measures their institutions put in place to control access to student electronic records are adequate to safeguard against unauthorized access.

### **Student Database Protection**

UW System institutions protect students' SSNs from unauthorized external access by restricting access to the student information database, where student records are maintained. The student information database is typically stored on a server. This server is connected to other application servers, forming a network, which enables UW employees and students to access the student records. Access to the database is through the application, such as PeopleSoft, and through direct connection.

Access to the student database through the application is managed by the application itself, which typically requires a login ID and password. The login ID and password are granted by the designated security administrator on a need-to-know basis.

UW System institutions also institute multiple levels of access. The level of access is determined by the security administrators. UW System institutions appear to approach access to SSNs differently. Some UW System institutions, including UW-Madison and UW-Green Bay, do not allow university employees with the lowest level of access to view the students' SSNs. UW-Madison also limits the view to the last four digits of an SSN for certain access levels. UW-Extension and UW-Stout are considering an approach similar to UW-Madison's and UW-Green Bay's. Even though UW-Extension may be considering a similar approach, UW-Extension's current approach has sufficient safeguards against unauthorized access. UW-Extension recently completed an internal review of its computer network control and found no significant weaknesses.

UW institution officials noted that UW employees who need access to student records must submit requests through their respective department management. The designated security administrators must approve the requests. Decisions to grant access are based on the employees' job functions or on the purposes for the request. Direct connection access to the student database is granted almost exclusively to UW employees whose job functions require exporting certain student information to other applications for institutional research and analysis.

### **Computer Network Protection**

To prevent unauthorized users from accessing student records, including SSNs and other personally identifiable information, UW System institution staff indicated their institutions have implemented some standard computer-network security measures. A computer network is simply a system of interconnected computers. The network allows users to share resources, but

also makes it vulnerable to unauthorized users. Some of the protections various UW institutions have put in place include:

- Firewall: A machine or software can create a protective barrier between two computer networks, sometimes even hiding an internal network from an external network, such as the Internet, or blocking or limiting traffic between these networks.
- Encryption: To protect the data flowing freely between computer networks, UW System institutions use a private key to encrypt the data when transmitting them over the Internet, converting them into a form that cannot be easily understood by individuals without the key.
- Vulnerability Probing: UW System institutions periodically assess their computer networks for weaknesses that might enable unauthorized users to break into the networks.
- Virus Scanning: UW System institutions use virus scanning software to constantly scan for viruses and disinfect them before they cause damage.

UW institution officials we interviewed expressed a high level of confidence in the security measures of their electronic student records. Without conducting an information technology security review, we cannot make a determination as to the effectiveness of the measures UW System institutions have put in place to protect against unauthorized access to student SSNs. However, some good practices that UW System institution staff indicated their institutions have emphasized with their employees include:

- turning off, logging off, or locking the computer monitor if and when employees go away from their desks even for a very short time;
- requiring passwords to have certain characteristics and level of complexity, and to be changed on a regular basis;
- guarding login IDs and passwords by having the staff log in for a student who needs access to the student information system, rather than giving the login ID and password to the student; and
- requiring employees who are granted access to student information systems to sign an agreement acknowledging to keep all records confidential.

Also, information technology websites at some UW institutions, including those for UW-Eau Claire Computing and Networking Services, UW-Madison Division of Information and Technology, UW-Milwaukee Computer Security Incident Response Team, and UW-Stevens Point Information Technology, include tips to students and staff on setting and guarding login ID and passwords.

## **Employee Training and Other Safeguards**

A number of UW institution officials and some experts agree that the best measures for guarding against inappropriate disclosure of and unauthorized access to students' personally identifiable information, including the SSN, are to stress good practices and to provide information and training to employees on privacy and confidentiality. Employees can be reminded, for example:

- to ask students to write down their SSNs on a piece of paper and then shred these papers, rather than having students give their SSNs verbally when they might be overheard; and
- to avoid providing student SSNs over the phone, even to individuals who have authorized access to the information.

In addition, UW System institutions post FERPA information on the institutions' websites. UW-Milwaukee includes in its requirements for access to the student-record system an online tutorial on FERPA.

Some UW institution officials who also serve as their institutions' FERPA contacts indicated that they have held training and seminars on privacy and confidentiality for faculty and staff. They also indicated that supervisors in departments that handle student records extensively cover privacy and confidentiality issues with new employees. Generally, UW staff with whom we spoke indicated that access to student information that includes SSNs is granted to university employees on a "need to know" basis, provided that the information is used for legitimate university or educational purposes.

## **SYSTEMWIDE GUIDANCE ON SOCIAL SECURITY NUMBER COLLECTION AND USES**

We conducted a search of other higher educational institution websites for policies on the collection and use of student Social Security numbers. We found that some higher educational institutions have adopted policies or guidelines specific to SSNs. Appendix 2 summarizes some of the policies or guidelines we reviewed. Also, Appendix 3 shows a resolution on the collection, storage, use, and disclosure of SSNs adopted by the Connecticut State University System.

The SSN policies and guidelines we reviewed emphasize different areas. Generally, these policies and guidelines restrict the collection, use, and display of the SSN and require proper notice when the SSN is solicited. While most of the policies and guidelines are institution specific, we did find some systemwide policies and guidelines at Connecticut State, University System of Georgia, Illinois State, and the University of Texas.

Regent Policy Document (RPD) 97-2, "Policy on Use of University Information Technology Resources," calls for UW System institutions to take reasonable precautions to protect electronic documents containing private and confidential information. Some UW System institutions, including UW-Green Bay, Madison, and Milwaukee, have adopted institutional policies on student-record privacy or FERPA-related guidelines.

Based on the instances we found in our review, we concluded that some instances where student SSNs are solicited and used do not appear necessary. Even when the collection is determined necessary for UW operations, UW System institutions have sometimes not provided the proper notice. Some UW institution officials with whom we spoke recommended that UW System legal counsel develop the notice, in order to be consistent across the UW System.

UW officials with whom we spoke indicated that they are aware of identity theft issues. We did not assess the overall level of awareness at the staff level. However, evidence suggests that identity theft incidents will likely continue to increase in the near future. Increasing staff and student awareness about identify theft, limiting the collection and use of student SSNs, and safeguarding the SSNs collected will help to reduce the risk of students becoming victims of identity theft. ***We recommend that UW Board of Regents or System Administration provide systemwide guidance on the collection, use, and maintenance of student SSNs.*** Adopting a Board of Regents resolution or establishing a systemwide policy statement would provide some guidance for UW institutions. Publishing resource information on UW System and institution web sites for staff and students about identity theft and privacy information could also increase awareness, and thus enhance UW institutions' efforts to safeguard SSNs.

## **CONCLUSION**

Our review indicates that UW System institutions have reduced the use of student Social Security numbers. All degree-granting UW institutions have stopped using the SSN as the student identification number and as the key identifier to student information databases. At the same time, we found a significant number of other instances where SSNs continue to be solicited and used. Some instances are required by law and others are not, but are necessary for UW operations.

UW System institutions have implemented measures to safeguard student records that contain SSNs and other personal and confidential information. However, we also found instances where SSNs are solicited without the proper notice required by federal law and where the SSN is used in ways that may increase the risk to student privacy. Thus, we have recommended that:

- UW System institutions review all institutional forms soliciting the SSN from students to determine whether SSNs are necessary and, if they are, ensure that the forms include the proper notice, consistent with the Privacy Act of 1974;
- UW System institutions review their current uses of student SSNs and establish a process for determining the appropriate future uses of student SSNs; and
- UW Board of Regents or System Administration provide systemwide guidance on the collection, use, and maintenance of student SSNs.

## Appendix 1

### University Of Texas System Sample Disclosures

#### **Disclosure for the employment process.**

Disclosure of your social security number (“SSN”) is requested as part of your application for employment with The University of Texas at \_\_\_\_\_ (the “University”). During the employment application process, your SSN will be used as a unique number in order to identify you within the University’s current applicant tracking system. Disclosure of your SSN at the time that you apply for employment is voluntary, but disclosure of your SSN is mandatory before you may be employed by the University. Federal law requires the University to report income and SSNs for all employees to whom compensation is paid. Employee SSNs are maintained and used by the University for payroll, benefits, internal verification, and administrative purposes, to verify employment, and to conduct background checks for security sensitive positions. The University reports SSNs to Federal and State agencies or their contractors as authorized or required by law and for benefits purposes. Further disclosure of your SSN is governed by the Public Information Act (Chapter 552 of the Texas Government Code) and other applicable law.

#### **Disclosure for the student application process.**

Disclosure of your Social Security Number (“SSN”) is requested for the student records system of The University of Texas \_\_\_\_\_ (the “University”) and for compliance with Federal and State reporting requirements. Federal law requires that you provide your SSN if you are applying for financial aid. Although an SSN is not required for admission to the University, failure to provide your SSN may result in delays in processing your application or in the University’s inability to match your application with transcripts, test scores, and other materials. Student SSNs are maintained and used by the University for financial aid, internal verification, and administrative purposes, and for reports to Federal and State agencies as required by law. The privacy and confidentiality of student records is protected by law and the University will not disclose your SSN without your consent for any other purposes except as allowed by law.

#### **General mandatory disclosure.**

Disclosure of your Social Security Number (“SSN”) is required of you in order for The University of Texas at \_\_\_\_\_ to [state intended use of SSN], as mandated by [Federal] [State] law. Further disclosure of your SSN is governed by the Public Information Act (Chapter 552 of the Texas Government Code) and other applicable law.

#### **General voluntary disclosure.**

Disclosure of your social security number (SSN) is requested from you in order for The University of Texas at \_\_\_\_\_ to [state intended use of SSN]. No statute or other authority requires that you disclose your SSN for that purpose. Failure to provide your SSN, however, may result in [state what may happen if the individual fails to provide SSN]. Further disclosure of your SSN is governed by the Public Information Act (Chapter 552 of the Texas Government Code) and other applicable law.

## Appendix 2

### Examples of Policies or Guidelines on Social Security Number Use and Collection Adopted by other Higher Educational Institutions

INSTITUTION	TITLE AND YEAR ADOPTED	POLICY EMPHASIS
Ball State University	Social Security Number Policy (date unknown)	Discontinue the use of SSNs as the student ID number; limit public display of SSNs; properly destroy documents containing SSNs; use, collect, and disclose SSNs only as permitted by laws.
Connecticut State University System	Board of Trustees Resolution (2002)	Use and display SSNs only as permitted by law, and provide proper notice when soliciting SSNs.
Georgia Institute of Technology	Social Security Number Policy (2002)	Limit collection and release of SSNs.
Illinois State University	Use of Social Security Numbers by Illinois State University (1996)	Restrict access to and use of SSNs.
Indiana University South Bend	Student ID/Social Security Number Policy (date unknown)	Make disclosure of SSNs voluntary; use a special number other than the SSN as the student ID; and limit disclosure of SSNs outside of the university.
North Carolina State University	Use of the Social Security Account Number by the University (date unknown)	Call for collection and use of SSNs to be consistent with federal laws and regulations.
Purdue University	Requesting Social Security Numbers for Educational, Employment and Other Recordkeeping Purposes (1978)	Limit solicitation of SSNs and use of SSN as ID number, and recommend language for notice when soliciting SSNs.
Temple University	Social Security Number Usage Policy (2004)	Use SSNs only as permitted by law or required by practical necessity; eliminate use of SSNs as primary identifier; and increase protection of SSNs and other personal and confidential information.
University of California-Los Angeles	Federal Privacy Act – Notices Regarding Social Security Numbers (1999)	Provide a summary of requirements with which university must comply when soliciting and using SSNs.
University of California-Santa Barbara	Collection and Use of Social Security Number (1985)	Provide a summary of requirements with which the university must comply when soliciting and using SSNs.
University of Michigan	Discontinuation of Use of Social Security Numbers as Common Identifiers at the University of Michigan (1996)	Discontinue the use of SSNs as common identifiers and as the key to information databases.
University of Northern Colorado	Student/Employee Identification Number Regulation (date unknown)	Establish the SSN Usage Committee to oversee SSN usage, and provide recommended language for notice when soliciting SSNs.
University of Texas System	Protecting the Confidentiality of Social Security Numbers (2004)	Reduce collection, use, and public display of SSNs; control access to SSNs; and establish accountability for protecting the confidentiality of SSNs.
University System of Georgia	Protecting Student Identity – Principles of Good Practice (2002)	Establish institutional policies and procedures for collection and use of SSNs; stop using SSNs as student ID number.

Source: Institution websites

## **Appendix 3**

### **RESOLUTION**

**concerning**

### **THE COLLECTION, STORAGE, USE AND DISCLOSURE OF SOCIAL SECURITY NUMBERS**

June 14, 2002

- WHEREAS, The Board of Trustees desires to protect the confidentiality and privacy of students and employees of the Connecticut State University System concerning the collection, use and disclosure of Social Security Numbers, and
- WHEREAS, The Board of Trustees deems it appropriate to institute a policy with regard to obtaining, using and disclosing such numbers; now be it
- RESOLVED, That, except in those cases and for those purposes in which Federal or State law permits or requires obtaining, using or disclosing a person's Social Security Number for identification or other prescribed reasons, no person shall be required to provide his or her Social Security Number to the Connecticut State University System or its universities, and no data system in the Connecticut State University System will publicly identify a person with a code or an identifying number that contains a reference to or duplicates a person's Social Security Number or otherwise uses or discloses a Social Security Number unless so permitted or required by Federal or State law, and be it further
- RESOLVED, That offices within the Connecticut State University System may continue to request, collect, store, or maintain Social Security numbers as permitted or required by Federal or State law, and be it further
- RESOLVED, That whenever Social Security Numbers are collected, stored, maintained, used or reported, students, faculty or staff in the Connecticut State University System must be notified, except as otherwise precluded by Federal or State law, (generally or individually, as the case may be) of any use or disclosure of their Social Security Number and personnel responsible for keeping, maintaining or disclosing Social Security Numbers pursuant to applicable Federal or State law must be notified that Social Security Numbers are confidential and must be protected from disclosure except as permitted or required by Federal or State law, and be it further
- RESOLVED, That compliance with this policy will be implemented as soon as is practicable.

A Certified True Copy:

William J. Cibes, Jr.  
Chancellor

Source: Connecticut State University System. <[http://w3.sysoff.ctstateu.edu/web/CSUweb\\_Trustees.nsf/b7989b92524436ce852569d8004a4615/1de026ca02e8dbde85256bdb006882d4?OpenDocument](http://w3.sysoff.ctstateu.edu/web/CSUweb_Trustees.nsf/b7989b92524436ce852569d8004a4615/1de026ca02e8dbde85256bdb006882d4?OpenDocument)>