

BOF#5

SECURITY AND PRIVACY ISSUES

Wednesday

December 1, 2010



START HERE
GO FURTHER
FEDERAL STUDENT AID®

Bridget-Anne Hampden

Deputy Chief Information Officer

FEDERAL STUDENT AID
U.S. Department of Education



START HERE
GO FURTHER
FEDERAL STUDENT AID®

The Top 10 Most Dangerous Places for Your SSN

10 - Medical insurance, offices & clinics

9 - Technology companies

8 - Nonprofits

7 - Medical businesses

6 - Federal government



The Top 10 Most Dangerous Places for Your SSN, cont.

5 – Local governments

4 – State governments

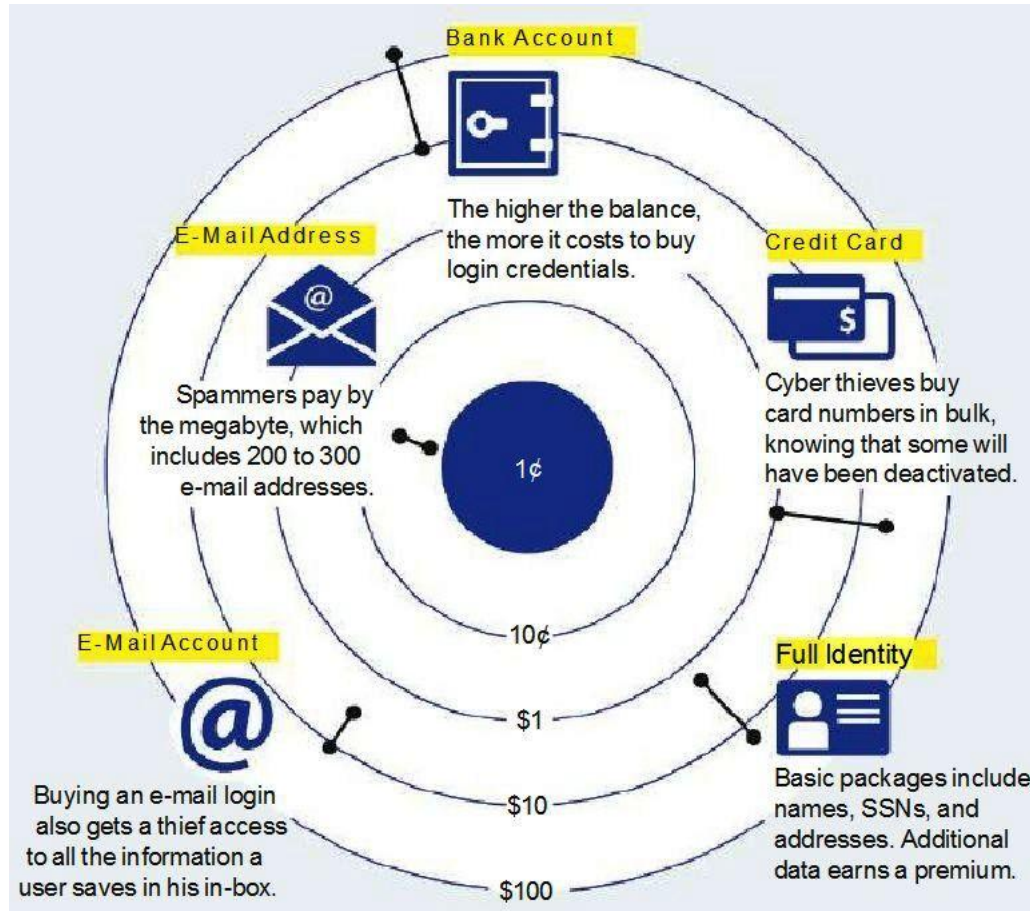
3 – Hospitals

2 – Banking & financial institutions

1 – Colleges & universities



The Motivation



Foundation for Protecting PII

Security Program

Privacy Program

Breach Response



A Quick Look at the Headlines

October 29, 2010, private info of 40,000 University of Hawaii Students posted online

August 10, 2010, private info of 30,000 Florida State College at Jacksonville and five other state college students accessible

June 3, 2010, private info of 15,800 Penn State University students may have been discovered by hackers

June 2, 2010, private info of 25,572 Penn State Students may have been exposed

January 6, 2010, private info of 51,000 North Carolina Community College System users may have been exposed



General Discussion

- University PII Checklist
- GA PII Checklist

University PII Checklist

School Name:

Address:

School Point of Contact:

Phone Number:

E-mail Address:

Question	I. Leadership	II. Privacy Risk Management & Compliance Documentation	III. Information Security	IV. Incident Response	V. Notice and Redress for Individuals	VI. Privacy Training & Awareness	VII. Accountability	Response (Yes or No)	If No, Is a Mitigation or Action Plan in Place? When Completed?	Security Impact (5 = highest)
----------	---------------	--------------------------------------------------------	---------------------------	-----------------------	---------------------------------------	----------------------------------	---------------------	-----------------------	-----------------------------------------------------------------	-------------------------------



University PII Checklist

(I. Leadership)

Question	I. Leadership
Has a senior official with privacy experience been appointed?	●
Does the senior privacy official report to the head of the organization?	●
Does the senior official have authority, resources and support to implement policies and programs aimed at protecting privacy and Personally Identifiable Information (PII)?	●
Have you established privacy policy and roles and responsibilities to ensure there is leadership and accountability for the privacy program?	●
Is leadership aware of its PII responsibilities?	●



University PII Checklist

(II. Privacy Risk Management & Compliance Documentation)

Question	II. Privacy Risk Management & Compliance Documentation
Have you conducted an inventory of where PII is stored; both paper and electronic? Does this inventory include protected health information that may be stored by your organization's health care unit?	•
Have baseline security requirements been put in place?	•
Is there a process to retire systems that hold PII data?	•
Does the organization have written privacy policies, guidance and instructions?	•
Does the institute share privacy information with other external organizations? If so, are there written agreements in place that specify how PII will be handled, controlled, protected, etc?	•
Are PII files securely stored when not in use? Are markings used to designate sensitive information (eg, "confidential")	•
Are office entry points controlled?	•
Are surveillance cameras in use?	•
Is there an after hours sign in log?	•



University PII Checklist

(II. Privacy Risk Management & Compliance Documentation, continued)

Question	II. Privacy Risk Management & Compliance Documentation
Has adequate secure storage space been provided to store PII?	•
Is after hours access to areas where PII is handled or used for business purposes restricted by card or key? If so, are locks/combinations changed periodically?	•
Have sensitive data destruction bins or shredders been provided to dispose of hard copy PII?	•
Are the following safeguards used to protect PII data shipments: double packaging, trackable deliveries, data sensitivity labels on the inside of the package?	•
Has an assessment been made that identifies data sensitivities, likelihood of a breach, risk levels, controls, test methods based on risks?	•
Area data transfers encrypted with strong algorithms?	•
Are periodic tests and risk assessments performed to identify weaknesses and vulnerabilities?	•
Based on the risk assessment, if applicable, has a remediation plan been developed?	•
Do you have written privacy policies around access rules for PII within a system and PII retention schedules and procedures?	•



University PII Checklist

(III. Information Security)

Question	III. Information Security
Are technical, managerial and operational security controls in place?	•
Are security background investigations completed on employees that have access to PII?	•
Are mobile devices encrypted?	•
Does network security include firewalls, network intrusion detection, auditing and intrusion prevention? Antivirus and antispyware?	•
Is protection of PII integrated with information security and IT? Do the privacy officer and the security officer regularly communicate?	•
Is there a commitment to reduce the collection and retention of privacy data?	•
Is security consistent with risk and sensitivity of privacy data?	•
Do information system controls cover access, configuration management, segregation of duties, continuity of operations and an organization-wide information security program?	•



University PII Checklist

(III. Information Security, continued)

Question	III. Information Security
Does host based security include configuration compliance, internal firewalls, access controls, host based intrusion detection, patch management and logging?	•
Does application security include a security plan, tests for known vulnerabilities prior to implementation, authorized access, rules of behavior, secure web interfaces and limited PII entries and displays?	•
Are security and privacy risk mitigation included throughout the project life cycle?	•
Is access to PII restricted to only those who need this information to conduct their official duties? For electronic systems, is role-based access used to enforce these restrictions?	•
Have privacy enhancing technologies (PET) including computer tools, applications and mechanisms like adopting user numbers instead of the SSN been considered to mitigate risk?	•
Do you employ session timeouts on computer workstations that have access to PII?	•
Do you enforce multifactor authentication for remote access to systems that contain or process PII?	•
Are computers equipped with software for secure file deletion?	•



University PII Checklist

(IV. Incident Response)

Question	IV. Incident Response
Have you developed and implemented a written data security breach disclosure and notification process?	•
Do you have in place a manual or automated system for tracking privacy incidents to ensure all are detected, reported and responded to in a consistent way?	•
Are you aware of Federal and state privacy regulations?	•
Do you have an incident response process that includes:	•
Who to contact when they suspect a loss or compromise of PII data?	•
An evaluation of the scope, the amount of damage and the number of individuals affected by the data breach.	•
Notification of the individuals whose data has been compromised.	•
Public relations management.	•
Mitigation and forensics.	•
Regulatory reporting.	•
Do you have a help desk and call procedure for all individuals whose data may have been compromised?	•
Have you ensured the enterprise breach disclosure effort is scalable to address the scope of the breach?	•
Are you prepared to offer appropriate remediation measures that are timely and effective? Examples include free credit monitoring services, fraud alert services, identity monitoring and personalized remediation services.	•



University PII Checklist

(V. Notice and Redress for Individuals)

Question	V. Notice and Redress for Individuals
Have you developed procedures for individuals to access their information and to correct or amend inaccurate information?	•
Is there a procedure in place for managing privacy complaints?	•
Is there a written statement regarding what private information is collected, the purpose of the collection, how the information is used, to whom the information is disclosed and shared, rights under the Privacy Act, and types of redress programs?	•
Do you track privacy complaints for purposes of internal and external reporting and process improvement?	•



University PII Checklist

(VI. Privacy Training & Awareness)

Question	VI. Privacy Training & Awareness
Are staff aware of what constitutes personally identifiable information?	●
Is mandatory security awareness training given to new employees on their responsibilities for PII?	●
Is there an annual requirement that is met for completing "refresher" PII awareness training?	●
Have staff been trained in procedures for protecting PII and reporting suspected loss?	●
Are staff members familiar with common threats to protecting PII such as Keyloggers and Trojan horses?	●
Do staff with access to PII sign a Rules of Behavior document that clearly states how PII must be protected, how PII breaches must be reported, and consequences for misuse of PII?	●
Are staff aware of the policies and resources available for managing PII?	●
Do staff encrypt PII data at rest? In transit?	●
Are staff familiar with the differences between encrypting a file and password protecting a file?	●



University PII Checklist

(VII. Accountability)

Question	VII. Accountability
Does the organization perform self-assessments of activities involving PII to determine where PII data exists, whether appropriate policies exist to ensure protection of PII, to identify GAPS and to determine if policies are effective and being followed?	●
Do you have signed agreements with your business partners that clearly state such partners' roles and responsibilities for protecting PII, and for responding to PII breaches/incidents?	●
Are there reporting requirements in place to measure the organization's progress and performance and to identify vulnerabilities in policy implementation? Are there consequences stated for individuals who misuse, or fail to adequately protect, PII and other sensitive personal information (eg, health information)?	●

GA PII Checklist

Guaranty Agency Name:

Address:

FSA Contact Name: Robert Ingwalson

Phone Number: 202-377-3563

E-mail Address: robert.ingwalson@ed.gov

Please submit completed form by e-mail to [GAPII Checklist@ed.gov](mailto:GAPII_Checklist@ed.gov)

Question	Response (Please reply Yes or No)	If No, Is a Mitigation or Action Plan in Place? When Completed?	Reference	Page	Security Impact (5 = highest)	Comment
----------	-----------------------------------------	-----------------------------------------------------------------------	-----------	------	-------------------------------------	---------



GA PII Checklist

(Data Privacy / Policies)

Question	Reference	Page	Security Impact (5 = highest)	Comment
Do you have a privacy program that includes policies, controls, training, and an incident response plan (including cyber events)?	NIST 800-122	ES-3,4 p 4-1, 2	5	You need to document your roadmap for privacy and keep everyone informed. Documented incident response procedures will help contain an incident before major harm can be done.
Do you employ documented policies, procedures, automated and manual controls of access to all systems and data?	NIST 800-53 r3	Appendix F-AC, Page F-3	3	Documentation will help ensure the appropriate controls are in place.
Do you have a mandatory computer security and awareness training program that systems users must complete prior to gaining access to one or more of your systems?	NIST 800-53 r3	Appendix F-AT, Page F-21-22	4	Even with a secure system, breaches can result from untrained users.

GA PII Checklist

(Data Privacy / Policies, continued)

Question	Reference	Page	Security Impact (5 = highest)	Comment
Do you have an enforced policy regarding the classification of users who access your system, the type of background clearances required, and periodic updates of their continued need for system access?	NIST 800-53 r3	Appendix F-PS, Page F-88	3	You need to know in what capacity and who is accessing your data.
Do you have documented security plans for each system / application that would be in compliance with Massachusetts Privacy Law 201 CMR 17.00?	NIST 800-53 r3	Appendix F-PL, Page F-85	4	Documented security plans can provide a roadmap to adequate security.
Do you have an enforced policy regarding the permissible use, and mandatory protections for portable electronic media that would be in compliance with Massachusetts Privacy Law 201 CMR 17.00?	NIST 800-53 r3	Appendix F-MP, Page F-71	5	Enforced encryption of information on portable media that is easily stolen or lost is a must.
Do you have an enforced policy regarding the appropriate use, and mandatory protections of all of your servers, networks, and storage devices that would be in compliance with Massachusetts Privacy Law 201 CMR 17.00?	NIST 800-53 r3	Appendix F-MA, Page F-66	4	Defense in depth will help prevent unauthorized disclosures.



GA PII Checklist

(Systems / Applications Access)

Question	Reference	Page	Security Impact (5 = highest)	Comment
Do you employ a strategy whereby all systems are categorized based upon their risk profile (e.g., High - systems with privacy data; Moderate - systems with some privacy data and reputational risk if compromised; Low - systems with no privacy data or reputational risk if data is lost)?	NIST 800-53 r3	Chapter 3, Page 18 Appendix F-RA, Page F-92	5	Categorizing the risk profile for a system is important to ensure adequate controls are implemented. If not completed, all systems should be identified as with a high risk profile and protected as such; which might be a waste of resources.
Do all systems rely upon your corporate trusted access management system to authenticate an individual's request for system access events, thus ensuring access to only those elements of data previously authorized?	NIST 800-53 r3	Appendix F-IA, Page F-54-55	5	Access control is essential for safeguarding a system and its data.



GA PII Checklist

(Risk Assessment)

Question	Reference	Page	Security Impact (5 = highest)	Comment
Do you have a pre-defined set of controls that are associated with the risk profile of systems (e.g., High - data encrypted at rest and in transit; two factors for remote access; Low - data encryption not required)?	NIST 800-53 r3	Chapter 2, Page 19 Appendix E, Page E-1	5	Controls should match your system's risk profile to ensure adequate controls are implemented.
Have all of the selected controls been implemented where possible?	NIST 800-53 r3	Chapter 3, Page 26	5	Validation of controls will identify gaps to remediate and prevent an incident.
Where selected security controls have not been implemented, have executive leaders / system owners formally (documented) accepted the risk associated with operating their system with sufficient control?	NIST 800-53 r3	Chapter 3, Page 17 Appendix F-CA, Page F-36 Appendix G, Page G-5	4	Leaders need to know the risks of the system to appropriately budget and also know the potential organizational impact for a systems operation.
Do you have a documented plan outlining periodic reviews of system risks and, in turn, a formal authorization process to operate a system?	NIST 800-53 r3	Appendix F-CA, Page 36-37	2	Documentation will help ensure risks are reviewed.



GA PII Checklist

(Centralized Logging and Review)

Question	Reference	Page	Security Impact (5 = highest)	Comment
Do you employ an audit and accountability strategy for systems whereby events are automatically logged and searchable?	NIST 800-53 r3	Appendix F-AU, Page F-24-31	3	This provides deterrence and after the fact assistance for compromises.
Do all of your systems create system log entries of all events (e.g., successful login, failed login, file / folder access, database access, etc.) that are then reviewed by members of your technology system security team for possible system / application security breach attempts?	NIST 800-53 r3	Appendix F-AU, Page F-24	3	This provides deterrence and after the fact assistance for compromises.

GA PII Checklist

(Change Management / Control)

Question	Reference	Page	Security Impact (5 = highest)	Comment
Do you have a staffed, documented system configuration management control process ensuring that all changes to the configuration of a system are evaluated?	NIST 800-53 r3	Appendix F-CM, Page F-38	5	Hardened configurations are essential to keep holes closed that could result in a security compromise.

GA PII Checklist

(Disaster Recovery / Business Continuity)

Question	Reference	Page	Security Impact (5 = highest)	Comment
Do you have a comprehensive, updated, recently evaluated contingency plan?	NIST 800-53 r3	Appendix F-CP, Page F-47-48	2	Although our main emphasis is maintaining confidentiality and integrity of data, availability is another business concern.
Have you successfully tested the full-spectrum of system identified in the contingency plan?	NIST 800-53 r3	Appendix F-CP, Page F-49	2	Although our main emphasis is maintaining confidentiality and integrity of data, availability is another business concern. Testing will provide the confidence that your system can be reconstituted when needed.

GA PII Checklist

(Physical Security)

Question	Reference	Page	Security Impact (5 = highest)	Comment
Do you have an enforced policy regarding physical / environmental protection of computer systems, applications, and data?	NIST 800-53 r3	Appendix F-PE, Page F-76	5	Physical and environmental security can impact the confidentiality, integrity, and availability of data.

By signing this, I am certifying to the best of my knowledge the accuracy and validity of the information security measures employed by my organization.

Signature: _____

Date: _____

Contact Information

We appreciate your feedback and comments. We can be reached at:

- Phone: 202-377-3508
- Email: bridget-anne.hampden@ed.gov