

Education/Awareness Subgroup

July 15, 2008

Discussion Items

D1. Don explained his reasoning for convening this lengthy meeting in order to accomplish some immediate tasks to assist Mark and his office in responding to agreements with Brad and President McRobbie in the area of security.

D2. Don talked about “the imperative” and the original letter Mark sent out to IUIE users to increase their awareness regarding security of data and to get them to sign a user agreement. This new audience is a different audience from the original communication; this is enterprise data users who were not covered in the IUIE audit.

D3. We need to discuss the outcome we are striving for in this communication. Suggests that the group not wordsmith the document but concentrate on the outcomes. Don clarified the group we are talking about for this communication. “Systems” is a difficult term for many users to understand. That means we need a new designation for the title of the communication; Dan asked if we could just list the systems. No IUIE users are included in the list that Mark has for this group.

D4. Beth Cate posed the question why we just don’t require ALL Indiana University Employees sign off on this type of agreement. We know who the “enterprise applications” users; others may not quite understand the intent of this communication. Merri Beth noted that we found over 400 people who had IUIE access who did not need it; this helped us clean up the IUIE user base. We will have to take Beth’s approach at some point, but we still may need to find a way to capture the “enterprise application” users group first.

D5. Don suggests that we need to do this in layers; you don’t want to overload people with too many communications though. Merri Beth brought up the need to put something in the original set up for network ID that requires them to sign such an agreement. Mark says that this group could add this requirement to the Accounts Management process. This would require some time to work out technically, so we could go forward with the communication to “enterprise application” users while the new process is worked out.

D6. Marilyn voiced concern about how to educate users about what they have access to and whether or not they have access to sensitive information. USO/UPO thinking about putting information in the OneStart area showing what people have access to. This, however, will take quite some time.

D7. Mark noted that many times users do not know they have access to applications because they have it through another application. We will eventually find these people once we get to the point of taking access away because people do not sign the use agreement.

D8. The current draft does not require people to respond and acknowledge receipt. This was due to the fact that all of the IUIE communications went to Mark; this is not realistic. How do we want to handle this part of the process?

D9. Don posed the question as to whether or not we have to wait to start the process until we have a list of all of the applications; the group felt we could at least list the major applications. Don posed the question as to what enforcement method Mark's office has. Merri Beth listed the applications we are discussing:

--Historically CDS Procedures used--

Follow up - IUIE

Enforceable HRMS – all

FIS – non-self service users

TIME – approvers role only

SIS – non-self service users

EPIC – certain roles TBD only

MMS

--NEW--

Non-enforceable ERA

Library – excluded because users have never required the standard enterprise user agreement

D10. Don proposed the blue labels above. At some point we could send the list of names of people who have not complied and send them to a responsible agent in each department or campus for enforcement. Dan indicated that he felt this list should go to the appropriate Data Steward for enforcement. This would help strengthen the ties between Data Stewards and Data Managers.

D11. Don proposed that we exclude the outcome we had with IUIE to discover those users who do not need their access any longer. This could be a follow-up outcome to all users. Merri Beth proposed separate communications which leads to more noise that users can absorb. Tom articulated that we actually have two goals: 1) to determine if users still need access to a given application, and 2) to be sure they have a signed user agreement. This would therefore include IUIE users who have access to these enterprise applications. Can we do this with one communication or do we need two separate communications?

D12. Mark asked for an extract of all enterprise users who do not have a user agreement on file. This is not the population we want now. We so need to use the same process we used with IUIE in order to

comply with what the IUIE Audit requested action on. Dan proposed sending communications to two populations: 1) Have use agreement on file, but need to know if they need access to enterprise applications, and 2) Do not have use agreement on file (must do this), and need to know if they still need access to enterprise application.

D13. As a wrap-up the group reviewed the details in the new communication.

1. Okay
2. Mark's office will send follow up on website mentioned here. Add how to remove sensitive data.
3. Pretty clear-cut; does this need clarification? Can we feasibly clarify this in this type of communication? Might add that you have your LSP help you do this.
4. Somewhat more controversial because some departments do not have a secure file server. UITS has a charge for their file server service though. There is a possible mechanical issue, but not something we shouldn't say. Policy statements are using the term unit instead of department. We will take a closer look at this, as some use the term org or organizational unit.
5. This is an unequivocal statement; in the Issues Notice it says this. We need to agree that we have standing to say this. The Board of Trustees issued a resolution May 2001 to give the OVPIT to make and implement policies (see notation on UPO page). One could argue that this gives us the authority to issue such an edict. Add instructions or link to tell people how to encrypt. There are some technical issues; nothing really convenient right now to make it easy. Grades are one major issue with faculty; it's hard for faculty to understand the reason for the edicts surrounding this data. This statement needs to be "word-smithed".
6. This is okay. If they don't do this, we will know that they haven't done this.

D14. Dan suggested and the group agreed that we should refer to non-computerized data as well. We will look into how to do this; it might be in a separate communication.

Second Agenda Item – Road Map Discussion

D1. Review of roadmap document prepared by Merri Beth and Scott. This will help this group determine the types of things we are responsible for and how we might move forward. There are two different ways of looking at the same information. They took a survey as well; this is the chart in the documents. These are the two tools. 1 to 5 takes us from where we are to where we want to get to. The roadmap tool is a process; this can indicate where this information comes from. The chart indicates the type of constituencies and examples of the types of activities that exist today. Within the security field these activities are the accepted pieces of awareness and training. [See notes from last meeting.](#)

This chart includes the types of activities included in each of the 4 phases. Used answers to the survey to assist in these categorizations.

D2. Don wants us to assess where we have priority gaps; don't know what that means yet. Merri Beth mapped this; we are not assessing the quality. This is just a snapshot too. The value of this committee

is to do some risk assessment. Which of these cells have the highest priority? What should be in cells if there is nothing there?

D3. Mark indicated that the matrix is going to be bigger, so we must determine which rows we want to deal with first. Dan asked if all of the rows are correct. What about affiliates for instance? Don wants to deal with things in manageable pieces first. So, let's validate the rows first. Mark noted that the chart is "system" based rather than "data" based. Beth and Mark noted that all users of student data, either through the SIS or elsewhere must be communicated with.

D4. Don suggests that we start as simple as possible, so maybe change the designation from systems to data. Add Affiliates as an additional bold in the chart or non-employees (affiliate, contractors, and students). For now we are going to remove departments; use data type.

D5. Merri Beth listed the types of data we should include:

DATA	ROLES/CONSTITUENCIES	TOOLS
Student	Employees	
-Grades	-Faculty	
-SSN	-Fulltime Appointed	
	-Hourly/Student	
	-LSP's	
HR		
-SSN		
Research		
-SSN		
Health		
-SSN		
Financial		
-Credit Card #		
-SSN		

Merri Beth will redo the chart based on these discussions so the subgroup can determine how to proceed. Where does the data exist and what tools exist? Then deal with types of users and how to communicate; training, awareness, etc.

D6. Mark explained how the new chart would be constructed. Don suggested we look at this in separate exercises. Need a row for each of the major data steward categories of data. We need to

begin with fairly broad categories and see how the instrument works. Scott suggested that we will discover whether or not we need to get more granular by crafting communication messages.

D7. What are the 3rd-rail data elements (phrase coined by Mark)? RED HOT (cause harm e.g. financial, identify theft, sever penalty (jail, fines)) SSN, Bank # (PIN), CC#, Driver's License, Health Info (PHI), student loan information, passport/visa numbers, confidentiality in contract, passwords/passphrases vs. embarrassing/harmful to our reputation or persons = restricted.

D8. Merri Beth passed out an additional chart with the answers, either A or R.

Action Items for both agenda items

A1. Put on the CDS agenda for next time a discussion of adding use agreement to Accounts Management such that all IU employees must sign in order to get an account.

A2. Make UA required at time of new employment

A3. Make tool to see all systems a user has access to

A4. Make UA expire at X interval and automatically e-mail person to do again.

A5. Mark will take the proposals from this meeting and come back with proposed communications for approval.

A6. CDS should reaffirm the Notice to give it enforcement capability.

A7. We will go back and draft these two versions ready as soon as possible.

A8. Next steps – Deliverables from Mark's office:

1) Only show data categories on the chart – use same columns

2) A document that identifies the green items above in the best way possible; take this as far as possible before our next meeting.