

INTRODUCTION TO THE SPIA PROGRAM

We have all come to appreciate the amazing opportunities that information technology (IT) offers Penn to better serve our teaching, research, and service mission. As a complex and dynamic organization, Penn has launched new IT applications and created databases and reports that enable faculty, staff and students to achieve new learning more efficiently and effectively.

We understand that information technology also creates risk -- one prominent area of risk being the difficulty of understanding and addressing internal and external threats to confidential, personal or proprietary data that, if compromised, could cause significant harm to individuals or to Penn. Consider some of the types of harm that can result from failure to adequately protect confidential data.

- Identity Theft
- Stalking / Harassment
- Damage to University Reputation
- Disruption of Operations / Services
- Legal Liability
- Regulatory Fines

Federal and state laws, industry practices, and principles of data stewardship have all driven home the fact that individuals who create, use, or maintain Confidential University Data are responsible for adequate protection of that data. The Security and Privacy Impact Assessment (SPIA) program is a resource to help each School/Center better understand what threatens the data in its computing applications and databases, where the greatest vulnerabilities exist, and what safeguards can be implemented. SPIA helps these organizations collect an inventory of their computing applications and databases, create a three-year plan for conducting risk assessments, and then complete detailed risk assessments according to the schedule developed by that organization. The tool offers suggestions for what safeguards may be appropriate in order to mitigate the most common threats and provides a reporting template to help synthesize the learning and proposed changes that result from the SPIA process.

It is important to note that SPIA is not a mandate that requires that all mitigation strategies be implemented. Rather, it is a roadmap to help organizations identify areas of risk and select appropriate strategies and timeframes to mitigate those risks.

How does SPIA work?

SPIA is broken out into five basic steps:

Step 1: Inventory applications and databases with Confidential University Data (see definition in Instructions) and create 3-year plan for conducting detailed risk assessments on a per-application/database basis. For each application/database, follow Steps 2-4:

Step 2: Assess current risks to existing applications and databases.

Security and Privacy Impact Assessment

Step 3: Identify safeguards you plan to implement.

Step 4: Revise risk levels based on planned implementation of safeguards.

Step 5: Develop executive summary to synthesize learning and plans for your School/Center.

What if I don't like everything about the tool?

SPIA is a tool for organizations looking for an approach to meet their responsibility of reasonably protecting confidential data. SPIA can be tailored to fit the needs or wishes of any organization. Each School/Center may modify the tool as they deem appropriate to meet the basic objective of understanding what data exists, evaluating current protections, and taking appropriate steps to mitigate priority risks.

For example, if an organization manages several applications on the same server and under the same conditions, the organization may group them into a single assessment.

How do I Get Started?

Again, a complete SPIA process involves the five steps listed above. Before beginning, make sure you have the following important documents. These can be found at the following site: <http://www.upenn.edu/computing/security/spia/> .

- [the Summary of School/Center Approach](#), to assist you in organizing for initiation of the program.
- [the Instructions](#), to guide you through the critical thinking and steps necessary to complete the program.
- [the Inventory Sheet](#) in Excel form to complete Step 1
- [the Risk Assessment Sheet](#) in Excel form to complete Steps 2-4.
- [the Executive Summary](#) in MS Word form to complete Step 5.
- [the Tracking Tool](#) to assist you in aggregating key program information over time.

IT IS IMPORTANT TO READ THROUGH THE INSTRUCTIONS AT THE OUTSET TO GAIN AN UNDERSTANDING OF THE OVERALL PROGRAM.

What if I need help?

The Office of Audit, Compliance, and Privacy, and Information Systems and Computing (ISC)'s Security Office are available to assist you with the use of the tools and in applying them to any areas within your School/Center. If you have questions, please write to spia@pobox.upenn.edu.

INSTRUCTIONS FOR SPIA PROGRAM

Preparation Stage

The efficiency and effectiveness of this program hinge largely on the initial planning and preparation that take place. For example, Step 1 calls for development of a complete inventory of applications and databases within the School/Center. In order to develop this inventory efficiently and accurately, it is crucial to have the right team in place. Depending on the size of the School/Center, this could mean including on the team the two or three individuals most familiar with operations and information systems in the organization, or forming a much larger team that reports information to a single project coordinator. Good planning in the team formation stage can avert significant lost time, and lead to more complete results.

In view of the importance of sound preparation, a [Summary of School/Center Approach form](#) has been developed to provide guidance for the program initiation steps.

STEP 1: Inventory

Name Your School / Center

Using the STEP 1 [Inventory Worksheet](#), start by identifying your school or center at the upper left corner of the sheet. You may break this up at whatever organizational level you feel appropriate for your School or Center. Then prepare to inventory your applications and databases.

Inventory Your Applications/Databases – Create the List

The inventory of applications/databases is the first major task and provides the basis for identifying where to conduct your risk assessment. The purpose of the inventory process is to make sure all systems containing Confidential University Data¹ are identified and scheduled for a detailed risk assessment.

¹ Confidential University Data includes:

* Sensitive Personally Identifiable Information – Information relating to an individual that reasonably identifies the individual and, if compromised, could cause significant harm to that individual or to Penn. Examples may include, but are not limited to: Social Security numbers, credit card numbers, bank account information, student grades or disciplinary information, salary or employee performance information, donations, patient health information, information Penn has promised to keep confidential, and account passwords or encryption keys used to protect access to Confidential University Data.

* Proprietary Information – Data, information, or intellectual property in which the University has an exclusive legal interest or ownership right, which, if compromised could cause significant harm to Penn. Examples may include, but are not limited to, business planning,

The scope should include applications and databases containing Confidential University Data that your School/Center is directly responsible for designing, managing, administering or operating. This may include data sets that are stored on individual desktops, laptops, or other portable devices and is not limited to large, more centrally-supported applications and databases.

As for central systems, generally Schools/Centers will not be responsible for listing or assessing University-wide applications and databases containing Confidential University Data that the School/Center is not responsible for designing, managing, administering, or operating (example: Schools that use BEN, Payroll/Personnel, Advancement, SFS, Penn InTouch, Advisor InTouch, Penn Portal need not list those applications and databases). *However*, if your School/Center extracts data from these systems and manages that data in local databases, those should be included in your inventory.

In the column headed “Application/Database Name,” provide a name for the application or database. This may be an acronym or a few words that describe a computer system through which data is created, stored, and retrieved to support a business function.

Description of Each Application or Database

In the column headed “Describe Information,” provide some additional detail about the type of information being processed, received, stored, or transmitted. For example, is it personal health information such as medications, test results, diagnosis, appointments, or other confidential data such as social security, credit card, employment, contact information, biometric, GPS location? Is it mission critical information such as emails, budget/finance records, or time and attendance data?

In the columns under the heading “Where is the information?,” indicate the media used to receive, store, or transmit the information. Simply enter an “X” under the appropriate media description. If you select “Other Portable or Wireless Device,” or “Other Electronic Media,” describe the media under “Describe Information” (see preceding paragraph) if you think this may be useful later when completing the detailed risk assessment.

In the column headed “Describe the source of the data,” describe the source specifically (e.g., other department/operating units, University central system, an external business associate, vendor).

financial information, trade secret, copyrighted material, and software or comparable material from a third party when the University has agreed to keep such information confidential.

* Any other data the disclosure of which could cause significant harm to Penn or its constituents.

Security and Privacy Impact Assessment

In the column headed “With whom is the data shared?,” describe the destination of the information in specific detail (e.g., other department/operating units, external business associates, vendors).

In the column headed “Estimate the volume of data,” estimate the volume of data based on the subject of the data (i.e. number of students, patients, employees, faculty, research subjects). This is important from the perspective of prioritizing your risk assessment and mitigation activities. Use whatever quantifiable measures you think best apply. Again, this is intended to help you focus your efforts on the greatest areas of vulnerability so use it only to the extent it provides you with that perspective.

Scheduling Your Risk Assessments

At this point it is time to create a three-year schedule for conducting detailed risk assessments on each application/database. Based on completion of the Inventory Sheet, you will likely have a strong sense as to which applications/databases should be assessed first. Emphasis should be placed on reviewing those systems you believe (without the benefit of a detailed analysis) may be at significant risk, or those systems that very little is known about.

Consider data criticality, based on the nature and use of the information, when setting your priorities. Think carefully about the following two questions when evaluating data criticality:

- 1) What could be the impact on the subject of the information, the University, my School, or Center if the information fell into the wrong hands?
- 2) What could be the impact on the University’s operation if the information were no longer available or its accuracy compromised?

In the column headed “Fiscal Year Assessment Plan,” list the year (covering the next three fiscal years) in which you plan to conduct a detailed risk assessment for each application/database. It may be useful to consider at this time whether you have certain applications/databases that are managed similarly, under the same computing environments and standards. You may want to schedule the assessment of such applications/databases for the same fiscal year.

It is important to note that this step does not necessarily describe the year that risk mitigation strategies will be *implemented*. Rather, you are just targeting in which Fiscal Year a detailed risk *assessment* (not necessarily remediation effort) will be performed for each application and database in your inventory.

STEP 2: Assess current risks to existing applications and databases

In STEP 2, you are to assess the existing risks to each application/database using the Risk Assessment sheet. The sheet has a list of possible known threats. You will need to copy these rows for each application/database and complete the steps separately for each. (Note: If you have multiple applications/databases that you believe are managed and secured identically you may combine them when assessing them against the threats listed in the tool). The tool is designed to take your rankings of probability and consequence for each threat and automatically score the risk as either “High”, “Significant”, “Moderate”, or “Low”.

The threats already identified are broad and most likely cover all relevant types of threats as they relate to privacy and security. However, you may identify additional threats and safeguards and add those to the tool as you feel appropriate. Remember, this is a tool to help you identify and objectively rank your risks. Modify it as you deem appropriate to accomplish that objective.

When evaluating each threat against your application/database, first consider what safeguards you have already taken and in the column headed “Current State Safeguard” enter “C” for those safeguards that are currently implemented. Given this level of existing security, determine the likelihood or probability of the threat being realized. Rank “current state” probability based on the following definitions:

Score Threat

- 0 = Threat does not apply to this application/database.
- 1 = **Rare** – The event would only occur under exceptional circumstances.
- 2 = **Unlikely** – The event could occur at some time, but probably will not.
- 3 = **Moderate** – The event should occur at some time.
- 4 = **Likely** – The event will probably occur at some time.
- 5 = **Almost Certain** – The event is expected to occur in most circumstances.

Score Consequences

Once you have scored the current probability of each threat against each application/database, you need to evaluate the current potential consequences of the threat being realized. Again, consider the types of harm that might result from inadequate protection of Confidential University Data, such as:

- Identity Theft
- Stalking / Harassment
- Damage to University Reputation
- Disruption of Operations / Services
- Legal Liability
- Regulatory Fines

Security and Privacy Impact Assessment

Rank the consequence of the threat being realized based on the following definitions:

0 = Threat is not applicable to this application.

1 = **Insignificant** – Negligible impact on ability to plan and conduct business activities with minimal reduction in customer service, operational efficiency and staff morale. Very limited, or no financial/political impact.

2 = **Minor** – Minor impact on ability to plan and conduct business activities with minimal reduction in customer service, operational efficiency and staff morale. Minimal financial or political impact.

3 = **Moderate** – Medium impact on ability to plan and conduct business activities with a moderate reduction in customer service, operational efficiency and staff morale. Some financial or political impact is experienced.

4 = **Major** – Major impact on ability to plan and conduct business activities with significant reduction in customer service, operational efficiency and staff morale. Considerable financial or political impact.

5 = **Disastrous** – Comprehensive impact on ability to plan and conduct business activities with total disruption in customer service, operational efficiency and staff morale. Devastating financial or political impact.

STEP 3: Identify safeguards you plan to implement

For each threat, review those safeguards listed that you have not already implemented and enter an “F,” in the column headed “Future State Safeguard,” if you plan to implement the safeguard to reduce your level of risk for that threat.

Reminder: This step does not necessarily mean that you are implementing the safeguard immediately. You are identifying which safeguards your organization plans to implement in the future, and in comments, you can describe what those plans are.

STEP 4: Revise risk levels based on planned implementation of safeguards

Using your Risk Assessment sheet look at each threat one more time, now considering any safeguards you plan to implement to mitigate the level of risk. Using the same definitions for probability and consequence used in STEP 2, rank each threat again. This will create a revised risk value.

Once this is complete, look at the reduction in the level of risk resulting from the additional safeguards you plan to implement (i.e., compare Current State Risk Value with Future State Revised Risk Value). Consider any budgetary constraints or cost effectiveness issues as you identify the safeguards to implement in order to reach an acceptable level of risk.

The column at the far right of the sheet is available for comments and additional documentation you may have regarding implementation planning, target dates, special circumstances, etc.

STEP 5: Executive Summary

Each School/Center should complete Step 5 once each year. In the first year, this summary will capture the scope of databases/applications identified in your inventory (Step 1), as well as findings from your first year's detailed risk assessment (Step 2-4). In subsequent years, another executive summary should be completed to reflect detailed assessments conducted, as well as any updates to your inventory of applications and databases. To complete Step 5, you will need the Executive Summary-Word Document. This template has been provided to help you to capture the findings of your assessment at a high-level. The summary should provide the following:

- Description of the work effort and any key approaches, the resources used and the number of applications/databases assessed.
- Summary of the findings describing the areas of greatest concern, as well as highlighting successes in how information is currently being managed.
- Summary of any significant improvement plans, their timelines and budget implications, as well as specific outcomes in terms of reducing risk, including quantitative measure, if known.
- Summary of any key learning from the process and any follow-up steps pertinent to future assessments.
- If this is not your first year participating in the SPIA program, please provide an update on the status of prior-year improvement plans. If this is your first year participating in the program, you may omit this part of the process.

The completed Executive Summary is to be approved and signed by the Senior Business Administrator and the IT Director of the School/Center.

The SPIA Coordinators for the School/Center may find it helpful to use a team approach for development of the Executive Summary. For example, if five applications are being assessed the Coordinators may wish to obtain a separate executive summary for each application, from the individuals who are most familiar with the respective applications; then the Coordinators can "roll up" the five individual summaries into one all-inclusive Executive Summary for the School/Center.

Reporting Process

The Executive Summary for the School/Center, signed by the Senior Business Administrator and the IT Director, should be reported to:

- The University's Office of Information Security and
- The Office of Audit, Compliance and Privacy..

The purpose of the reporting is to:

SPIA

Security and Privacy Impact Assessment

1. Ensure that the School/Center understands where Confidential University Data resides, the risks involved with regard to such data, and safeguards to help mitigate the risks.
2. Provide an opportunity for School/Center IT and business leadership to review the assessment and provide feedback.
3. Provide central IT and other leadership the ability to learn about trends in risks and solutions and to identify when a central solution might be appropriate.

Tracking Tool

Because the SPIA program involves processes that continue from one fiscal year to the next, a Tracking Tool is provided to facilitate management of the program steps for Schools/Centers. Use the Tracking Tool to aggregate key information on each application/database being assessed in your School/Center, including planned fiscal year for detailed risk assessment; whether the detailed assessment has been completed; and whether the Executive Summary has been submitted. The tool is provided as a support for the SPIA Coordinators in the School/Center, and need not be submitted under the reporting process outlined above.