Quick Guide to Completing the Security and Privacy Controls Questionnaire (SPCQ)

This Job Aid is designed to help you understand how to complete the Security and Privacy Controls Questionnaire (SPCQ).

This is a quick guide to completing the Security and Privacy Controls Questionnaire; for more in-depth information, and links to assist you in implementation of required security measures, please refer to the Security and Privacy Controls Questionnaire Review slide deck (PowerPoint).

Mandatory Security Requirements:

- Password Management
- Patch Management
- Virus Protection
- Security Controls
- Wireless Access Requirements
- System Log Review
- Encryption for Electronic Storage of DHS/HFS Data – Best Practice!
- Visitor Log or Visitor Escort (if printing/storing Data)
- Training
- Contract Submission for IT/Shredding Vendor

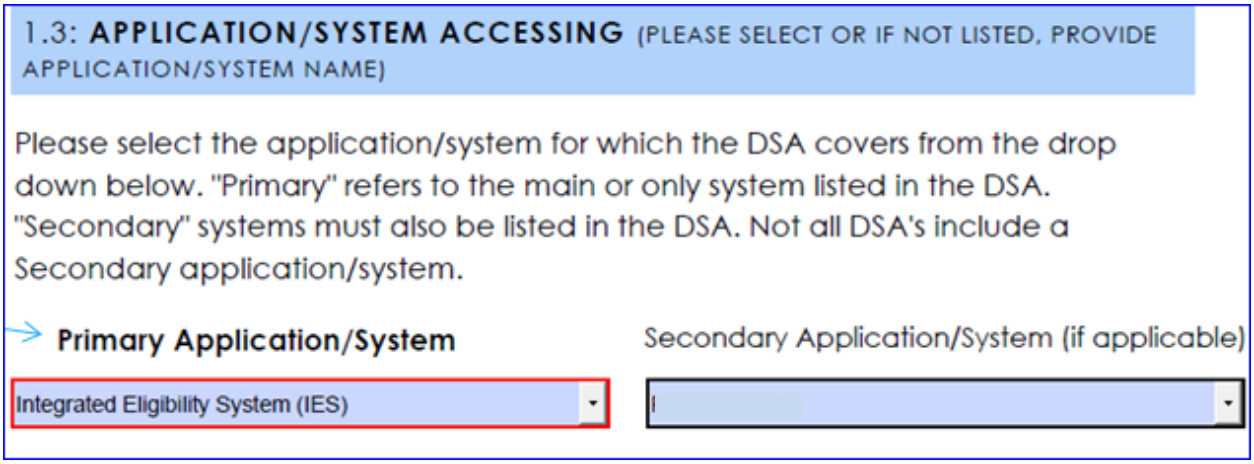
Tips and Hints to Completing the SPCQ:

- Required security controls have a **RED** outline – if you hover over a red button it will give you additional information!
- Answer ALL required questions! – Missing information on the form or leaving a required security question unanswered will result in the SPCQ being sent back to your agency for further revision!
- If none of the boxes within a subsection apply for your agency, use the “Additional Information” box to tell us how you fulfill requirements for that section.
- Formatting Workarounds:
    - When you print your document, some of the ‘Additional Information’ you typed in the narrative box may be cut off. If necessary, please insert additional pages that allow you to provide detailed explanations.
    - You should include your detailed responses directly after the page where you would have entered the information. Be sure to state the Heading/Section/Question and page you’re referencing.

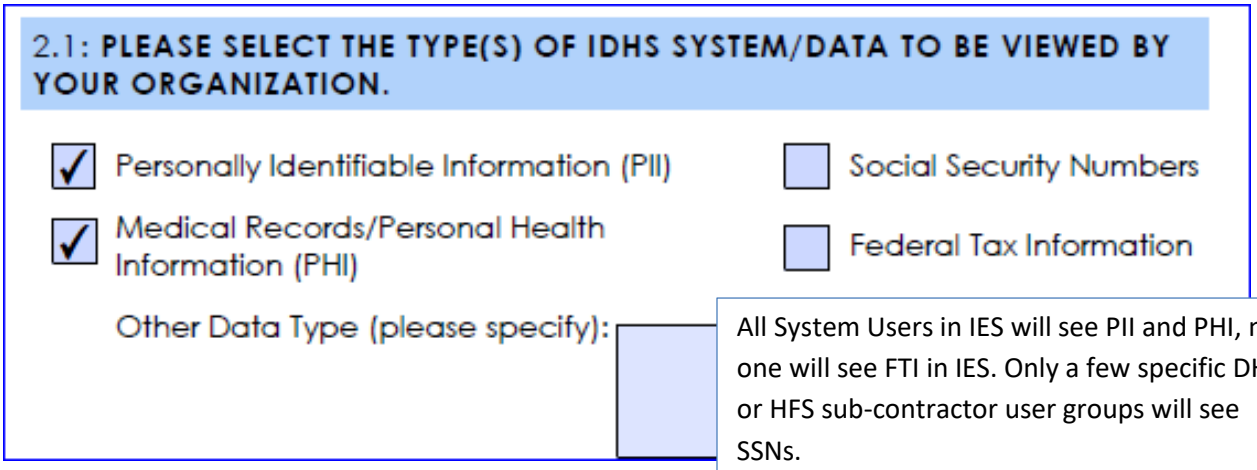
Quick Guide to Completing the Security and Privacy Controls Questionnaire (SPCQ)

Section 1 What System?

If you need current information, you will use the **Integrated Eligibility System**; if you **require** historical information (prior to 10/01/2017) you will also complete the Secondary Application/System and select PACIS-ACID and PACIS-ANQR using the Additional Application/System box).



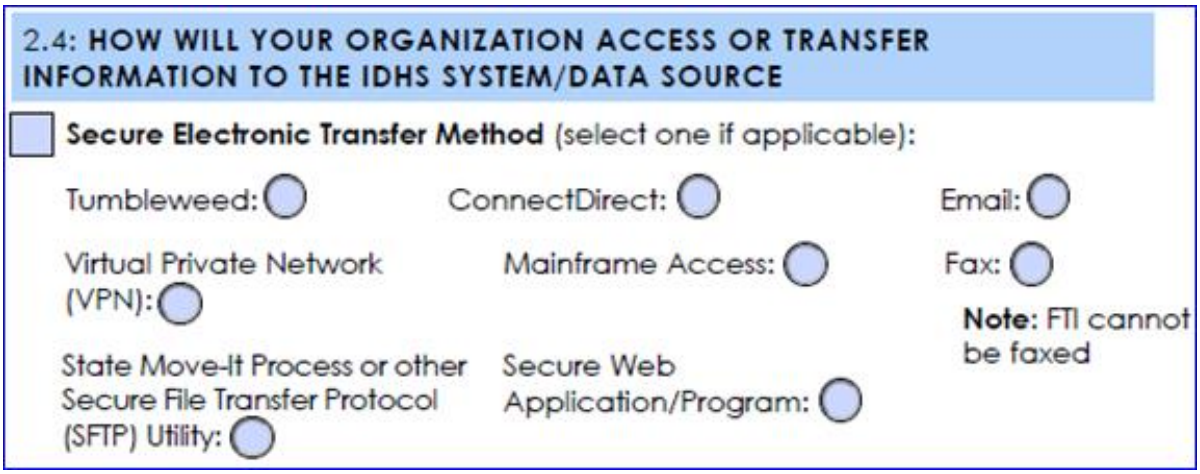
Section 2.1 PII and/or PHI?



All System Users in IES will see PII and PHI, no one will see FTI in IES. Only a few specific DHS or HFS sub-contractor user groups will see SSNs.

Section 2.4 Data Transfer Method

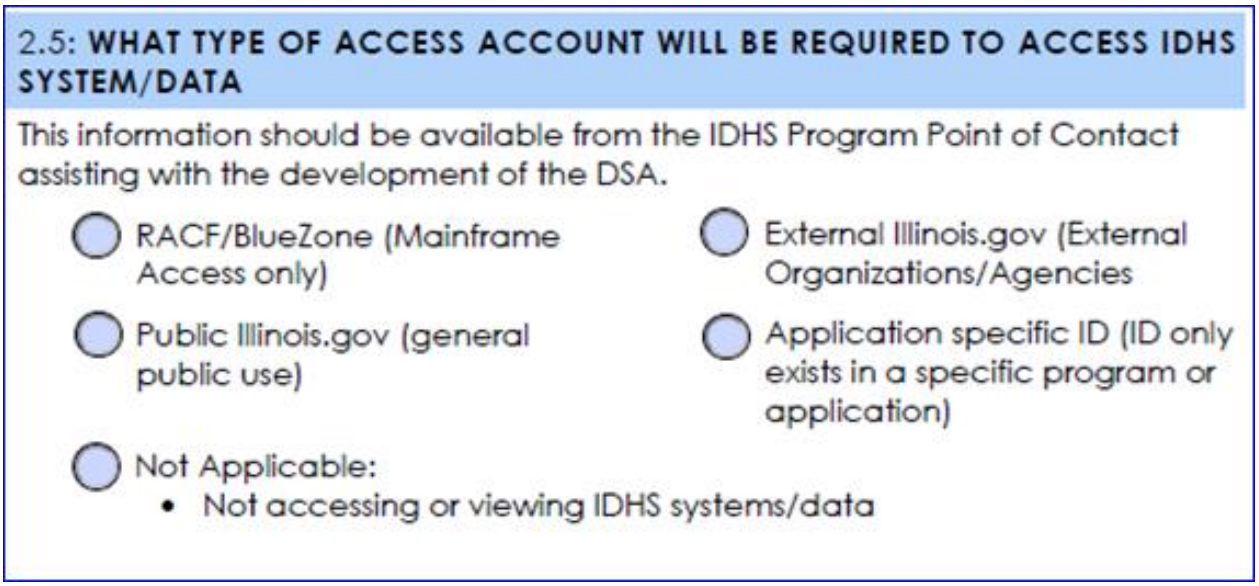
If you will access IES only, choose "Secure Web Application/Program", if you will access PACIS also choose "Mainframe Access"



Section 2.5 Access Account Type

Quick Guide to Completing the Security and Privacy Controls Questionnaire (SPCQ)

External Agency IES users will choose External Illinois.gov, PACIS users will also choose RACF/BlueZone

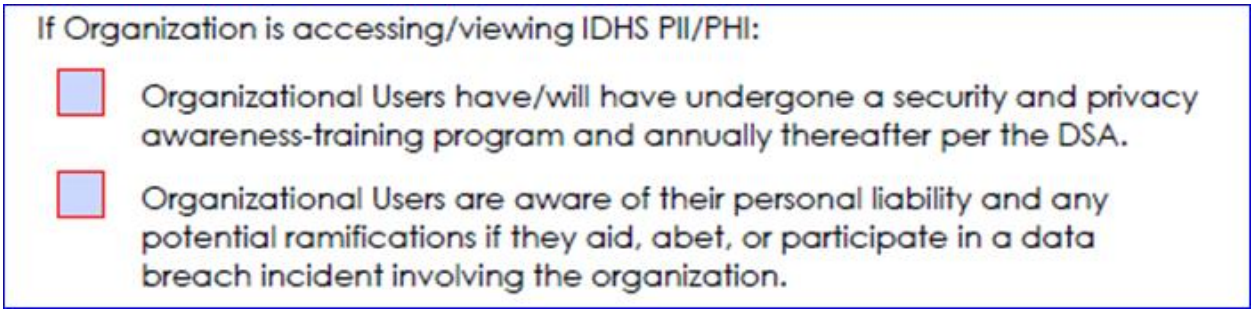


Section 2.6.5 Secure Storage of IDHS/HFS Data

Security of the Data you are viewing, downloading, storing and destroying must be implemented from start to finish! Remember, this information is private and should be protected at all times. Destruction/disposal of paper documents **MUST** be in compliance with the Data Sharing Agreement. If you are using an external vendor for shredding, you must submit a copy of the contract you have with the shredding company – this contract should include confidentiality language.

Section 3.2 Security and Privacy Policies

ALL IES and PACIS users will view PHI and PII. As indicated by the Red outline, these must be checked it order to comply with your Data Sharing Agreement.



Section 4.2 Password/Account Management

Identity of Individual Users MUST be verified by Government/state/student picture ID – This is generally done upon initial employee hire. This ID must be kept on file for auditing purposes.

You must have security measures in place for managing individual user accounts/passwords at your agency. Industry Best Practice recommends the following:

- Reset passwords: 30/60/90 days
- Disable an account after 60 of days of inactivity

- Delete accounts after 90 days of inactivity
- Review accounts annually
- Password criteria: Minimum of 8 characters in length and at least 3 of the following:
- Uppercase, lowercase, number, special character.
- 3 login in attempts before lock out
- Applications/session termination after 15 minutes of inactivity

Section 4.3 Required User Documentation and Training

Training Attestation Forms, Confidentiality Statements, and a picture ID of each IES User must be kept on file at the agency for audit purposes. Both Security Awareness and HIPAA Training are required as all system users will see PII and PHI in IES.

All forms and training can be accessed at the DHS IES TransitionCenter
http://www.dhs.state.il.us/page.aspx?item=76603

Section 5: System and Network Security (Your Agencies System!)

Requirements:

- Patch Management
- System Updates
- Virus Protection
- If your networks is wireless – it must comply with federal standards

For more information on federal standards and links on Patch Management tools, refer to the Security slide deck.

Section 7 Security Controls Testing and System Compliance

Requirements:

- Testing of security and privacy controls and system log reviews are a requirement. You cannot just check this box, you need to tell us through the sub boxes or additional information boxes how you achieve this requirement. Additional information on how to implement these is available in the Security slide deck.

Section 8 Security Incident Handling and Reporting and Compliance

All of these measures are requirements of the Data Sharing Agreement and you must comply with these.

Signature Page

Both pen and ink and digital signatures are now accepted on the Security and Privacy Controls Questionnaire.