Chapter 14

Securing Forms & Copyright Protection

Adding security to forms to prevent users from changing the form. Should you copyright your forms?

Chapter 14

Securing a form is protecting the form against changing its appearance and content. For eForms, all forms should be secured without exception. Even the most basic forms requiring no more than a signature should be secured and protected against changing the form contents. Any content displayed on government websites and available for public consumption should be considered a target for security and protection. This rule should extend to every document a government website hosts even those documents not considered forms.

IN THIS CHAPTER

Securing a PDF Document

Acrobat provides several opportunities to secure PDF files. You can use Acrobat Security, you can use a 3rd party solution for securing files, you can use in-house security options developed by your IT department, and you can certify PDF files.

The simple and easy method for applying security is handled by Acrobat Security. For the purposes of this book I'll address Acrobat Security but I encourage all readers to search for solutions acceptable for your branch of government. There may be mechanisms in place now in your agency for securing documents including PDFs. You should spend some time researching security options available to your department.

Applying security to a PDF is handled in the Document Properties. You can secure files protecting certain activities while granting permissions for a number of other activities. These choices are found in the Acrobat Security window.

To secure a PDF form, do the following:

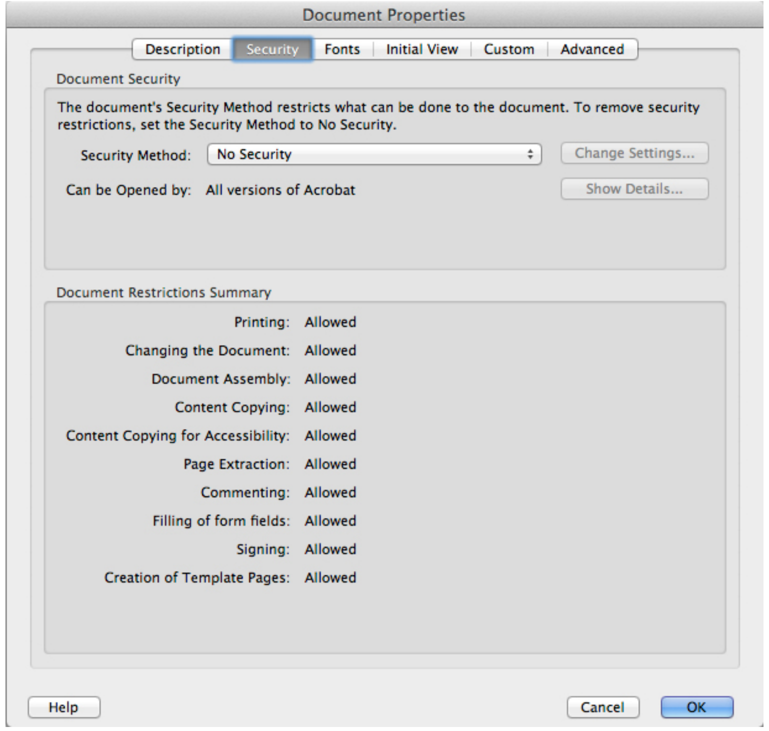
1. **Open the form in Acrobat.**
   Securing a document is the last step you perform before deploying a form. You should test the form, be certain the form is assembled properly and ready to deploy.

2. **Save a copy of the form.**
   Saving a copy compacts the file and eliminates any overhead not needed for the form to be opened, populated, and returned to you. As you add form elements, copy/paste fields, delete fields, etc. during an editing session, Acrobat retains unnecessary information and file gets bloated. Rewriting the file by saving as a new file compacts the data and often results in a smaller file size. In addition, you want to secure the form you deploy while maintaining the original unsecured form on a secure intranet not available to the public.

3. **Open the copy you save and open the Document Properties.**

   Press CTRL/Command + D or choose File ➤ Properties to open the Document Properties window.

Figure 14.1 Document Properties



Document Security

The document's Security Method restricts what can be done to the document. To remove security restrictions, set the Security Method to No Security.

Security Method: No Security

Can be Opened by: All versions of Acrobat

Document Restrictions Summary

Printing:	Allowed
Changing the Document:	Allowed
Document Assembly:	Allowed
Content Copying:	Allowed
Content Copying for Accessibility:	Allowed
Page Extraction:	Allowed
Commenting:	Allowed
Filling of form fields:	Allowed
Signing:	Allowed
Creation of Template Pages:	Allowed

Click the Security tab in the Document Properties window.

4. **Choose a Security Method.**
   Click the Security tab. From the Security Method drop-down menu you see several options for securing the document. For the purposes of this discussion we look at Password Security. Unless you have another security method in place, this security option will work well for the eForms you deploy except documents related to national security.

   From the menu options choose Password Security. The Password Security window opens.

5. **Adding Restrictions.**
   Be certain to not check the box for Require a password to open the document. Checking this box requires the constituent to know a password in order to open the PDF in Adobe Reader. The eForms you host won't require people knowing a password to open the forms.

   Check the box for Restrict editing and printing of the document. A password will be required in order to change these permission settings. When you check the box, options you find in the Password Security – Settings window are made available to you.

6. **Disallowing Printing.**
   The first item to address is whether you want the end user to be able to print the form. This may be a matter that needs some discussion in committee. You can force constituents to follow your lead in achieving sustainable measures by disallowing printing. Or you can provide users the ability to print files for their own personal filing system. If you do restrict printing, you should create a webpage that explains the fact that no forms can be printed, they must be handled electronically, and your reasoning for not permitting printing.

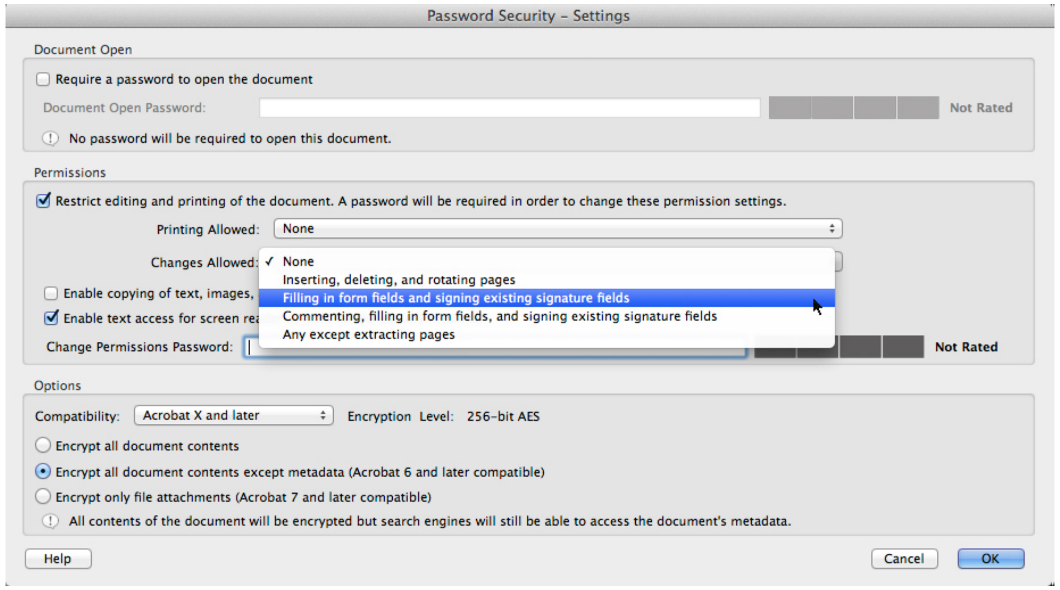
7. **Enable Form Fill-In.**
   From the Changes Allowed drop-down menu choose *Filling in form fields and signing existing signature fields*. You must enable this permission or users won't be able to fill in the form.

8. **Enable text access.**
   By default the item for *Enable text access for screen reader devices for the visually impaired* is checked. You should leave this item enabled so your forms meet with accessibility standards and permit users with screen readers the ability to complete your forms.

9. **Change Permissions Password.**

   This is where you add password security to your form. On the right side of the text box is a scale that measures the strength of your password. Typing a few characters results in a weak password. Using upper and lowercase characters, numbers, and certain symbols results in a password with more strength.

Figure 14.2 Password Security Settings



Password Security – Settings

Document Open

□ Require a password to open the document

Document Open Password: Not Rated

(!) No password will be required to open this document.

Permissions

☑ Restrict editing and printing of the document. A password will be required in order to change these permission settings.

Printing Allowed: None

Changes Allowed: ✓ None

Inserting, deleting, and rotating pages

Filling in form fields and signing existing signature fields

Commenting, filling in form fields, and signing existing signature fields

Any except extracting pages

□ Enable copying of text, images,

☑ Enable text access for screen rea

Change Permissions Password: Not Rated

Options

Compatibility: Acrobat X and later Encryption Level: 256-bit AES

○ Encrypt all document contents

● Encrypt all document contents except metadata (Acrobat 6 and later compatible)

○ Encrypt only file attachments (Acrobat 7 and later compatible)

(!) All contents of the document will be encrypted but search engines will still be able to access the document's metadata.

Be certain to enable form fill in and signing existing signature fields.

10. **Compatibility.**

    From the menu choose Acrobat X compatibility. This encryption level is much stronger than earlier versions of Acrobat compatibility.

    Check the box for *Encrypt all document contents except metadata (Acrobat 6 and later compatible)*. This box should be checked so your forms can be found using Internet search engines.

11. **Click OK.**

    When you click OK you are prompted to re-enter your password. Type the password exactly the same as the password you supplied in the Change Permissions Password text box.

12. **Save the file.**

    The security settings are not added to the document until you save the file.

Cataloging Passwords

One of the best ways to keep a record of passwords for PDF files in your department is to create a PDF form where new passwords are stored. You can encrypt the file with password security for opening the document. Once open, you can perform a search with Acrobat Search to find document form numbers and passwords associated with them. Keep this file on a secure intranet server where only the forms design departments have access.

Storing passwords in an encrypted file requires users to know only one password to open the PDF. When a user opens the file, the user has access to all passwords used on the forms you list in the file.

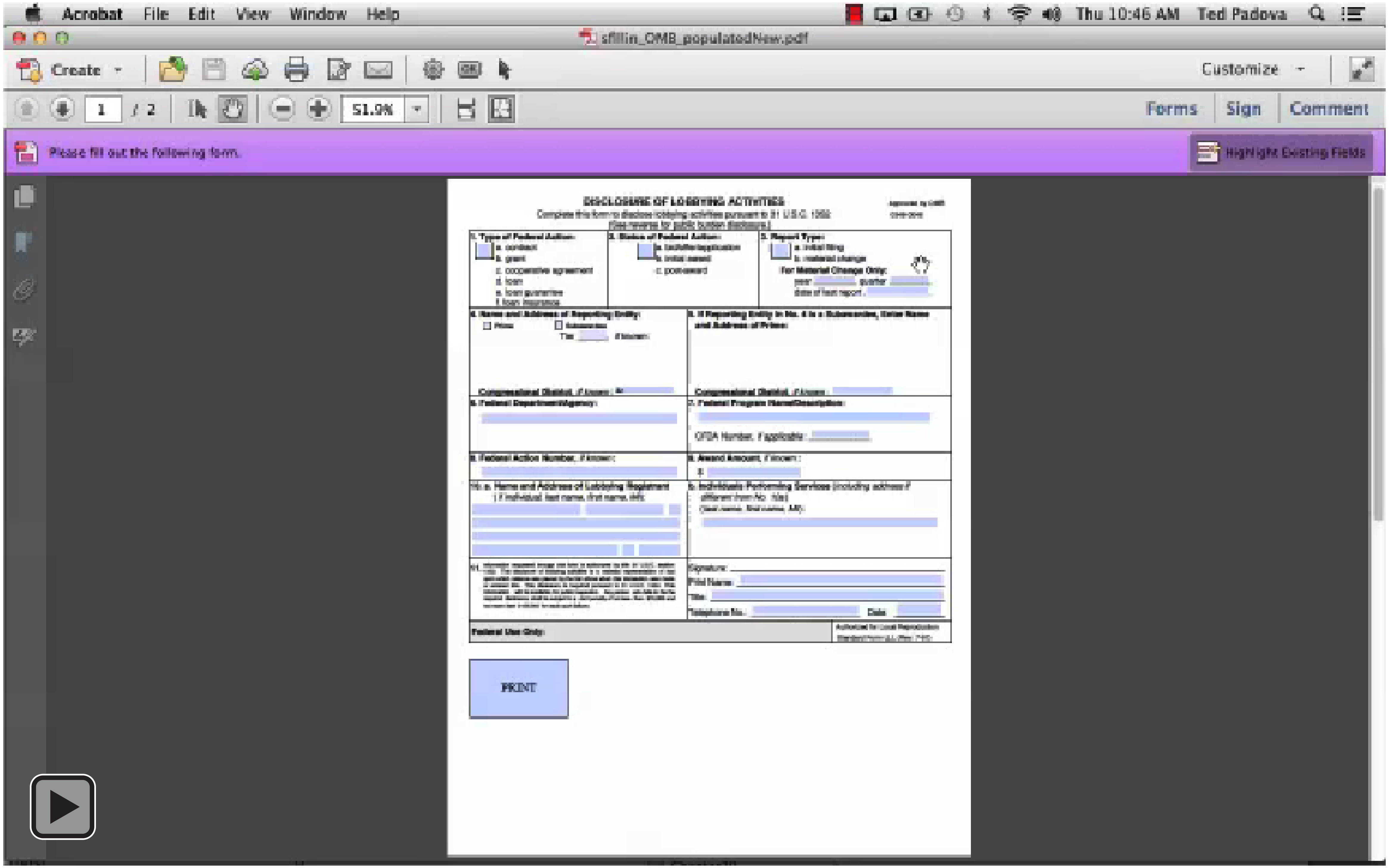
Copyrighting Forms

Almost all forms on USA Federal government websites are considered to be in the public domain and therefore do not carry copyright protection unless specifically noted on the form. US States vary according to policies established by the states. Many US State forms are copyrighted and cannot be reproduced or displayed in any content whether printed or online.

This is a matter for your office to decide. Unless you have specific reasons for doing so I would recommend you not copyright forms —especially if you're proud of the forms hosted on your site. Your web content may be assessed and evaluated by magazines, reporting agencies, and studies that examine developments in use of eForms. Independent researchers can benefit by showing the community of government offices examples of well-designed and functional eForms.

If your forms are scanned documents, have no fields, no department seals, and designed poorly, by all means, copyright your forms. You don't want samples of your forms appearing in a study by ComputerWorld!

Movie



DISCLOSURE OF LOBBYING ACTIVITIES

Complete this form to disclose lobbying activities pursuant to 31 U.S.C. 1352

(See reverse for public burden disclosure.)

Approved by OMB

[illegible]

1. Type of Federal Action:
   - a. contract
   - b. grant
   - c. cooperative agreement
   - d. loan
   - e. loan guarantee
   - f. loan insurance

2. Status of Federal Action:
   - a. bid/offer/application
   - b. initial award
   - c. post-award

3. Report Type:
   - a. initial filing
   - b. material change

   For Material Change Only:

   year ____ quarter ____

   date of last report ____

4. Name and Address of Reporting Entity:

   □ Prime □ Subawardee

   Tier ____, if known:

   Congressional District, if known: 4c ____

5. If Reporting Entity in No. 4 is a Subawardee, Enter Name and Address of Prime:

   Congressional District, if known: ____

6. Federal Department/Agency: ____

7. Federal Program Name/Description: ____

   CFDA Number, if applicable: ____

8. Federal Action Number, if known: ____

9. Award Amount, if known:

   $ ____

10. a. Name and Address of Lobbying Registrant (if individual, last name, first name, MI): ____

    b. Individuals Performing Services (including address if different from No. 10a) (last name, first name, MI): ____

11. [illegible]

Signature: ____

Print Name: ____

Title: ____

Telephone No.: ____ Date: ____

Federal Use Only:

Authorized for Local Reproduction

Standard Form LLL (Rev. 7-97)

PRINT