OVERVIEW

Welcome and thank you for using the *DHS PushButtonPD™*. This document provides users not familiar with the tool the information necessary to begin using the program for the first time.

SOFTWARE REQUIREMENTS

The tool has only been tested on Microsoft Excel 2016 on a Microsoft Windows-based platform. It may be possible to run on other platform types, however, this has not been a prior requirement. Please contact NICCS@hq.dhs.gov for other platform support.

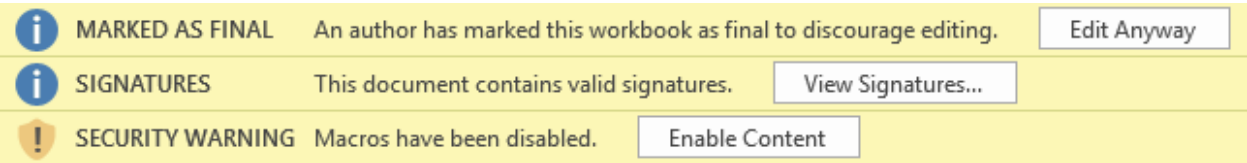
The software is a fully self-contained Excel workbook macro that requires Microsoft Excel co-located on the same Operating System as the worksheet to function. This means that the tool may not function properly when placed on a remote network file share, using Office365, or is run directly from an email attachment. It is able to run via a virtual desktop (e.g. Citrix or VMWare), provided the Excel and worksheet are on the same platform.

Finally, the first time the tool is used, the outer Digital Signature protecting the workbook data must be removed, digitally-signed macros must be permitted, and the software license must be accepted. A walk-through of this process is provided in the next section of this document.

FIRST-USE PROCEDURE

Opening the *DHS PushButtonPD™* for the first time requires the following steps.

1. Obtain the file
    a. From an email attachment:
        i. Open the email with the DHS PushButtonPD™ attachment.
        ii. Right click the attachment and *SAVE AS* to a location on your computer.
        iii. Double-click on the file to open.
        iv. *CLOSE* any pop-ups that appear.
    b. From the webpage:
        i. https://niccs.us-cert.gov/workforce-development/dhs-cmsi-pushbuttonpd-tool
        ii. Click on "1. DHS PushButtonPD™ Tool"
        iii. *SAVE AS* to a location on your computer.
        iv. Double-click on the file to open.
        v. *CLOSE* any pop-ups that appear.
2. Remove the Digital Signature
    a. You should see a set of YELLOW BANNERS near the top of the screen.



    b. Ensure the label marked "SIGNATURE" reads "**This document contains valid signatures.**" ***If any other wording exists, please proceed directly to the TROUBLESHOOTING section later in this document.***
    c. Under the label entitled "MARKED AS FINAL", press the *Edit Anyway* button and answer *YES* and *OK* to any pop-ups that appear. NOTE: This action removes the outer digital signature and allows the user to write data to the workbook. The user will receive a pop-up saying "*Run-time error '1004': This command cannot be performed while the document is open as read-only*" until this step is performed.
    d. Under the label entitled "SECURITY WARNING: Macros have been disabled", press the *Enable Content* button.
    e. Close any pop-ups that appear and press the *SAVE* button (🖫) in the upper left-hand corner on the worksheet itself.
    f. Close and reopen the tool.
    g. When the tool is re-opened, read and accept the software license and pop-ups that appear. The tool should now function normally.

TROUBLESHOOTING

INSPECTING THE DIGITAL SIGNATURE (NEW WORKSHEET)

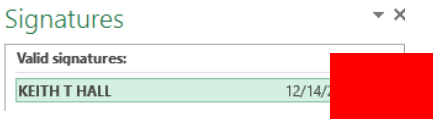
The Digital Signature may be inspected prior to opening or activating the spreadsheet. Note that the outer digital signature is only present on a ***new*** file. Files that have been used before will only contain a digital signature on the macro.

1. Click on the *FILE* tab near the upper left hand portion of the workbook.

2. Under the *INFO* tab along the upper left hand side, find and select the *View Signatures* button.

3. Ensure the Digital Signature is **BLACK**. If the tool is brand new, and the signature is **RED**, do NOT use the tool and contact NICCS@hq.dhs.gov to report the issue.

4. Hover the mouse over the Digital Signature and a small drop-down arrow should appear. Select the down arrow, then select *Signature Details*.



5. The signature is issued by DHS CA4 and match the file properties and creation date.

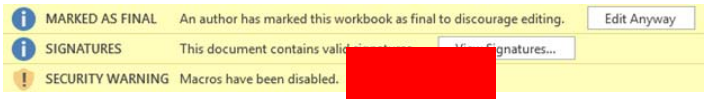
TROUBLESHOOTING

INSPECTING THE DIGITAL SIGNATURE (USED WORKSHEET)

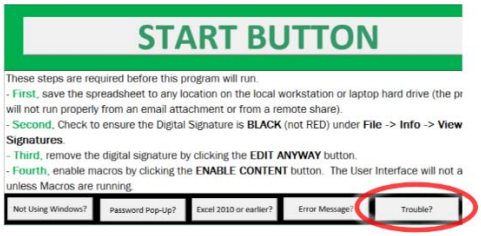
!!! ONLY PERFORM THIS PROCEDURE ON A PREVIOUSLY USED OR OPENED WORKSHEET !!!

The tool has a built-in feature to detect if the macro's Digital Signature has been tampered with. This feature can also be utilized to inspect the properties of the outer Digital Signature. However, it does require enabling the macros to run – which is problematic if you suspect your program has been already tampered with, which is why it should be used with care.

1. Under the label entitled "SECURITY WARNING: Macros have been disabled", press the *Enable Content* button.



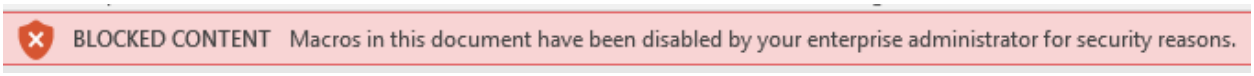
2. From the *Instructions* tab of the worksheet, select the *Trouble?* button.



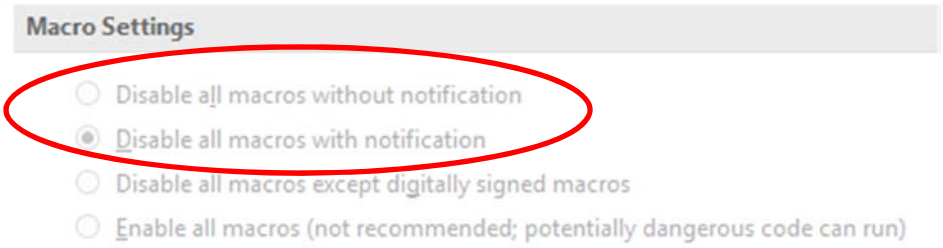
3. The pop-ups will analyze certain environment variables and provide this information to the user. However, under no circumstances should a program have the following message appear: "*WARNING: The Macro Digital Signature is not present*." If this happens, please contact NICCS@hq.dhs.gov for further assistance.

DISABLED MACROS

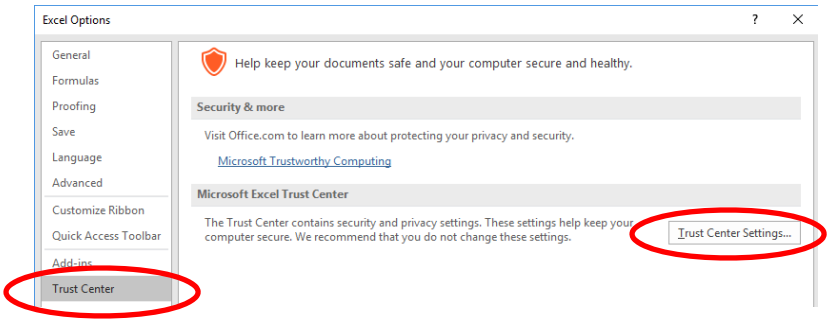
It is possible that the organization has disabled Macros from running in the environment.



If this is the case, then Macro Settings will be set to "Disable all macros" either with or without notification.



To find Macro Settings; navigate to FILE → OPTIONS → TRUST CENTER → TRUST CENTER SETTINGS



There are two recommended methods to re-enabling Macro's securely; and both methods may be combined and used. Please note that in some cases, you may need the assistance of your local IT support in order to enable a workable solution.

METHOD 1: PERMIT DIGITALLY SIGNED MACROS FROM TRUSTED PUBLISHERS

Reference: https://technet.microsoft.com/en-us/library/ff428091.aspx

1. Change "Disable all macros with notification" to "Disable all macros except digitally signed macros "
2. Add the DHS CA4 PKI Certificate (e.g. DHSPushButtonPD.p7b) to "Trusted Publishers"

The disadvantage is that when the certificates expire, the macros will be disabled until re-signed and the updated certificate is loaded in as a 'trusted publisher'.

METHOD 2: TRUSTED LOCATION

Reference: https://technet.microsoft.com/en-us/library/cc179039.aspx

Add a special folder name to a location on the computer (ex. Document folder or the Desktop). Macro-enabled files would be permitted to run from that folder, and anti-malware programs can scan, inspect, and/or quarantine the location.

WITHIN DHS ONLY

Service Desk Ticket # *REQ000000932294: Change in Excel Macro policies after Win10 Upgrade* contains the workaround details for DHS users.