These activities need to be done once per season. They should be completed BEFORE the round begins.
REMEMBER THIS DOES MANY SECURITY SETTINGS, BUT NOT EVERYTHING!

CyberPatriot can use Administrative Templates to wreak havoc upon your image
Because these scripts apply some settings to many Administrative Templates, you should "Fix Administrative Templates" before you follow these instructions
It will be impossible to "Fix Administrative Templates" after running the following scripts.
You should also run the Windows Change Password Script before following these instructions because of the command to Reset Security Policy settings which could erase changes made here.

These directions show you how to apply security settings using publicly available scripts from the following sources:

- Microsoft Security Compliance Toolkit
- US Department of Defense Security Technical Implementation Guides (STIGs)

Although there is much overlap, each script secures different items. Use both.

Downloading the parts

1. **Don't unzip these files when downloading! We'll do it later.**
2. Visit: https://www.microsoft.com/en-us/download/details.aspx?id=55319
3. Click the big blue download button
4. Put checks next to:
   - LGPO.zip
   - Microsoft Edge v117.zip (or higher version)
   - Windows 10 Version 22H2 Security Baseline.zip
   - Windows Server 2022 Security Baseline.zip
5. Click next and click the blue Download button save the zip file
6. Visit: https://public.cyber.mil/stigs/gpo/
7. Click OK to acknowledge the government warning.
8. Scroll to the bottom, and click to download **Group Policy Objects (GPOs)** ***month/year*** (not the readme) and save the zip file

Creating GPO uploads (done days before competition)

1. On your desktop, create the following folders:
   a. ADMX
   b. ADML
   c. Win10
   d. Server2022
   e. Server2022DC
2. Move the **LGPO.zip** file you downloaded and put it on the desktop with the other folders and unzip it which will create a folder. We will refer to that folder as **LGPO_30**.
3. Put the **Windows 10…Security Baseline zip** file you downloaded from Microsoft onto your Desktop and unzip it. Rename the folder that was created **MS10.** If it doesn't unzip due to an

error about file path name too long, move it to the root level (C:\) and try unzipping. If it still doesn't work, change the group policy listed in the **Prepare to Update Security Policies** section**.**

4. Put the **Windows Server 2022 Security Baseline.zip** file you downloaded from Microsoft onto your Desktop and unzip it. Rename the folder that was created **Winserver.** If it doesn't unzip due to an error about file path name too long, move it to the root level (C:\) and try unzipping. If it still doesn't work, change the group policy listed in the **Prepare to Update Security Policies** section**.**
5. Put the **U_STIG_GPO Package zip** (names vary) file you downloaded from the Defense Dept. onto your desktop and unzip it. Rename the folder that was created **U_STIG**
6. Put the **Microsoft-Edge-….zip** file you downloaded from Microsoft into your **U_STIG** folder (yes, really) and unzip it.
7. Open the **U_STIG** folder, and then open the **ADMX Templates** folder.
8. Open the **Adobe** folder. Copy the files that have the extension .admx at the end into the **ADMX** folder you created on your desktop. If you can't see the file extensions, on Windows:
    a. Click the View tab.
    b. Select "File name extension"
9. Open the **en-us** folder. Copy the files that have the extension .adml into the **ADML** folder that you created on your desktop.
10. Repeat the previous two steps with the following folders:
    a. Google
    b. Microsoft
    c. **Microsoft** Edge
    d. Mozilla
11. From the **U_STIG** folder, copy the following folders. Paste them into the **Win10**, **Server2022** & **Server2022DC** folders. You'll probably want to select them by holding down the <control> key, clicking on these items and pressing ctrl-C to copy and ctrl-V to paste.
    1. DoD Adobe Acrobat Pro DC Continuous
    2. DoD Adobe Acrobat Reader DC Continuous
    3. DoD Google Chrome
    4. DoD Internet Explorer 11
    5. DoD Windows Defender Antivirus STIG
    6. DoD Microsoft Edge
    7. DoD Mozilla Firefox
    8. DoD Windows Firewall
    9. Microsoft-Edge-…Security-Baseline
12. From the **U_STIG** folder, copy the **DoD Windows Server 2022 MS and DC** folder to your **Server2022DC** folder.
13. Open the **Support Files** folder that is inside your **U_STIG** folder
14. CAREFULLY COPY the file **Sample_LGPO.bat** and paste it into your **Win10, Server2022** and **Server2022DC** folders. **WARNING**: This is a BAT file and will start to do things if you double click it by mistake. Use Control-C and Control-V to copy and paste.
15. Open the **U_STIG** folder. Then open the **Support Files** folder. Then **Local Policies** folder.
16. Copy: (names might be slightly different)

10. **DoD Windows 10…** to your **Win10 folder**
11. **DoD Windows Server 2022 MS** to your **Server2022** folder

17. From the folder **LGPO_30**, copy the program **LGPO.exe** (application). Paste it into your **Win10, Server2022** and **Server2022DC.** Each of these folders will secure the particular Operating System.
18. From the folder **LGPO_30**, copy the program **LGPO.exe** (application) into **Tools** which is in **Scripts** which is in your **MS10** folder. . It goes here: MS10 > Scripts > Tools
19. From the folder **LGPO_30**, copy the program **LGPO.exe** (application) into **Tools** which is in **Local_Script** which is in your **Winserver** folder. . It goes here: MS10 > Scripts > Tools
20. Copy these folders to your USB Flash drive:
    - **ADMX**
    - **ADML**
    - **Win10**
    - **Server2022**
    - **Server2022DC**
    - **MS10**
    - **Winserver**

During Competition: Prepare to Update Security Policies on an image

1. Run WSUS Offline and Windows Update as many times as necessary so there are no updates needed. Don't do any feature updates using Windows update.
2. Note: If at any time during this process you get an error about the file name being too long, do this on your computer or on the image, whichever is giving you the error:
    a. Go to the search bar, search for and start "gpedit.msc"
    b. If this doesn't work on your home computer, download Policy Plus: https://www.techspot.com/downloads/7112-policy-plus.html and search for "win32 long paths"
    c. On the left, find:
    "Computer Configuration > Administrative Templates > System > Filesystem" and click on it
    d. On the right, find the "Enable win32 long paths" item and double-click it.
    e. In the properties window, select the "Enabled" option and then click "OK."
    f. Restart your image or computer, this should fix the error message.
3. Using Copy and Paste (ctrl-C & ctrl-V) copy either the **Win10** or **Server2022** or **Server2022DC** folder to the desktop of your image. Only copy what's needed for the image. Normally use the **Server2022** folder for Windows Server 2022. If the Readme says that the server is a "domain controller", or Active Directory is a Critical Service, use **Server2022DC**.
4. Using Copy and Paste (ctrl-C & ctrl-V) copy the either the **MS10** folder or the **Winserver** folder to the desktop of your image.
5. Click on the folder icon in the taskbar at the bottom of the screen to open Windows Explorer. Then on the left, click on Local PC, then in the center Local Disk (**C:)**.
6. Drag the **MS10** folder or the **Winserver** to the root level (C:) of your Windows image (the folder you've opened up)

Apply DoD STIGS

1. Use your phone to take a picture of your scoring page. This will help you restore things if this causes you to lose points.
2. Open the ADMX folder. Then Open the **Recycle Bin**. In the **Recycle Bin** window on the left click on **Local Disk (C:)**. In this window open the **Windows** folder then the **PolicyDefinitions** folder. Copy all of the files in your **ADMX** folder here. When it asks for Administrative approval, check the "☐ Do this for all current items" box then "Continue".
3. At the top of the **PolicyDefinitions** window, double click to open the **en-US** folder. Copy all of the files in your **ADML** folder here. You can close these windows.
4. Open up the folder you copied to the desktop (Win10 , Server2022, or Server2022DC). Right click on **LGPO.exe** (application) and choose **Properties**. Click on the **Compatibility** tab. Near the bottom, check the box next to **Run this program as an administrator**. Click **OK**. Note: If you don't do this, you will get a bunch of "Access Denied" errors when running the script.
5. Double click on **Sample_LGPO.bat** and let the script run.
6. Your settings should be applied. After about a minute, it will end with "Press any key to continue" Don't worry about a few warnings or "failed to apply" messages
7. You may need to close the Command Line program.
8. If you received a deduction on your scoring page about "Account Lockout Policy…", don't worry, the Microsoft Security Baseline will fix that.
9. Note: When you restart your image from now on, you will get a Defense Department Warning, this is normal and put in by the STIGs!

Apply Microsoft Security Baseline

1. Use your phone to take a picture of your scoring page. This will help you restore things if this causes you to lose points.
2. At the root level of your C: drive, open up the **MS10** or **Winserver** folder, then **Scripts** then **Tools**. Right click on **LGPO.exe** and choose **Properties**. Click on the **Compatibility** tab. Near the bottom, check the box next to **Run this program as an administrator**. Click **OK**. (Note: Sometimes Microsoft calls Scripts, Local_Script)
3. Go back to the **Scripts** folder by clicking on the "up" arrow in the tool bar
4. Click on the folder's **File** menu and highlight **Open Windows PowerShell** and slide to the right and click **Open Windows PowerShell as administrator**.
5. Make sure your PowerShell prompt ends with "Scripts". If "Tools" is the last word, type `cd ..` and press <Enter> or <Return> If that doesn't fix it, close and navigate to the Local_Script folder and try again.
6. The prompt should either be:

   ```
   PS C:\Winserver\Scripts\
   ```

   or

   ```
   PS C:\MS10\Scripts\
   ```

   If it isn't, start over and make sure you are in the correct folder.

7. Type the following command at the **PowerShell** prompt and press enter (spaces are important):

   ```
   Set-ExecutionPolicy Unrestricted
   ```

8. Answer **Y** to the question.
9. If you are unable to do this in PowerShell, see **Broken – PowerShell** in the Reference Guide.
10. When you type the following commands, the response should be in BLUE. If you get a response typed in red, you probably did something wrong. Double check everything. See the notes two items down.
11. Windows 10 or Windows server: Depending on the ReadMe and the image you are using, type one of the following into the **PowerShell** prompt and press <Enter>:
    a. Windows 10 image, the ReadMe has no mention of being part of a domain or Active Directory (MOST COMMON-use this for most Windows 10 images):

       ```
       .\BaselineLocalInstall.ps1 -Win10NonDomainJoined
       ```

    b. Server image, the ReadMe has no mention of being part of a domain or Active Directory (MOST COMMON-use this for most Windows server images):

       ```
       .\Baseline-LocalInstall.ps1 -WSNonDomainJoined
       ```

    c. Windows 10 image, part of a domain or Active Directory (VERY UNCOMMON-use only if the ReadMe says the image is part of a "domain"):

       ```
       .\BaselineLocalInstall.ps1 -Win10DomainJoined
       ```

    d. Server image, Domain Controller in Active Directory (only seen in final round before). If Active Directory is a Critical Service, you should probably use this one. The ReadMe should specifically say that it is a "domain controller":

       ```
       .\BaselineLocalInstall.ps1 -WSDomainController
       ```

    e. Server image, Active Directory is a Critical Service, but it specifically says that this server is NOT the Domain Controller (never before seen in CyberPatriot online rounds):

       ```
       .\BaselineLocalInstall.ps1  -WSMember
       ```

12. Microsoft has been changing the names of things. If your script doesn't run, or runs in a few seconds, check the following:
    a. Does the PowerShell prompt end with "Local_Script"? If not, close it and try again.
    b. Do you see `BaselineLocalInstall.ps1` in the Local_Script folder? Sometimes Microsoft leaves the `-` out. Use whatever name is in the folder.
    c. Try opening Notepad and then opening `BaselineLocalInstall.ps1`. You should see the commands (like `-Win10NonDomainJoined` in the script. Make sure you're typing what is there.
13. Your settings should be applied. That should run for about a minute.
14. When the script has run, type the following command at the PowerShell prompt:

    ```
    Set-ExecutionPolicy Restricted -Scope LocalMachine
    ```

15. Close PowerShell.

CyberPatriot uses stronger settings for Auditing and Logs than is standard. You must either use "Windows Advanced Auditing Upload" directions or manually configure these settings. Use gpedit.msc to manually check all of following settings to make sure you haven't missed anything that is scored. (approximately 29 different policies). Setting everything to "Success and Failure" is the easiest way to fix this.

Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\

Distributing these files

- You may only give these to other members of your team!
- Use 7-Zip to compress the folders into a zip file.
- Send the zip file to your teammate.
- Team members receiving these files should start on these directions at "**Prepare to Update Security Policies on an image** (done during competition)"
- **These scripts don't do everything found in CyberPatriot, only most. It is a best practice to review the Security Settings document and double check everything marked with a "X" to make sure it is set.**
- **YOU MUST use Windows Security settings to double check settings for "audit" settings.**

Publicly available sources:

Reset group policies to defaults:

https://www.thewindowsclub.com/how-to-reset-windows-security-settings-to-its-defaults

Microsoft Security Compliance Toolkit:

https://www.microsoft.com/en-us/download/details.aspx?id=55319

US Department of Defense Security Technical Implementation Guides (STIGs)

https://public.cyber.mil/stigs/gpo/

Change Log:

- 7.2 9/22/23 – moved to Server 2022 from 2019. Not completely tested. Changed some MS download directions.
- 7.3 9/25/23 – tested & fixed changes on 7.2. Added instructions to install AMDX Templates and ADML language files.