Defense Security Service
Industrial Security Field Operations
National Industrial Security
Program (NISP) Authorization
Office (NAO)

**NAO Quality Assurance (QA)
Secure Hardware Baseline for
Windows 7/10 Job Aid**

June 2017

Revision
Log

Date	Revision	Description of Change
2016OCT19	1.0	Initial Draft
2016OCT27	1.1	Updates based on feedback
2016DEC20	1.2	Updates based upon feedback from Policy
2017MAR02	1.3	Added Disclaimer
2017JUN27	1.4	Updates to reflect Windows 10 applicability

<u>DISCLAIMER</u>

Use of the NAO Configuration Toolkit is at the discretion of facility personnel who are ultimately responsible for the proper security configuration of information systems processing classified information. Facility personnel are responsible for ensuring compatibility with the security settings applied to the authorized information system by the NAO Configuration Toolkit, and are advised to test the configuration on non-production systems prior to applying the GPO to systems in the production environment. The Defense Security Service is not responsible for errors or system failure based on use of the NAO Configuration Toolkit.

Background:

The purpose of this Job Aid is to assist the user through the process of hardening a Windows 7/10 standalone machine to a number of technical baseline compliance standards required by NAO for the National Industrial Security Program (NISP) and its participants. The configuration settings are based upon recommended guidance found in the Defense Information System Agency (DISA) Security Technical Implementation Guides (STIGs) and the National Institute of Standards and Technology (NIST) special publications. These security configurations are provided in the form of a GPO (Group Policy Object), which is applied to the local machine via Microsoft's command line tool "Local Group Policy Object Utility" or LGPO. The user is not limited to LGPO, as the NAO supplied GPO can be applied via Microsoft's Security Compliance Manager (SCM), Microsoft Management Console (MMC), or any other program capable of reading and applying ".INF" and ".POL" files.

The NAO provided GPO is intended to configure the technical security settings of a fresh installation of Microsoft Windows 7/10 x86/x64 (all versions) to within 85% of compliance. Some configuration settings were intentionally not configured to prevent the user from locking themselves out of the machine if certain parameters (e.g. a weak Administrator password, no emergency Administrator account) were not in place prior to running the configuration tool.

It is important to note that the Information System Security Manager (ISSM) is ultimately responsible for the proper configuration and testing of the system, regardless of the use of this GPO or not. Furthermore, additional security settings may still require configuration or tailoring in accordance with the SSP for the system and/or applicable policies. The use of this job aid is intended to strengthen system security controls, ease the configuration process, assist with continuous monitoring, and expedite security reviews.

Users implementing this GPO may utilize Microsoft's Local Group Policy Object Utility (Version 1.0), which can be obtained at no cost to the user and is located at the following URL: https://blogs.technet.microsoft.com/secguide/2016/01/21/lgpo-exe-local-group-policy-object-utility-v1-0/

Applying the NAO Configuration:

1. Download Microsoft's Local Group Policy Object Utility (Version 1.0) at the URL provided above (optional). You may also use a different application that supports Group Policy Objects.
2. Unzip the archive file to a folder on the Desktop. You may place this folder in another directory if desired, just make note of the path to the folder containing the LGPO executable. This utility is not installed, but rather runs from an elevated command line in the directory containing the executable.

3. Obtain the NAO GPO by logging into OBMS and navigating to the "Headquarters" section of the ODAA Bulletin Board tab. Click on the post titled "NAO Windows Configuration Toolkit" and download the ZIP package.
4. Extract the package contents to your desired directory.
5. Launch an elevated command prompt window:
    a. Press the Windows key
    b. Type 'cmd"
    c. In the results, right click on the "CMD" Utility and click "Run as Administrator".
    d. Accept any Windows UAC prompts that occur and click "Allow" if asked to allow the elevation of privileges.
6. At the elevated command prompt, change directories to the directory housing the LGPO.exe executable. For example, if you extracted the LGPO executable to a folder on the Desktop titled "LGPO", then type the following at the command prompt to change directories: "cd C:\Users*your-username*\Desktop\LGPO" and press the "Enter" key. Note that there is a space between "cd" and the path.
7. In Windows Explorer, navigate to the directory containing the NAO GPO Folder previously downloaded and extracted.
8. Double click on the folder, and in the address bar at the top of the Explorer Window right click on the name of the folder containing the GPO and select "Copy address as text".
9. Return to the command line window, and type the following command: LGPO.exe \g [*Paste the path to NAO GPO here, do not include brackets*]. Note that there is a space between "LGPO.exe" and a space between "\g" and the path to the NAO GPO.
10. Hit "Enter" to run the configuration file.
11. Reboot the machine manually through the Start menu, or by typing shutdown \r in the command line terminal.