**Ops Required Configs:**

-Enable the WinRM service  
**Enable-PSRemoting -Force**  
-Set the WinRM service to start automatically  
**Set-Service -Name WinRM -StartupType Automatic**  
-Allow connections from any IP address (adjust as necessary; run in CMD Line)  
**winrm set winrm/config/client @{TrustedHosts="\*"}**  
-Configure the firewall to allow WinRM connections  
**New-NetFirewallRule -Name "WinRM-HTTP-In-TCP" -DisplayName "WinRM-HTTP-In- TCP" -Protocol TCP -LocalPort 5985 -Action Allow -Direction Inbound**

**New-NetFirewallRule -Name "WinRM-HTTPS-In-TCP" -DisplayName "WinRM-HTTPS-In-TCP" -Protocol TCP -LocalPort 5986 -Action Allow -Direction Inbound**

-May need to set basic authentication

**Set-Item -Path WSMan:\localhost\Service\Auth\Basic -Value $true**

\*\*\*Reminder\*\*\* Need to Add new NSG Inbound rule Labeled 'Nessus' and open ports 139 and 445. Add scan IP as a source.

-Install OpenSSH Server  
**Add-WindowsCapability -Online -Name OpenSSH.Server~~~~0.0.1.0**  
-Start the SSH Server service  
**Start-Service sshd**  
-Set the SSH Server service to start automatically with the system  
**Set-Service -Name sshd -StartupType 'Automatic'**  
-Confirm the firewall rule is configured. It should be created automatically during setup.  
**if (-not (Get-NetFirewallRule -Name "SSHD-In-TCP")) {New-NetFirewallRule -Name "SSHD-In-TCP" -DisplayName "OpenSSH Server (sshd)" -Enabled True -Direction Inbound -Protocol TCP -Action Allow -LocalPort 22}**

-Create inbound/outbound rules to allow TCP traffic on port 5900 for VNC

**New-NetFirewallRule -Name "VNC-In-TCP-5900" -DisplayName "VNC (TCP-In) - Port 5900" -Enabled True -Direction Inbound -Protocol TCP -LocalPort 5900 -Action Allow**

**New-NetFirewallRule -Name "VNC-Out-TCP-5900" -DisplayName "VNC (TCP-Out) - Port 5900" -Enabled True -Direction Outbound -Protocol TCP -LocalPort 5900 -Action Allow**

-Install Chrome and update

-Install RealVNC, SCP, and Putty

**STIG Compliance**

-Turned on AV and ran an update

-InstallRoot tool and install certs:

DoD Root CA 3, DoD Root CA 4, DoD Root CA 5, DoD Root CA 6

-Run the Federal Bridge Certification Authority (FBCA) Cross-Certificate Removal Tool once as an administrator and once as the current user.

-Run updates.reg in root directory of this script

-Copy the .admx and .adml file from \ADMX Templates\Microsoft and ADMX Templates\Microsoft\en-US to \Windows\PolicyDefinitions and \Windows\PolicyDefinitions\en-US directories respectively.

\*\*\*You may want to copy the Edge and Chrome ADMX/ADML files over too.\*\*\*

-Created user **remote\_user** and added them to the following groups:

Access Control Assistance Operators; Backup Operators; Device Owners; Network Configuration Operators; Power Users; RDS Endpoint Servers; RDS Management Servers; RDS Remote Access Servers; Remote Desktop Users; Remote Management Users; Users