4101 Washington Avenue
Newport News, VA 23607
Telephone 757-380-2000
HII.com

To: All Valued Suppliers

From: Supplier Compliance

Date: June 16, 2023

Subject: MOVEit Application Vulnerability

As you may already be aware from news reports, Progress Software, the developer of a data migration application called MOVEit, has discovered a critical vulnerability that could allow an unauthenticated attacker to gain unauthorized access to the MOVEit Transfer database. HII requests that each supplier determine whether it uses the MOVEit application and to notify HII immediately if it does either at NNSSupplierdata@hii-nns.com or Suppliercerts@hii-ingalls.com.

Should your business currently use MOVEit, HII asks that you immediately mitigate this vulnerability by disabling all HTTP and HTTPs traffic to your MOVEit Transfer environment. Specifically:

- Modify firewall rules to deny HTTP and HTTPs traffic to MOVEit Transfer on ports 80 and 443.
- It is important to note that until HTTP and HTTPS traffic is enabled again:
    - Users will not be able to log on to the MOVEit Transfer web UI
    - MOVEit Automation tasks that use the native MOVEit Transfer host will not work
    - REST, Java and .NET APIs will not work
    - MOVEit Transfer add-in for Outlook will not work
- **SFTP and FTP/s protocols will continue to work as normal**

As a workaround, administrators will still be able to access MOVEit Transfer by using a remote desktop to access the Windows machine and then by accessing https://localhost/. For more information on localhost connections, please refer to MOVEit Transfer Help: https://docs.progress.com/bundle/moveit-transfer-web-admin-help-2023/page/Security-Policies-Remote-Access_2.html.

Progress Software is currently testing a patch and will update customers as soon as possible. More information can be found at Knowledge Base article.

DISCLAIMER: The information provided in this memo is for informational purposes only.