PRO V&V	**ENGINEER CHANGE ORDER (ECO) ANALYSIS FORM**

Manufacturer:	Election Systems & Software (ES&S)
System:	ASA 5505, ASA 5506 and ASA 5512
ECO Number:	979
ECO Description:	Cisco Adaptive Security Appliance (ASA) Firmware update

Overview:
Cisco ASA devices used in Unity and EVS releases are affected by a new critical vulnerability as described on the Cisco website (https://www.cisco.com/c/en/us/support/docs/csa/cisco-sa-20180129-asa1.html).
Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.
A vulnerability in the Secure Sockets Layer (SSL) VPN functionality of the Cisco Adaptive Security Appliance (ASA) Software could allow an unauthenticated, remote attacker to cause a reload of the affected system or to remotely execute code.

Firmware Update:
ASA 5505 - Firmware update to v9.1.7.23
ASA 5506-X Firmware update to v9.6.4.3
ASA 5512 - Firmware update to v9.1.7.23

Supporting Documentation:
ES&S ECO#979 Cisco ASA Firmware.pdf
Cisco Adaptive Security Appliance Remote Code Execution and Denial of Service Vulnerability.pdf
ASA 5506 – 5506x Functional Testing_Redacted.pdf
ASA 5512-X Functional Testing_Redacted

Engineering Recommendation:
Reviewed manufacturers (CISCO) documentation along with the ES&S system architecture. ES&S performed an internal test and determined that this testing was sufficient for the function of this system application. Pro V&V then analyzed the test documentation provided by ES&S and determined that no additional testing is required.

Engineering Analysis: De Minimis

Reviewer:	**Approver:**
William Bush	Wendy Owens
Printed Name	Printed Name
William Bush	Wendy Owens
Signature	Signature
3/14/18	3/14/18
Date	Date