

**PRO V&V**



**ENGINEER CHANGE ORDER (ECO) ANALYSIS FORM**

**Manufacturer:** Election Systems & Software

**System:** EVS & Unity (Cisco ASA Firmware)

**ECO Number:** 999

**ECO Description:** Software update required to address identified Cisco ASA device vulnerability.

**Overview:**

Cisco ASA devices used in Unity and EVS releases are affected by a new 'High' vulnerability. Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.

ES&S Cisco ASA Devices Affected:

ASA 5505, ASA 5506, ASA 5512

Systems Affected:

EVS 5100, EVS 5110, EVS 5300, EVS 5303 EVS 5310, EVS 5320, EVS 5321, EVS 5330, EVS 5340, EVS 5501, EVS 5502, EVS 6010, FL EVS 4520 v1, FL EVS 4530v1, FL EVS 4530v2 FL EVS 4500 v4, Unity 3411

**Supporting Documentation:**

ECO 999 Cisco ASA CVE-2018-0296 Vulnerability.pdf

Cisco Security Advisory cisco-sa-20180606-asaftd.pdf

Cisco ASA Software Upgrade Testing\_Redacted.pdf (*ES&S internal testing documentation*)

**Engineering Recommendation:**

Technical documentation and firmware update review performed to approve change. Pro V&V determined that the firmware update will not adversely affect any system functions. No additional testing is required.

**Engineering Analysis:** De Minimis

**Reviewer:**

Wendy Owens

Printed Name

Wendy Owens

Signature

7/2/18

Date

**Approver:**

Michael L. Walker

Printed Name

Michael L. Walker

Signature

7/3/18

Date