DEFENSE INFORMATION SYSTEMS AGENCY
P. O. BOX 549
FORT MEADE, MARYLAND 20755-0549

IN REPLY REFER TO: Infrastructure Directorate (IE)

14 January 2020

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Department of Defense Information Network (DoDIN) Approved Products List (APL) approval of the Fidelis Cybersecurity, Inc. Fidelis Network Release (Rel.) 9.1.4 Tracking Number (TN) 1816201 as an Intrusion Protection Systems and Intrusion Detection Systems (IPS and IDS)

Reference: (a) DoDI 8100.04, "DoD Unified Capabilities," 09 December 2010
(b) DoD CIO "Unified Capabilities Requirements (UCR) 2013," July 2013

1. DoDIN APL approval of the Fidelis Cybersecurity, Inc. Fidelis Network Rel. 9.1.4 TN 1816201 as a (IPS and IDS) has been granted. The Risk Management Executive (RME) recommended DoDIN APL placement on 09 October 2019 based on the Cybersecurity (CS) testing completed by the Telecommunications Systems Security Assessment Program (TSSAP) led CS test teams. This solution achieved Interoperability (IO) certification from the Joint Interoperability Test Command (JITC) on 08 March 2019. This approval is effective upon the date of this memorandum and expires **10 October 2022** unless a critical issue is identified that invalidates either the CS or the IO posture of this product as determined by the JITC or the Chief Information Officers (CIO) for Combatant Commands, Services, and Agencies. Please note that Services and Agencies are required to recertify and reaccredit their systems every three years. Please refer to the DoDIN APL for official posting of this solution at the following site: https://aplits.disa.mil/apl.

2. This product/solution must be implemented only in the configuration that was tested and approved. To ensure an acceptable level of risk for each site's Authorizing Official (AO) / Designated Accrediting Authority (DAA), please utilize this solution's deployment guide and refer to the Conditions of Fielding (CoF) as depicted within the Cybersecurity Assessment Report (CAR). The CAR is included in the Cybersecurity Assessment Package (CAP) and can be requested from the Approved Products Certification Office (APCO) per paragraph 4 of this document.

3. The IO certification letter containing the detailed components and configuration on this product is available at the following site:
http://jitc.fhu.disa.mil/tssi/cert_pdfs/Fidelis_Network_9-1-4_TN1816201_Initial_08MAR2019.pdf
On 14 January 2020, the following extension was approved via Desktop Review (DTR) #1 (requested to update the Rel. from 9.1.4 to 9.1.4 [1] to resolve open CS findings):
http://jitc.fhu.disa.mil/tssi/cert_pdfs/Fidelis_Network_9-1-4_1_TN1816201_DTR1_13JAN2020.pdf

DISA Memo, IE, DoDIN APL Approval Memo, Fidelis Cybersecurity, Inc. Fidelis Network Rel. 9.1.4 TN 1816201, 14 January 2020

4. Due to the sensitivity of the information, the CAP must be requested directly from the APCO by a government civilian or uniformed military personnel.

E-Mail: disa.meade.ie.list.approved-products-certification-office@mail.mil

For: GRADIJAN.ROBERT.GEORGE.1398029980
Digitally signed by GRADIJAN.ROBERT.GEORGE.1398029980
Date: 2020.01.14 08:12:23 -05'00'

Charles H. Osborn
Acting Executive, Infrastructure Directorate