Comments Review 800-171B

This message has a digital signature, but it wasn't verified because the S/MIME control isn't currently supported for your browser or platform.

F

fox@nevaridge.com
Today, 1:51 PM
sec-cert

Reply all

Hello,

After a review of the draft subject document I believe the 3.6.1e and 3.6.2e are a huge stretch for small or medium sized companies. I have worked for large, medium, and small industrial base contractors in my 20+ yrs in the field and only the large companies are doing this regularly in the unclassified/corporate networks. One medium sized company I worked for had this for their classified operations ONLY, but only due to the USG contract revenue they were receiving to perform the contract; allowing for the expense. Small companies can barely comply with 800-171 period, unless they are fortunate enough to have a seasoned IT and Security professional on their staff who can maneuver the guidance within budget constraints.

To ask for a SOC or CIRT team is an unrealistic enhancement to have in-house or to subcontract out for small or medium companies. The cost for little gain/assurance would be crippling to imagine. I would call this a “wishlist” item at best. There are less expensive methods to meet the spirit of the enhancement with a simple log server using a free SIEM (i.e. Graylog). This enhancement needs to be much broader than “A SOC capability can be obtained in a variety of ways. Larger organizations may implement a dedicated SOC while smaller organizations may employ third-party organizations to provide such capability”. That statement puts too much ambiguity into meeting compliance and gives an assessor WAY TOO MUCH leeway to interpret the meaning leading to inconsistencies/imbalances of enforcement.

I would reassess these sections.

NEVA RIDGE TECHNOLOGIES

Jim Fox
Security Manager, FSO
6685 Gunpark Drive, Suite 230
Boulder, CO 80301

303-531-2769 (Direct)
www.nevaridge.com