Comments on Draft 800.171B

ME Mark Emery <mark.emery@theemerygroup.com>

Reply all

Tue 8/6, 2:23 PM

sec-cert

Inbox

All,

First I apologize for my comments being late; I hope they will still be considered by the authors.

1. Protecting CUI is extremely important to the US Government as stated by the authors. If this protection is so important, why does the Government "contract" the responsibility to protect this information/data to contractors and sub-contractors? Protecting information/data is an "inherently" governmental responsibility; the Government must have direct control, not "contractual" or "compliance" control over the CUI.
    a. The premise of 800.171 and its revision is based under a presumption that the Government must delegate this authority to protect CUI in order to work with its industrial base. Thus, all of the controls, basic and enhanced, derive from this assumption.
    b. I propose that the controls for CUI be considered from the point-of-view of the CUI, not the networks upon which the CUI resides. This perspective will allow the authors to propose "data centric" security controls for CUI that are maintained, monitored, and enforced by the Government through policy, technology (secure data access), and real time monitoring of CUI data usage. This will assure that the Government maintains a chain-of-custody over the CUI.
2. Implementing data centric security controls for CUI first starts with discovery and classification
    a. Tools are available to discover CUI and classify it for appropriate use
    b. Discovery should be done in the Government systems, first, where data should receive its original classification (first as CUI, then by identifying the CUI by program)
    c. Discovery should also be run on all legacy data held by Government contractors; CUI not associated with the appropriate program should be cryptographically shredded.
3. The second critical step is to armor the CUI with enterprise, not ad hoc tools, that provides the Government with controlling authority over who and what systems may utilize the data
    a. The Government creates communities of use, perhaps with Active Directory, that control CUI access
    b. Third parties (contractors and sub-contractors employees) can be granted access to the CUI data by being entered into the community
    c. The Government Program Manager who owns the CUI decides the employees, contractors and systems that have access to the CUI
4. Finally, the Government must establish a monitoring system that records every event of CUI use, change, or sharing, regardless of location
    a. The armored data can report back to the Government any unauthorized use of CUI, and even authorized use, but in an abnormal way
    b. The information collected from the data use can be integrated with the Government SEIM

for behavioral analysis, and if suspicious activity occurs steps can be taken to shut down access to the data.

c. The Government will have a fully auditable and forensically sound log trail of all CUI data use.

5. Persistent data encryption is the most likely methodology for protecting CUI (this is not mere encryption at rest, or encryption in transit; it requires that data be encrypted from the moment of creation, or capture, throughout its life cycle to eventual destruction)
    a. Encryption Key Management is owned by the Government under two-person authority
    b. Keys should be generated using True Random Numbers
    c. Contractors and sub-contractors receive any necessary key material from the Government

Mark Emery
Managing Partner
703-655-2701