From: [redacted] via 800-171comments
To: 800-171comments@list.nist.gov
Subject: [800-171 Comments] comments 800-171
Date: Thursday, July 6, 2023 3:28:19 PM

Dear US Government,

General Feedback: Email is a large attack vector for us and all other companies. We have 20 items we measure for how well we have email security implemented which we review quarterly. Only one of those 20 items is listed in NIST, SPAM. There is no mention of modern basics like URL monitoring, sandbox detonation, imposter detection, SPF/DKIM/DMARC records, domain monitoring, post auto-pull, etc.. The same is true of the other basics from core items of a modern security program, endpoint, cloud, identity, incident response capabilities, etc.. None of the useful things are mentioned. These frameworks are missing all the basics that give you the most bang for your buck in stopping threats. Being agile is key to addressing the changing threat landscape. If your framework is not agile it will create a bureaucracy that will ensure companies are hacked. Legacy government systems, controls and breaches, case, and point. I would recommend a complete rehaul of 800-53 instead of trying to move 800-171 closer to 800-53. Both control lists feel archaic like something from 30-40 years ago. It is a lot of busy work with little value, wasted money. Don't get me wrong mandatory DFARS is good to bid on a contract, but the requirements need a full overhaul. Stick to core and basics from breaches and nail them and update them regularly. For example, a bullet-proof standardized conditional access policy goes a long way. ISACS discuss this and test as a group to provide the new standard for the group. 800-171 Rev 2 is better than rev 3 if an overhaul of 800-53 is too difficult for a bureaucracy.

3.13.6 Network Communications - This control needs to be reworded. Most will do a zoned network architecture(i.e., not a system boundary but a network boundary). There are some that do it for some ICS environments and some that do host firewalls for managed Windows and Linux hosts. Some will do it for all internet communications and commonly attacked ports and protocols. No companies do it for all hosts/systems. You may also want to consider defining "system". In government it can refer to a group of computers or a single computer and I see it used interchangeably throughout. Companies only ever use it in the singular instance, except some primes who have mixed gov private terms. Keep that in mind when you write policy standards for non-gov. Also keep in mind that standards used in policy are policies. Meaning these are not things you should consider doing. These are the things you must do. Don't include anything that you aren't saying must be done. While host firewalls work well in some instances network firewalls work well in others. Expect hosts/systems to communicate through switches, not everything can go through a network firewall and not every host/system has firewall capability.

3.4.8 Authorized Software - I'd wager >90% of DIB companies have nothing for this control. In many of our ISACs there are very few of us that implement this control. The reason most companies don't do it is because it is the fastest way for a CISO to get fired. Breaking business continuity is much more likely with this control than from external threats. Many of the vendors that implemented this type of technology have gone out of business. The few that remain largely don't market it. It's largely taboo to even talk about at CISO conferences. Even at the first revival meeting of NDISAC it was poo-pooed by all but 3 companies. If at some point in the future, you don't get comments from me

regarding NIST it will be because we implement this control. It is trivial for our penetration testers to bypass it. At other prime's I've worked at APT's always got around it. The only thing it is good for is ransomware, as commodity ransomware doesn't generally have application control bypass built-in since nobody does it. Even Microsoft who has products doing this (AppLocker and MDAC) do not use it in a way that would stop most threats. Operationally they have full exceptions for any DLL shimming, and they have full exception for "Program Files" because their own software is too disruptive. They also do not even provide a management interface for it. Strategically they've already replaced it with IPSEC FW app policies and integration with modern CPUs for memory monitoring.

Government loves documenting things. Consider removing ~90% of the times document is mentioned. Written policy is nice but 99% of IT policy exists in software not in documents.

Thanks,

Dan Vickery | **CISO**

O: [redacted] | [redacted]
