Comment:

I wish to thank the authors for providing the public the opportunity to provide feedback on the draft NIST SP on protecting high-value CUI in non-Federal systems. I want to call attention to the section 3.13, which I think is especially innovative compared to government cybersecurity techniques demonstrated up to this point. But I do still see areas for potential improvement in the draft: # Balancing Diversity vs. Secure Implementations I feel the advice given in 3.13.1e to introduce diversity may cause organizations to look for measures that would actually weaken security overall by adopting less-secure tooling for the sake of software diversity. Many software packages exist on "security tiers". Using ASLR techniques would certainly add defense in depth to resisting attack, but introducing the BSD-era sendmail in addition to modern qmail or postfix for the sake of diversity would make things *much* easier for an attacker. Diversity only makes sense to the extent that it doesn't cause one to add software with less security design into an architecture already using secure methods. Rather than unnecessarily increasing attack surface to hopefully disrupt an attacker (who will only be temporarily delayed, if at all), there can be good reasons to focus your attention on a security-critical function by doing it once, to ensure you do it right. Likewise, the training and cognitive burden of having to maintain parallel implementations of common functions may itself introduce vulnerabilities. E.g. I'd rather have an NGINX expert maintain an Apache httpd install than having an Tomcat expert do so, but it would be even better for our NGINX expert to securely maintain NGINX. I see the point being pressed for here but I don't think the current draft captures the pros/cons adequately and as a result risks having Federal cybersecurity compliance staff downgrading non-Federal organizations that have actually made prudent security decisions. At the very least I recommend discussing the concepts of 'attack surface' and stressing diversity that combines to mitigate or eliminate entire classes of security bugs, rather than neutral examples like VPN-in-VPN. Another example pro-diversity would be use of commercial CAs in applications intended for use from BYOD mobile rather than a private PKI, to avoid training users to ignore security warnings. # Security vs. Durability Sect 3.13.2e recommends disrupting attack surface through unpredictability and various other techniques. I'm strongly supportive of this approach. But I would add that there is a potential tradeoff here with other functional key parameters like data durability and system availability. An attacker might be able to more easily cause a denial-of-service in a dynamic architecture, even if they can no longer gain a local presence. And if the attacker *can* gain local presence, they seem likely to just use the custom toolset that would have been developed to make the system tractable for local sysadmins. All the same, this model aligns cleanly to a DevSecOps construct with frequent deployments and is to be encouraged as a result. # Spear Phishing Spear-phishing of network sysadmins remains the most prevalent initial infection vector from APTs (e.g. consider the description of APT 10's "Cloud Hopper" attacks at https://www.reuters.com/investigates/special-report/china-cyber-cloudhopper/). The draft addresses spear-phishing, but only in "3.2.2e" (Awareness & Training). However I believe that training alone will not materially reduce successful attacks

	of this method; most of those to be trained are already familiar by virtue of the knowledge and expertise that made them admins in the first place, and spear phishing can be made nearly indistinguishable from legitimate email. Some discussion of potential technical measures would be appropriate, possibly including cloud-based email or attachment quarantine (to address attachments executing malicious code). Multifactor authentication to address spear-phishing to gather authenticators is indirectly addressed, as is logical and physical segmentation, but all the same some further discussion above and beyond awareness training is warranted. As long as spear phishing remains so effective, it will severely hamper the effectiveness of the more advanced and dynamic mitigations described. It would be useful for non-Federal organizations that have taken technical steps to try to address spear-phishing to be able to refer to this SP to defend those steps when discussing the approach their architecture takes to mitigate or tradeoff cybersecurity risks. --- Thank you again for the opportunity to provide feedback. Regards, - Michael Pyne *
First Name:	Michael
Middle Name:	
Last Name:	Pyne
Mailing Address:	
Mailing Address 2:	
City:	
Country:	United States
State or Province:	Virginia
ZIP/Postal Code:	
Email Address:	michael.pyne@gmail.com
Phone Number:	
Fax Number:	
Organization Name:	
Submitter's Representative:	
Government Agency Type:	
Government Agency:	
Cover Page:	HTML