#	Organization	Commentor	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
1	Venafi	Paul Turner	T	13	After ID.AM-2	Identify	Trust, established by cryptographic keys (e.g., SSH) and digital certificates, is foundational to all cybersecurity. As the primary conveyors of trust in distributed environments, keys and certificates, are being targeted in attacks. Here are several examples: • Millions of computers are infected with malicious code designed to steal keys and certificates (Symantec http://bit.ly/128lDh4) • Underground markets for compromised certificates have emerged (CSIS http://bit.ly/1dRMTux) • 1 in 5 public cloud instances available for free contain backdoors from unknown SSH keys (Dell SecureWorks http://bit.ly/1dROYGG) • “A PKI is critical infrastructure. Treat it like one.”Aart Jochem, NCSC-NL 4/13 (NIST/NCSC-NL http://1.usa.gov/1dROosK) Organizations must have an inventory of keys and certificates used by infrastructure components and other systems to ensure the security of those credentials. Informative Reference: • NIST ITL July 2012	Add the following subcategory: "Cryptographic keys and digital certificates that establish trust are inventoried"

2	Venafi	Paul Turner	T	16	Before PR.AC-1	Protect	The operations groups responsible for managing the systems where keys and certificates are deployed are rarely trained in cryptographic key security best practices. In addition, most commerical organizations have poorly defined policies for cryptographic keys and digital certificates and virtually no enforcement, leaving these critical elements of trust vulnerable to compromise and making them primary targets for attacks. It is imperative that organizations define and enforce policies in this area.	Add the following subcategory: "Policies to secure and protect cryptographic keys and digital certificates are established and enforced"
3	Venafi	Paul Turner	T	16	PR.AC-1	Protect	The majority of cryptographic keys and digital certificates used on infrrastructure systems are stored in files (on disk) that are protected by passwords. The same password is often used across multiple systems and keystores. The keys/certificates and files are manually managed by administrative groups that experience regular resource turnover, increasing the likelihood of a compromise. Though management is important, the emphasis must be on securing and protecting these assets.	Change Subcategory description to the following: "Identities and credentials are managed and secured for authorized devices and users"
4	Venafi	Paul Turner	T	22	After DE.CM-3	Detect	Cryptographic keys and digital certificates broadly serve as the basis of trust for critical infrastructure and supporting systems. As stated earlier, most are stored in password protected files, leaving them open to exploit. Consequently, cryptographic keys and digital certificates must be monitored to detect vulnerabilities and exploits--such as administrative changes (i.e., reassigned or terminated individuals who had access to the key) and unauthorized changes (e.g., changing of trust anchors used for verification).	Add the following subcategory: "Cryptographic keys and digital certificates are monitored to detect vulnerabilities and exploits"

5	Venafi	Paul Turner	T	24	After RS.PL-1	Respond	The Dutch government was forced to stop services to its citizens after the DigiNotar CA compromise because they had no inventory of their certificates and no defined response plan for the replacement of certificates if a CA compromise occurred. Most commercial and government organizaztions have no defined response plan for the compromise of a CA, SSH key, or other cryptographic keys. The nearly ubiquitous use of cryptographic keys and digital certificates for the trust and authentication of mission critical infrastructure makes response plans a crucial part of any cybersecurity plan.	Add the following subcategory: "Trust compromise response plan is established and implemented"