To: NIST
From: Paul Turner, Venafi
Subject: Addressing Trust in Preliminary Cybersecurity Framework

The Preliminary Cybersecurity Framework is well organized and will help ensure government and commercial organizations secure and protect critical infrastructure. However, the framework omits the critical element of trust, established by cryptographic keys and digital certificates, which is foundational to all cybersecurity. Any infrastructure component or system, whether hardware or software, cannot be considered secured if it cannot be trusted. Cryptographic keys and digital certificates, as the primary conveyors of trust in distributed environments, are being targeted in attacks and create a major vulnerability when not properly secured. Aart Jochem from NCSC-NL summarized this at the NIST CA Workshop in April 2013: "A PKI is critical infrastructure. Treat it like one." (NIST/NCSC-NL http://1.usa.gov/1dROosK)

The recommendations included in this response complement the Core Framework to ensure this critical cybersecurity element is not omitted and vulnerabilities overlooked. NIST's long history in promoting standards and security guidance for cryptographic keys and digital certificates demonstrates the importance trust plays and why it must be included in the Cybersecurity Framework.

Cybersecurity trends demonstrate why securing and protecting cryptographic keys and digital certificates must be explicitly documented in the Core Framework:

- 6.6% of all malware and 24% of Android mobile malware are now enabled by compromised digital certificates (McAfee http://bit.ly/1dRMEj7)
- Millions of computers are infected with malicious code designed to steal keys and certificates (Symantec http://bit.ly/128lDh4)
- Weak cryptographic exploits are now feasible, leading software vendors to deprecate use of methods long known to be vulnerable (Microsoft http://bit.ly/1dRMRTf)
- Underground markets for compromised digital certificates have emerged (CSIS http://bit.ly/1dRMTux)
- One in five public cloud instances available for free contain backdoors from unknown SSH keys (Dell SecureWorks http://bit.ly/1dROYGG)
- Well known cryptographic vulnerabilities go unpatched or resolved, dramatically increasing the risk of exposure (ThreatPost http://bit.ly/1gH24nT)
- Cyberespionage organizations, such as APT1, are known to use legitimate looking certificates to enable attacks (Mandiant http://bit.ly/1dRMLLz)
- Compromise of a critical infrastructure such as Certificate Authority can lead to chaos and the inability for government and business to operate on the Internet as demonstrated by the breach of DigiNotar (NIST/NCSC-NL http://1.usa.gov/1dROosK)

Note: All of the above references have no affiliation with the submitters of these recommendations.

Because of these threats and the omission of securing and protecting trust, we recommend the following additions to the Core Framework:

Function	Category	Subcategory	Informative References
Identify	Asset Management	Insert After ID.AM-2: Cryptographic keys and digital certificates that establish trust are inventoried	• NIST ITL July 2012
Protect	Access Control	Change PR.AC-1: Identities and credentials are managed and secured for authorized devices and users	• NIST ITL July 2012

Function	Category	Subcategory	Informative References
Protect	Protective Technology	Policies to secure and protect cryptographic keys and digital certificates are established and enforced	• NIST SP-800 57
Detect	Security Continuous Monitoring	Cryptographic keys and digital certificates are monitored to detect vulnerabilities and exploits	• NIST SP-800-131A • NIST SP-800 57
Respond	Response Planning	Trust compromise response plan is established and implemented	• NIST ITL July 2012