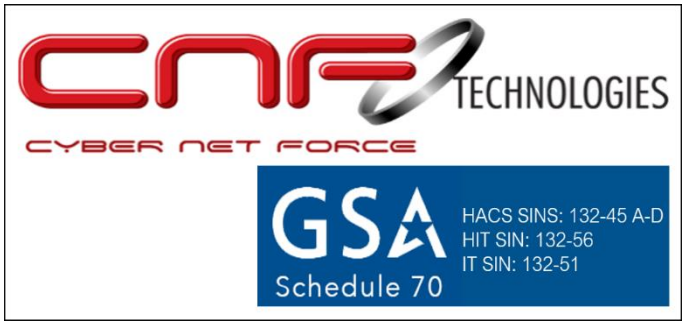
PRESS RELEASE

For immediate release

CNF Awarded the Highly Adaptive Cybersecurity Services (HACS) SINs on IT Schedule 70



SAN ANTONIO 27 Mar. 2018 – CNF Technologies has been awarded and their cybersecurity professional services are available through the GSA IT Schedule 70 Highly Adaptive Cybersecurity Services (HACS) Special Item Number (SINs). The HACS SINs provide government agencies an efficient venue to access pre-vetted capable vendors such as CNF to expand their capacity to test sensitive and high priority systems, address vulnerabilities, and protect the nation's Cyber/IT infrastructure from adversaries. CNF internally selected five seasoned professionals to represent the company through a rigorous technical oral evaluation administered by senior representatives from the Department of Homeland Security (DHS) and GSA. The select team of CNF professionals coupled with CNF's extensive experience and exceptional past performance supporting the Department of Defense, Intelligence Community, and other Federal Agencies encountered zero difficulties in achieving the HACS SINs award.

Information on How to Order and the specifics on the HACS SINS can be found below and through the following link: GSA HACS SINs

- **132-45 A Penetration Testing-** is security testing in which assessors mimic real-world attacks to identify methods for circumventing the security features of an application, system, or network.
- **132-45B Incident Response-** services help organizations impacted by a Cybersecurity compromise determine the extent of the incident, remove the adversary from their systems, and restore their networks to a more secure state.
- **132-45C Cyber Hunt-** activities are responses to crisis or urgent situations within the pertinent domain to mitigate immediate and potential threats. Cyber Hunt activities start with the premise that threat actors known to target some organizations in a specific industry, or specific systems, are likely to also target other organizations in the same industry or with the same systems.
- **132-45D Risk and Vulnerability Assessment**- conduct assessments of threats and vulnerabilities, determines deviations from acceptable configurations, enterprise or local policy, assesses the level of risk, and develops and/or recommends appropriate mitigation countermeasures in operational and non-operational situations.

About CNF Technologies

CNF is a top cybersecurity provider in San Antonio Texas. Applying exceptional expertise and extensive experience, CNF is a proven provider in developing, testing, fielding, sustaining, and employing Cyber weapon systems and technologies for Offensive and Defensive Cyber Operations, Cybersecurity Risk Management, and support to Law Enforcement and Counterintelligence operations. CNF's rapid prototyping capability produces state of art cyber defense platforms enabling efficient and all-encompassing cybersecurity for Department of Defense (DoD) enterprises, information, and infrastructure.