ENSURE COMPLIANCE IN CYBERSECURITY

ATTENTION DEPARTMENT OF DEFENSE, GSA AND NASA CONTRACTORS:
All DoD, GSA and NASA contractors must meet the Federal Acquisition Regulation (FAR) minimum cybersecurity standards or risk losing federal contracts.

If you're like many businesses, you may not know what is expected or even how to get started. Not to worry. CONNSTEP has assembled a team of leading cybersecurity experts to help ensure you will be compliant with the controls described in **NIST Special Publication 800-171**.

YOUR BEST DEFENSE IS HERE

CONNSTEP's experienced team has designed a comprehensive four-step cybersecurity program. We will help you gauge your current situation and tailor a plan specifically for your internal capabilities, budget and time sensitivity. Here's how it works:

STEP 1: DISCOVERY – the professional assessment of your company's practices related to the new standard. If necessary, a gap analysis will be completed to document the scope to be remediated.

STEP 2: REMEDIATE TO MEET NEW STANDARD – supports all necessary fixes to ensure compliance. This may include updates to firewalls, patches, policy development, employee training, physical security, network configuration, etc.

STEP 3: TEST AND VALIDATE – verifies that all technology and physical security aspects are working properly. A penetration test may be necessary.

STEP 4: MONITORING/REPORTING – establishes ongoing monitoring and scanning of the required enterprise network. Creates a working process to log, remediate and report (as required) cyberattacks.

DON'T RISK LOSING BUSINESS. WE CAN HELP.
Contact CONNSTEP today at **800.266.6672 or info@connstep.org** to get started.

DID YOU KNOW:

61%
of experts in technology and policy predict a major cyberattack causing widespread harm will occur by 2025, according to a Pew Research Center report.

$445 Billion
is lost annually to cybercrime and espionage across the entire world economy, according to the Center for Strategic and International Studies.

46,605
breaches of federal computer networks occurred in 2013, according to the S. Computer Emergency Readiness Team.