MEETING THE NIST 800-171 STANDARD

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.

PRE-DISCOVERY

In order to make our discovery phase successful and productive, it will be important to gather as much information from the organization as possible prior to our onsite assessment. This enables us to make better use of our time onsite with your team, and ensures that we will be able to complete as many requirements reviews as possible during our visit.

Our pre-discovery checklists and early proof documents will center on your organization's existing policies, training programs, IT systems documentation, and the flow of data through your organization.

ASSESSMENT

The Center's assessment will map all 110 requirements of the NIST 800-171 standard to the applicable areas of your business, and provide informed analysis as to whether those requirements currently are being met. The assessment will serve as a focal point for all proof documentation, compensating controls, explanations of how applicable each requirement is to your organization, and will be cross-referenced with your remediation plan. This assessment also will include a gap analysis, which will allow your organization to understand how you are compliant to the standard.

GAP REPORT

Based on the results of our assessment, a Gap Report will be developed and presented to your organization for review. This report will contain all of the steps required to bring your business within the NIST 800-171 standard and will be constructed based on the following criteria:

> *Risk Management*
Which (currently unmet) requirements pose the greatest risk to your organization, both from a cybersecurity perspective, and whether they jeopardize your chances of gaining new federal and defense contracts?

> *Dependency Upon Other Requirements*
Which unmet requirements are dependent on related NIST 800-171 requirements being met first, in order to be satisfied?

> *Timeliness of Meeting the NIST 800-171 Standard*
How much time do we have before your organization needs to show proof of compliance, or compete for a new contract?

STEP 2: REMEDIATE TO MEET THE NEW STANDARD

This phase supports all necessary fixes to ensure compliance. This may include updates to firewalls, patches, policy development, employee training, physical security, network configuration, etc. Our solution will be vetted and delivered to your organization based on the following criteria:

> *Best Organizational Fit*
The Center will present your organization with solutions from providers who are best positioned to meet your needs, based on their scope, technical requirements, and other factors unique to your organization.

> *Budgetary Considerations*
During our pre-discovery phase, the Center will have worked with your organization to understand the scope of at-risk contracts affected by DFARS or FAR legislation, and some basic budgetary guidelines for your company's ability to meet the NIST 800-171 standard. The Center will present solutions that are best suited to meet your organization's needs, while striving to meet your budgetary concerns.

> *Compliance Best Practices*
In any circumstances where provider diversity is necessary, whether to avoid conflicts of interest, or to avoid certain restrictions regarding implementation and testing, The Center will divide the remediation plan into segments to avoid those conflicts and/or restrictions.

REMEDIATION IMPLEMENTATION

Upon selection and approval of remediation services from The Center's partners, we will track the successful completion of implementation milestones, and monitor the completion of milestones against the timelines identified in your remediation plan.

REVIEW OF REMEDIATION SERVICES & ATTAINMENT

During the attainment of certain milestones in your remediation and implementation process, and upon completion of your remediation plan, The Center will provide comprehensive updates and reporting, for use internally and with interested third parties.

STEP 3: TEST AND VALIDATE

This phase verifies that all technology and physical security aspects are working properly.

SCOPING & SELECTION OF TESTING & VALIDATION SERVICES

Based on the scope of your organization's systems and your contractors' needs for particular certifications, The Center will recommend the appropriate tests, audits and scans. The Center also will connect your organization with any relevant providers in our partner network.

STEP 4: MONITORING/REPORTING

This phase establishes ongoing monitoring and scanning of the required enterprise network as required in the standard. It also creates a working process to log, remediate and report cyber-attacks.

SCOPING & SELECTION OF MONITORING & REPORTING SERVICES

Based on the scope of your network systems and certain NIST requirements for continuous monitoring, The Center will connect your organization with our partner network of appropriate monitoring providers. The Center will also will provide standardized processes and procedures for reporting cybersecurity events to the office of the DoD CIO, per federal regulations.