CDSystems

NIST Security Assessment

WHO IS IT FOR?

- **U.S. government contractors and sub-contractors…**
  must be compliant with DFARS. DFARS requires adherence to NIST SP 800-171 – *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*.
- **Any organization concerned about cybersecurity…**
  where other, more specific regulations such as PCI or HIPAA don't apply must still follow best practices. NIST is the most generic and widely-accepted framework for cybersecurity.

WHY IS IT IMPORTANT?

- Companies could lose their federal contracts.
- Companies could lose their:
  - **Reputation** – It's hard to regain confidence after a data breach or other incident.
  - **Intellectual property** – If you lose your IP, it may be irreplaceable.
  - **Entire business** – In extreme cases, a breach could lead to complete loss of business.

HOW CAN WE HELP?

The NIST-based security assessment is designed to:

- **Identify gaps** in NIST compliance.
- **Develop a roadmap** for remediating gaps in NIST compliance.
- **Pass an audit** – Find problem areas so you can make adjustments before an audit.

WHAT IS INCLUDED?

The NIST security assessment includes:

- **NIST-based gap analysis** – Determine where the holes are in your current environment that would lead to issues meeting regulatory compliance.
- **Vulnerability assessment** – Find areas of weakness in your technical environment and a roadmap for remediation, leading to reduced organizational risk.
- **Configuration review** – Determine if unsafe or out-of-the-box settings on firewalls, servers, and other key infrastructure are putting your organization at risk.
- **Policy & procedure review** – Determine if gaps in policy exist, if policies refer to old/outdated technology, and if employees are following procedures set forth in policies.
- **Interviews with key stakeholders** – Policies are great but if employees aren't following them, action must be taken.
- **C-level and granular reporting** – Executive-level summary as well as detailed reporting.