NIST 800-171 Assessment/Cyber-Security Protocols/Best Practices

The following are a set of "best practices" from the MTI Cybersecurity Committee for you to consider in your cybersecurity policy. July 2019.

- NIST 800-171 Broken Down Into Two Main Aspects:
  - **Cyber Security Policy:** What are the rules and policies you set in place to ensure adequate security throughout your company's network. How do you safeguard servers, what are your best practices for every individual employee and their password management, use of email, data, etc. It's basically everything you do to prevent breaches whether that be to a malicious hack, employee falling victim to an email phishing scam or whatever you can dream up.
  - **CUI or Controlled Unclassified Information:** This obviously gets back to your cyber security policy but the other main focus besides that policy is on the CUI that you are handling. For ourselves, that basically means blueprints with control requirements or maybe some specifications, material specs, etc. The big concern here is with how you handle that both physically and also digitally of course. We have to safeguard how/where it is stored and work to ensure it cannot be hacked or otherwise accessed by individuals internally with malicious intent. So preventing unauthorized printing of these documents, emailing of them, sharing in any way. Compared to machine shops that might need to revise and help design a prime's print we have a leg up in that we are usually just receiving the document one way and then storing it.

- Things that should be included in your cyber security policy:
  - Regulating of our users both privileged and non-privileged.
    - Even in this basic step of establishing users and logins you must incorporate your policies from HR regarding background checks, verification and training.
  - Password policy (password management, complexity requirements, frequency of change requirements) as well as multi-factor authentication for login.
  - Education/training on best practices for various aspects of the policy to all employees. Educate on threats, what we are trying to prevent, guidance on password policy, etc. This also includes scheduled briefings with employees on current threats or trends in cyber security to be aware of.
  - Address things like remote access whether that means employees accessing emails via their phone or logging into work remotely via laptops or tablets. This could also include vendors or customers and limiting them accordingly.
  - Software: I'm not nuanced enough in this stuff but there will be plenty of additional pieces of software to consider whether that is for password management, anti-virus, firewalls, active auditing, etc.
  - Auditing: You need to have the ability/software to self-audit and obtain the results you need for actual "paper trails" on successes or failures in any aspect of the policy. This process of auditing will become scheduled and a way to constantly monitor how you are performing or if any breaches have occurred. It's not good

enough to simply run an audit, you have to of course understand it and be able to react accordingly to address any issues.
    - Email, email encryption: Pretty much everything you would imagine here in securing emails, educating employees to threats and safeguarding.
    - Establishing policy on internet usage and enforcing it.
    - Plans and policy for patching updating software or hardware to ensure everything is up to date and safeguarded as well as possible.
        - Part of this becomes creating a baseline “spec requirement” for computers, servers, etc. Minimum requirements and if anything falls out of spec updating or buying new as needed.
    - Scheduled maintenance plans for everything and ways to log and track this as well.
    - Other things that could be expanded on but I’ll just list to spare you all would be physical security, backup/recovery policies, mobile device policy, media control (external hard drives, thumb drives, CDs), risk assessments.
- Elements to consider regarding CUI:
    - What CUI does your company come into contact with that is government/DoD related?
    - How do you receive it? How is it stored both physically and digitally?
    - Do you only receive it or is there any reason it would be sent out externally?
    - If it only comes in, your primary focus becomes where is it stored and how do you protect it and limit its spread. Ideally it is stored in as few of locations as possible with as limited users as possible having access.
    - What policies or restrictions do you have in place to prevent its reproduction? Is it view only or can an employee potentially re-print it, email it out, etc.? This of course shouldn’t happen, but you have to plan for anything.
    - Regarding physical copies how do you ultimately discard of them? Are they properly destroyed? This also applies to outdated hard drives or other hardware that could contain CUI.
    - Consider everything for storage as there are things you might overlook or not naturally think about. Scanners, fax machines, etc.
    - If any company is dealing with CUI, and they do not have at least their Gap Analysis along with a completed POA&M, they do not comply with NIST 800-171,
    - Anyone who does have those completed, and is showing progress to completion, is currently in compliance.
    - This link, https://nvlpubs.nist.gov/nistpubs/hb/2017/nist.hb.162.pdf , is a self-assessment, and it’s 70 pages. Anyone who deals with ITAR / Government regulations needs to understand this isn’t a small project. It’s going to cost with man hours (inside or outside), equipment, software, hardware in the mid 5 figures.
    - Under Secretary of Defense, rules now state the US government is starting to audit primes and will eventually be looking into auditing sub-tier contractors (all of us). Which means if you do not comply, you could be losing work. Heat treaters are already getting asked by primes on their progress on this issue.