IMPACT WASHINGTON

PART OF THE MEP National Network

CYBERSECURITY BEST PRACTICES

(CMMC/NIST 800:171 IMPLEMENTATION & COMPLIANCE)

PROTECT THE CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY OF YOUR INFORMATION

Are you wondering about:

- Breach Remediation
- Complete Threat Management
- Proactive Threat Intelligence
- Penetration Testing
- Cyber Incident Reporting Guidance
- Cyber Security Compliance to (CMMC/NIST 800:171)
- How to protect your customers, company, and supplier information?

We meet you where you are to get you where you need to be

✓ Achieve a level of Cybersecurity with less cost, less time, and more security than if you tried to do this alone.

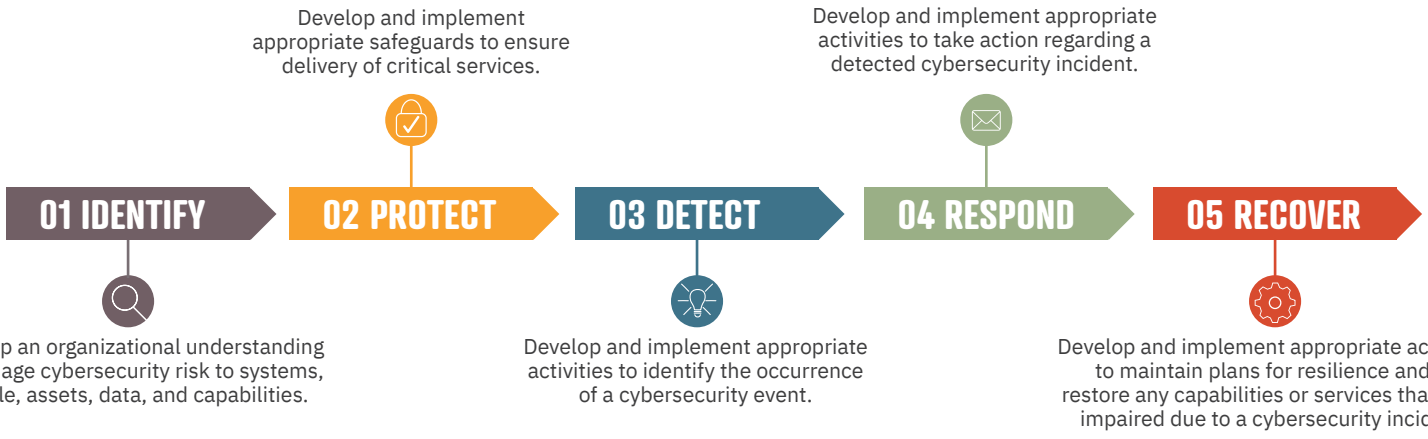
✓ Avoid Costly cyber breaches and attacks, including the cost of shutting down and recovering.

✓ You will be NIST 800-171/CMMC compliant for companies in the defense industry.

✓ Win new contracts, open new markets / and diversify the sales pipeline.

FLEXIBLE FRAMEWORK ESTABLISHES OR IMPROVES CYBERSECURITY FOR ORGANIZATIONS OF ANY SIZE

Impact Washington's guidance uses NIST Framework for Improving Critical Infrastructure Cybersecurity. The Framework was designed with Critical Infrastructure (CI) in mind and is highly versatile and applicable to organizations of all sizes, sectors, and maturities. **It is broken down into five steps: Identify, Protect, Detect, Respond, and Monitor/Recover.**



Our approach is simple...we will:

1. Assess your current state
2. Develop an organized plan to implement actions as needed.
3. Deliver remote or in-person assistance using time effective online software platform to track and complete tasks

See Framework Success Stories here.
For guidance on assessing your current state, vulnerabilities and to develop a plan to bolster your organization's Cybersecurity, contact Impact Washington

WWW.IMPACTWASHINGTON.ORG
INFO@IMPACTWASHINGTON.ORG | 425.438.1146