VMEC
VERMONT MANUFACTURING EXTENSION CENTER

PART OF THE MEP National Network™

CYBERSECURITY

As of December 31, 2017, all manufacturers involved in the Department of Defense (DoD) supply chain that handle, process, or store Controlled Unclassified Information (CUI) must comply with the Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204-7012 "Safeguarding Covered Defense Information and Cyber Incident Reporting."

These cybersecurity requirements will also soon apply to manufacturers that are part of supply chains for other federal institutions, including the General Services Administration (GSA), NASA, and the Department of Energy (DOE), per the National Archives and Records Administration (NARA).

You must comply with DFARS, if you handle any Controlled Unclassified Information:

- Covered Defense Information (CDI)
- Confidential Unclassified Information (CUI)
- Controlled Technical Information (CTI)
- DoD Critical Infrastructure Security Information (DCRIT)
- Critical Infrastructure Information (CRIT) in reduced time to market and reduced costs of manufactured product

Why Does My Company Need to Comply with DFARS requirements?

Failure to comply will **lead to the loss of DoD contracts** as DFARS requirements are enforced.

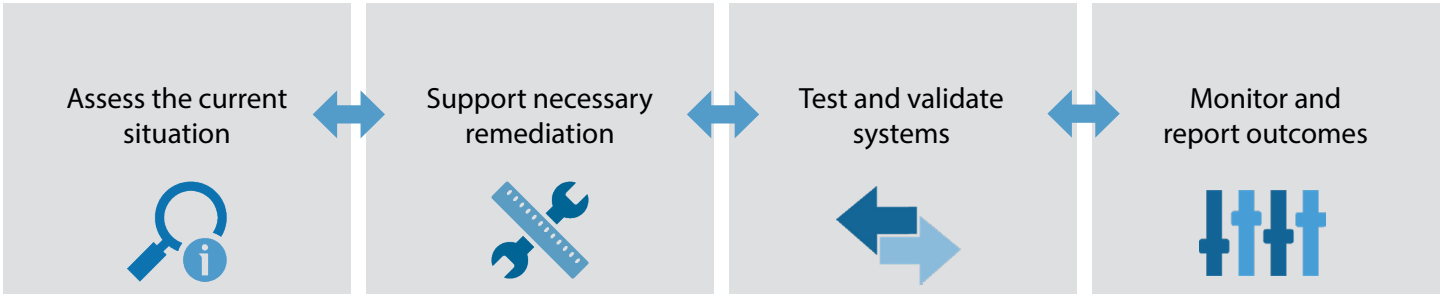
Compliance is a **competitive advantage** in the face of low adoption among DoD suppliers.

NARA will adopt similar requirements, creating a general Federal Acquisition Regulation (FAR) requirement for all federal contractors.

TAKE ACTION TO COMPLY

To become DFARS compliant, you must develop a Systems Security Plan, conduct a Security Assessment against the SP 800-171 Security Requirements, and develop a Plan of Action with detailed milestones to address any deficiencies. Work with your local MEP Center, which is connected to NIST via the MEP National Network™, to create a plan that fits your budget, capabilities, and timing.

The MEP National Network's four-step process will allow you to retain your federal contracts.



Since 2014, the MEP National Network has worked with DoD suppliers to comply with the new DFARS cybersecurity requirement. To date it has:

- Provided cybersecurity awareness and assistance to more than 3,100 small and medium-sized manufacturers that are part of DoD manufacturing supply chains.
- Published a detailed Cybersecurity Self-Assessment (NIST Handbook 162) specifically for manufacturers, which has been downloaded more than 45,000 times.
- Provided cybersecurity assistance to defense contractors in 19 states during 2018, via projects funded by the DoD Office of Economic Adjustment (OEA).

THE MEP NATIONAL NETWORK

The MEP National Network is a unique public-private partnership that delivers comprehensive, proven solutions to U.S. manufacturers, fueling growth and advancing U.S. manufacturing.

CONTACT US:

To become DFARS compliant and learn more about the emerging cybersecurity requirements for federal contractors, contact:

1540 VT RT 66, Suite 103, VT Tech Enterprise Center, Randolph, VT 05060

(802) 728-1432

vmec@vmec.org

VMEC VERMONT MANUFACTURING EXTENSION CENTER

PART OF THE MEP National Network™

www.vmec.org