CYBERSECURITY RISK MANAGEMENT WORKSHOPS

Awareness and Education for companies who are currently *(or those wanting to become)* government and/or defense suppliers

WORKSHOP DETAILS

1. Do you have government and/or defense customers?
2. Are you looking to enter or expand your presence as a supplier in the government and/or defense market?
3. Do you know about DFARS 7012, the CMMC Interim Rule, and NIST SP 800-171?
4. Are you confident that you have satisfied DoD's recently modified DFARS requirements?
5. Have you uploaded your current cybersecurity self-assessment to DoD's Supplier Performance Risk System (SPRS)?

If you answered "yes" to questions 1 and/or 2 and are interested in more information about questions 3 through 5, please register for one of these in-person or virtual workshops.

These hands-on workshops will address these questions, provide a road map and implementation tools, and teach you how to use them to secure your information.

Following the workshops there will be an opportunity to participate in virtual follow-on mentoring/coaching cohort sessions, which will run from September - November.

LOGISTICS

DATES / LOCATIONS:
8:30 a.m. - 4:00 p.m. (CT)

September 14
Fargo

September 15
Grand Forks

September 15
Virtual

September 16
Minot

September 17
Bismarck

TO REGISTER:
www.impactdakota.com/events

These workshops are **FREE** and lunch will be provided.

Workshop registration fees covered by a UND Center for Innovation OLDDC-OEA grant.

Meet the Presenters:

Matt Christmann, Iviry System Analyst and Cyber Compliance Specialist, has over 15 years USMC experience working in intelligence fields. He has been certified as a CMMC Registered Practitioner (RP) and has a Security+ CE certification. Matt has spent the last several years providing guided gap analysis sessions to contractor organizations to identify current states of compliance. He also provides detailed planning and project management support for remediation actions and develops tailored policy and plan documentation in support of NIST and CMMC requirements.

Jennifer Kurtz, Cyber Program Director for the Colorado MEP center (Manufacturer's Edge) is the designated "go-to" cybersecurity lead for the NIST MEP Rocky Mountain states (CO, MT, ND, SD,
UT, WY). She was on the security design team for the first IRS electronic tax filing program in the early 1990s; created and implemented the first system security plan at Delco Remy International in the late 1990s; developed and taught graduate courses in telecommunications, cybersecurity, and project management at Ball State University and Regis University for 13 years; and has completed more than 20 client engagements to implement security standards in the past few years. She is a member of the NIST MEP Cybersecurity Working Group and Steering Committee teams, recognized as an internationally published author, and invited speaker and panelist for numerous conferences and webinars.

Jodie Mjoen, Impact Dakota Chief Operating Officer/Senior Business Advisor, has 26 years' experience implementing federal, industry and customer regulatory compliance requirements at manufacturers throughout the United States and abroad. He is a member of the NIST MEP National Network (NN) Cybersecurity Working Group team and the Cyber Program Lead for Impact Dakota. Jodie has been providing ND manufacturers with Cybersecurity support services since 2019.

Workshop Presenters & Partners:

IMPACT DAKOTA
People • Purpose • Process • Performance
Impact Dakota is the official representative of the MEP National Network in North Dakota.

IVIRY

Manufacturer's EDGE
TRANSFORMING COLORADO ONE COMPANY AT A TIME

UND CENTER FOR INNOVATION
UNIVERSITY OF NORTH DAKOTA

NORTH DAKOTA SMALL BUSINESS DEVELOPMENT CENTERS
Your Ideas - Our Expertise - Your Success

BSC BISMARCK STATE COLLEGE
North Dakota's Polytechnic Institution

MINOT STATE UNIVERSITY

NDSU NORTH DAKOTA STATE UNIVERSITY

NORTH DAKOTA PROCUREMENT TECHNICAL ASSISTANCE CENTER
Government Contracting Assistance